Mémoire présenté devant le CNAM
pour l'obtention du diplôme de Master Droit Economie Gestion mention Actuariat
et l'admission à l'Institut des Actuaires
le 20 janvier 2022

Par : Rosalba MATERA LAURENT

Titre: La gestion du risque cyber dans les captives

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 signatures

Alexandre HASSLER
Nicolas ZEC

Membres présents du jury de la filière

Nathanaël ABECERA
David FAURE
François WEISS

Présidente du jury

Sandrine LEMERY

Secrétariat :

Bibliothèque :

Entreprise :

Nom : MARSH SAS

Directeur de mémoire métier :

Nom : Jean-Marie NESSI

Signature :

Invité :

Nom : Cyrille BRAND

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

Signature du candidat

RESUME

Mots clés : Cyber, cyber silencieux, captive, R, tarification, générateurs de scénarios, exposition, perte d'exploitation, vol ou perte de données personnelles, benchmark, solvabilité, modèle interne partiel

Le développement croissant des technologies de l'information rend l'utilisation d'ordinateurs et d'objets connectés de plus en plus incontournable. Dans ce contexte, les cyber-attaques contre les systèmes informatiques des entreprises ont explosé et se poursuivront dans le futur.

Sur le plan assurantiel, ce risque est encore mal connu car les entreprises « attaquées » préfèrent ne pas communiquer afin de préserver leur réputation. De plus, l'imagination débordante des hackers n'a sûrement pas encore dévoilé toutes les possibilités de sinistres envisageables.
Il reste difficile pour un assureur de proposer un tarif pour une couverture d'assurance cyber.

Par ailleurs, certaines grandes entreprises ont mis en place des sociétés d'assurance captives dans l'objectif d'y céder une partie de leurs risques appelés « risques propres ». Cet outil stratégique leur permet de prendre une part active à leur gestion des risques et d'optimiser le transfert au marché de l'assurance. La souscription de programmes « Cyber » peut rentrer dans ce cadre, en fonction des conditions et des cycles du marché, et de l'appétence aux risques de l'entreprise et de sa captive.

Mais toutes les captives ne portent pas le risque Cyber de façon visible. En effet, un sinistre « Cyber » majeur pourrait être pris en charge par un programme « dommage » ou « Responsabilité Civile » si le risque cyber n'est pas explicitement exclus. Si cette partie de risque n'a pas été tarifée de manière explicite, les résultats et la solvabilité de la captive risquent d'en être affectés.

Ce mémoire propose des pistes d'optimisation de la gestion du risque « cyber » dans les captives et une mesure des conséquences potentielles d'une exposition au risque "Cyber silencieux". Sont abordées les questions d'exposition, de tarification puis dans une approche prospective, de solvabilité.

Dans cette étude, les captives sont évoquées en tant qu'outil de gestion des risques - au-delà d'éventuelles considérations d'avantages offerts par certaines juridictions. De plus, le risque cyber est étudié en tant que risque de souscription, le risque opérationnel de la captive est exclu.

ABSTRACT

Key words: Cyber, silent cyber, captive, R, pricing, scenario generators, exposure, business interruption, data breaches, benchmark, solvency, partial internal model.

The increasing development of information technologies makes the use of computer and connected objects more and more unavoidable. In this context, cyber-attacks against corporate IT systems have exploded and this trend will continue in the future.

On an insurance point of view, this risk remains poorly known, because companies under attack prefer not to communicate to preserve their reputation. Moreover, the overflowing imagination of hackers has certainly not yet revealed all the possible future disasters.
It is still difficult for an insurer to suggest a price for a cyber insurance cover.

In addition, some groups have set up captive insurance companies with the aim of ceding part of their risks, commonly known as "own risks", to them. This strategic tool allows them to take an active part in their risk management and optimize the transfer to the insurance market. The underwriting of "Cyber" programs can fit into this framework, depending on market conditions and cycles, and on the risk appetite of the company and its captive.

But not all captives carry the Cyber risk in a visible way. Indeed, a major "Cyber" loss could be covered by a "damage" or "Third Party Liability" program if the Cyber risk is not explicitly excluded. If this portion of risk has not been explicitly taken into consideration in the pricing, the captive's results and its solvency may be affected.

This study suggests optimizing the management of the "Cyber" risk into the captives and to measure the potential consequences for captives exposed to "silent cover".

In this study, captives are considered as a risk management tool - beyond possible considerations of benefits offered by certain jurisdictions. In addition, cyber risk is examined from the perspective of underwriting risk, so it excludes the operational risk due to cyber-threat in the captive.

REMERCIEMENTS

J'adresse mes plus profonds remerciements à mon tuteur métier, Monsieur Jean-Marie Nessi, Président de l'organisme de formation CARITAT pour le temps qu'il a consacré à m'encadrer dans la réalisation de ce mémoire, ses conseils avisés mais également son dynamisme à me motiver dans la poursuite de cette tâche ardue.

Je tiens également à remercier la société MARSH par l'intermédiaire de mon Directeur, Monsieur Cyrille Brand de m'avoir donné la possibilité de réaliser ce mémoire qui permet d'approcher de façon plus précise la tarification et la quantification de l'exposition du risque Cyber des clients de MARSH et de leurs captives.

Je souhaite également exprimer ma reconnaissance à tous les membres de ma fantastique équipe Analytics Solutions de MARSH Paris. En effet, Jennifer, Nasser, Olga, Cathia, Weronika, Vanessa, Claire et Bogdan m'ont accompagnée dans ce périple dans une ambiance de travail agréable, affichant leur bonne humeur, leur soutien indéfectible et prodiguant leurs conseils.

Je salue également les anciens et nouveaux professeurs du CNAM Actuariat, ainsi que le personnel administratif, qui m'ont apporté les outils nécessaires à la concrétisation de mon parcours en actuariat de nombreuses années après la fin de mon parcours académique initial.

Une pensée profonde va également à mes amis du CNAM et notamment à Audrey, Lucile, Murielle, Alexis, Walid, Baptiste, Guillaume, Nico, Raphaël … afin qu'ils s'accrochent pour cette dernière ligne droite de travail sur le mémoire … car le jeu en vaut la chandelle !!

Enfin, je remercie ma famille et plus particulièrement mon époux François et mes enfants Pierre et Anaïs qui m'ont soutenue dans ce projet « fou » et qui ont supporté avec patience mes doutes lors des examens et lors de la réalisation de ce mémoire.

SOMMAIRE

INTRODUCTION

Avec le développement des nouvelles technologies, le déploiement massif de l'utilisation des applications connectées dans la gestion de la vie courante, les attaques et piratages des réseaux se sont multipliés.
Les entreprises ne sont pas épargnées, la numérisation des processus de production est régulièrement la cible des pirates à l'affût d'une faille dans les systèmes d'information. Ceci est d'autant plus vrai que les chaînes d'approvisionnement ou d'autres parties opérationnelles de bon nombre d'entreprises se trouvent souvent réparties dans le monde, ce qui augmente le nombre de risques auxquels ces entreprises sont exposées.

Pour les entreprises comme pour les particuliers, la question n'est donc pas de savoir SI ils sont exposés au risque Cyber mais plutôt QUAND ils auront à subir une attaque et de quelle ampleur celle-ci sera ?

Si nous considérons les plus petites entreprises, celles-ci ont souvent estimé qu'elles n'étaient pas autant exposées que les grosses entreprises internationales, ce que les exemples d'attaques récentes ont démenti. Selon une étude conduite par Forrester Consulting[1], *« 67% des entreprises françaises ont été victimes d'un cyber-incident sur l'année 2018. Les PME ont été clairement de plus en plus visées par les cybercriminels puisque 47% des entreprises de moins de 50 salariés ont déclaré avoir été touchées en 2018 contre 33% l'année précédente, et 63% des entreprises de taille moyenne (50 à 249 employés) assurent avoir été victimes en 2018 contre 36% en 2017 »*. Ainsi, les petites entreprises n'ont pas encore pris conscience qu'elles doivent développer et déployer une organisation appropriée de cyberdéfense qui les rendra d'autant moins vulnérables. Elles ne se sentent pas encore réellement concernées par des couvertures d'assurance adéquates.

Les grandes entreprises quant à elles sont de plus en plus sensibles à se couvrir contre ce risque grandissant et font de plus en plus appel aux assureurs et aux réassureurs afin de leur réclamer des solutions adaptées à leur taille et à leur profil de risque. Souvent, elles réussissent à mettre en place avec leurs assureurs des programmes de couverture sur-mesure adaptés à leur profil.

Mais le risque cyber est encore mal connu et mal maitrisé, et les offres déployées par les assureurs ne sont pas encore très matures, certains acteurs étant réticents à développer des couvertures pour ce type de risque.

[1] L'étude *Cyber-sinistres Hiscox 2018* a été réalisée par Forrester Consulting sur la commande du groupe international d'assurances spécialisées notamment en cyber-risques Hiscox. Elle est basée sur une enquête réalisée en ligne du 12 octobre au 7 décembre 2018 auprès de 5 392 professionnels (plus de 1 000 pour le Royaume-Uni, les Etats-Unis et l'Allemagne, et 500 pour la Belgique, la France, l'Espagne et les Pays-Bas), dressant un échantillon représentatif de toutes les tailles d'entreprises et des différents secteurs.

L'approche TOUT RISQUE SAUF …

En effet, d'un point de vue assurantiel, les premiers sinistres « cyber » observés étaient pris en charge par des couvertures dans lesquelles ils n'étaient pas nommément ni inclus ni exclus. Les programmes d'assurance Dommages et Responsabilité Civile des entreprises ont, à cet effet, été utilisés comme des polices 'TOUT RISQUE SAUF …' couvrant ainsi ces sinistres d'une typologie nouvelle et non spécifiquement exclus. La tarification de ces polices ne tenait pas compte de cette composante mettant ainsi en danger l'équilibre du portefeuille de ces types de contrats pourtant standards. La survenance de plus en plus fréquente d'attaques aux systèmes d'information a alors permis au cours des dernières années d'identifier les premiers sinistres « cybers », de les qualifier et de développer une nomenclature pour les nommer en définissant certaines typologies d'incidents (les « ransomware » par exemple).

Une nomenclature évolutive

La logique de police TOUT RISQUE SAUF … a évolué vers une logique de couverture de sinistres nommément désignés puisque l'observation d'incidents relatifs au risque cyber a entrainé une meilleure connaissance de ces typologies de sinistres. Pour que l'industrie de l'assurance se donne les moyens de couvrir ce risque, elle doit mettre en place des bases de données relevant les incidents, les sinistres ainsi que la manière dont les incidents se transforment en sinistres. Elle développera alors ses connaissances du risque, et grâce à ces bases de données, elle pourra mettre en place des outils de tarification en y associant une courbe d'apprentissage.

L'entreprise qui peut subir une attaque cyber, doit de son côté être consciente de ce risque et mettre en place une gestion des risques lui permettant de faire face à ce nouveau danger. Elle attend également une réponse du marché de l'assurance qui peut s'avérer relativement éloignée de ses préoccupations, car la couverture de son exposition réelle ou de ses actifs incorporels peut parfois lui paraitre insuffisante. En effet, la simple observation de l'évolution de la sinistralité, de sa typologie, fait clairement apparaître que celle-ci ne cesse d'augmenter et d'étendre son champ.

L'utilisation de la captive

La plupart des grandes entreprises ont un avantage intéressant sur le plan de la gestion du risque, car elles possèdent des sociétés d'assurance et/ou de réassurance captives, qui constituent des outils stratégiques leur permettant d'optimiser leur gestion du risque. La captive retient une part du risque difficilement transférable au marché et l'entreprise va s'auto-assurer pour cette partie du risque.

Ainsi elle acquiert une certaine expérience de la spécificité des sinistres liée à ce risque, elle apprend à gérer le risque, à construire sa propre courbe d'expérience, tout en ayant comme objectif l'amélioration de la gestion des incidents et la mise en place des plans de prévention adaptés à ses exigences et à ses typologies propres.

La captive s'avère donc un outil particulièrement intéressant pour aider l'entreprise à connaitre et à appréhender le risque cyber. Pilotées depuis la captive, les informations sont étudiées spécifiquement

pour le groupe dans le cadre de son ERM. La captive fait ainsi le lien avec le marché et maîtrise mieux la gestion de son transfert vers les assureurs externes voire les réassureurs.

Toutes les entreprises ne vont pas forcément utiliser leurs captives pour se couvrir contre le risque cyber, d'autres peuvent ne pas être réellement conscientes de l'évolution « pressentie » que pourrait prendre ce risque dans le futur, du fait de nouvelles typologies d'attaques imaginées par les cybers criminels. Dans ce cas, même si ces entreprises souscrivent le risque cyber dans leur captive, la police transférée peut s'avérer insuffisante pour couvrir les nouvelles typologies d'incidents. Parfois même, certaines entreprises vont préférer ne pas s'assurer et assumer entièrement le risque cyber.

Une nécessité d'adaptation du marché de l'assurance

La base Cyence fournies par la société Guidewire Cyence Risk Analytics™, mesure l'impact financier des risques cyber pour le secteur de l'assurance via la science des données et la modélisation financière. Fort de l'appui de cet outil et d'autres outils développé grâce au big data et à l'intelligence artificielle, le marché de l'assurance peut adapter son offre en tenant compte de la prise de conscience et de la gestion plus opérationnelle de ce risque par les entreprises. Il pourra utiliser cette expérience développée grâce à la gestion des risques dans les Entreprises pour parfaire ses connaissances et son offre assurantielle.

L'approche utilisée dans ce mémoire

Dans ce mémoire, la problématique du risque cyber est abordée sur un échantillon d'entreprises qui possède une ou des captives car il a vocation à mesurer le risque souscrit par la captive qu'il soit dénommé ou silencieux.
La première étape consiste à mesurer l'exposition[2] de ces entreprises au risque cyber en utilisant les données de la base commune d'incidents du marché de l'assurance, la base Cyence. Les générateurs de scénarios développés par le courtier Marsh à partir de l'observation de sinistres passés simulent des événements qui servent alors de base de données à l'évaluation des pertes d'exploitation et des pertes consécutives au vol et à la perte de données. Ils permettent de caractériser les expositions de l'entreprise au risque cyber et de quantifier la part de ce risque transféré à la captive, par l'utilisation d'un modèle de tarification développé sur la base des scénarios.

En parallèle, les captives des groupes étudiées sont classées selon les programmes qu'elles souscrivent.

- Soit la captive couvre déjà le risque cyber par un programme spécifique.
- Soit la captive couvre des programmes dans lesquels le risque cyber n'est pas spécifiquement exclu. Dans ce cas, elle pourrait être exposée en cas de sinistre, car les programmes RC, Dommages mais aussi Fraude et D&O (Responsabilité Civile des Mandataires Sociaux) peuvent engober le risque Cyber dit « silencieux ».
- Soit la captive n'a pas d'exposition au risque Cyber,

[2] L'exposition sous-entend l'exposition maximum d'une entreprise à savoir le sinistre maximum qu'elle pourrait subir.
Une analogie peut être réalisée avec le SMP (Sinistre Maximum Possible) utilisée pour la branche « dommage ».
L'exposition peut aussi être déclinée en fonction des percentiles et donner les montants de sinistres correspondant à chaque percentile ou **période de retour**. La période de retour représente l'inverse du percentile et est associée à la fréquence d'un sinistre selon sa sévérité.

Dans cette étude, il convient de noter que les captives sont étudiées d'un point de vue de leur risque de souscription et non de leur risque opérationnel.

Une classification sur les données *a priori*, qui ont servi à alimenter les générateurs de scénarios est réalisée sur l'ensemble de l'échantillon des captives. Celle-ci va permettre de dégager le cas échéant, des classes de captives homogènes, qui pourraient être regroupées et éventuellement restreindre l'étude de tarification à un nombre moins important de captives. La classification va permettre d'apporter des détails sur les caractéristiques des « classes » de captives.

Dans un deuxième temps, les résultats du modèle de tarification développé avec les scénarios sont comparés aux primes que souscrivent les captives qui couvrent déjà des programmes cyber. Un *back testing* est également réalisé en utilisant un benchmark de sinistres cyber recueilli par Marsh et permettant d'ajuster une distribution de la sévérité.

Puis le risque « cyber silencieux » est mesuré sur les programmes des captives qui pourraient être appelés en cas de sinistre, même si celles-ci ne souscrivent pas du risque cyber dénommé. Une estimation de la « prime manquante » est comparée à la prime souscrite par la captive pour les programmes identifiés. Il s'agit d'estimer la part de prime qui aurait dû être tarifée – avec le modèle développé - si la tarification initiale avait tenu compte de possibles sinistres liés au risque cyber.

Pour aller plus loin, une piste de réflexion est également proposée sur le calcul du SCR CAT Non-Vie et sa composante liée au risque Cyber. En effet, avec la Formule Standard et la classification des programmes cyber dans la LoB « Pertes Pécuniaires Diverses », la prise en compte de ce risque dans le SCR CAT se fait en considérant 40% de la prime, ce qui semble relativement « optimiste ». Plusieurs possibilités de Modèles Internes Partiels sont simulées. Le plus conservateur suggère l'utilisation du 99,5^{ème} percentile de la distribution des programmes souscrits par la captive.

PARTIE I – CONTEXTE DE L'ETUDE

A. LE RISQUE CYBER

Selon Allianz Risk Barometer[3], en 2020, le risque cyber devient pour la première fois la menace numéro un identifiée par les entreprises, alors qu'il n'émergeait qu'au 15ème rang 7 ans plus tôt.
Ce classement est corroboré par l'étude de la commission des risques de la FFA[4] (Fédération Française de l'Assurance) qui pour la 4ème année consécutive classe le risque de cyberattaques létales comme risque émergent principal pour les assureurs et les réassureurs. Rajoutons à cela qu'en 2020, le confinement et le développement du télétravail du fait de l'épidémie de COVID 19 a largement contribué à l'augmentation des attaques cyber et en parallèle aux dépenses mondiales en équipements, logiciels et services liés à la sécurité informatique. En effet, selon une étude de marché réalisée par International Data Corporation (IDC), celles-ci se sont élevées à 125,2 milliards de dollars en hausse de 6% par rapport à 2019.

Dans la première partie de cet exposé, nous définissons le risque Cyber ainsi que les différentes typologies d'attaques perpétrées par les cyber terroristes. Nous décrivons les possibles conséquences et leurs évolutions au cours du temps. Pour ce faire, nous analysons les spécificités des 10 attaques cyber les plus médiatiques sur les 10 dernières années et celles relatées par les médias pour l'année 2020. Cette analyse nous permet de dégager les évolutions des typologies de cyber attaques depuis 10 ans et les tendances pour le futur, dans un contexte où l'utilisation d'internet et des objets connectés ne cessent d'augmenter. En 2020[5], 60% de la population mondiale était connectée à internet soit un total de 4,66 milliards d'internautes dans le monde, parmi lesquels 4,2 milliards utilisent les réseaux sociaux représentant 6h54 passées en moyenne en ligne *selon le dernier Digital Report 2021, publiée par Hootsuite et We Are Social.*

1. DEFINITIONS

Définir un risque est toujours une tâche ardue puisqu'il s'agit de poser un cadre autour d'évènements aléatoires suceptibles de causer des dommages. Il existe une multitude de définitions du risque cyber, différant selon les acteurs et les enjeux auxquels ils font face.

Le terme *« cyber »* est l'abréviation de cyberspace. Le cyberspace représente le domaine intéractif composé de tous les systèmes numériques utilisés pour stocker, modifier et communiquer l'information.

[3] Baromètre des risques 2020 d'Allianz : les incidents cyber pour la première fois en tête des risques d'entreprise| AGCS
[4] Cartographie 2020 des risques émergents pour la profession de l'assurance et de la réassurance | Fédération Française de l'Assurance (ffa-assurance.fr)
[5] Digital 2021 - Social Media Marketing & Management Dashboard - Hootsuite

Il comprend tous les systèmes d'information utilisés en support des infrastructures, des services et du commerce. La définition du risque cyber doit donc couvrir l'intégralité des systèmes d'information et les risques propres à leur utilisation.

La *« risque cyber ou cyberrisque »* est défini par le gouvernement français comme *« une atteinte à des systèmes informatiques réalisée dans un but malveillant ».* Elle cible différents dispositifs informatiques : des ordinateurs ou des serveurs, isolés ou en réseaux, reliés ou non à Internet, des équipements périphériques tels que les imprimantes, ou encore des appareils communicants comme les téléphones mobiles, les « smartphones » ou les tablettes.

Il existe quatre types de risques cyber aux conséquences diverses, affectant directement ou indirectement les particuliers, les administrations et les entreprises : la cybercriminalité, l'atteinte à l'image, l'espionnage, le sabotage.

Ainsi le cyber risque se définit comme tout risque de perte financière, d'interruption des activités ou d'atteinte à la réputation d'une entreprise en raison d'une défaillance des systèmes de technologies de l'information.

L'**APREF**[6] (Association des Professionnels de la Réassurance en France) dans son étude sur l'assurabilité de risques cyber (2016) complète cette définition en définissant le risque cyber comme toutes atteintes à :

- Des systèmes électroniques et/ou informatiques [de production, d'exploitation, de gestion d'informations et de télécommunication] sous le contrôle de l'entité ou de ses prestataires et/ou
- Des données informatisées (personnelles, confidentielles ou d'exploitation) appartenant à ou sous le contrôle de l'entité, qu'elles soient transférées ou stockées chez elle ou chez ses prestataires

Consécutives à :

- Un acte malveillant ou de terrorisme
- Une erreur humaine, une panne ou des problèmes techniques
- Un évènement naturel ou accidentel

Ayant pour conséquences :

- Des dommages corporels, matériels, et/ou immatériels (frais ou pertes financières), subis par l'entité et/ou ses employés
- Une mobilisation de ressources internes ou externes
- Des dommages corporels, matériels, et/ou immatériels, frais ou pertes financières causés par l'entité à des tiers (y compris chaines logistiques / sous-traitants)
- Une atteinte à la marque et/ou à la réputation de l'entité

[6] Étude sur la réassurance des Risques Cyber - Juin 2016 - APREF

Le réassureur Swiss Re[7] résume de son côté cette définition en qualifiant le risque cyber comme *« n'importe quel risque provenant de l'utilisation de données et leur transmission ».* Ces deux définitions intègrent les dommages physiques causés par les cyber attaques, les pertes et corruptions de données et ses conséquences financières. Il est intéressant de noter que les définitions des réassureurs sont beaucoup plus larges que celle donnée par le gouvernement français. Elles ne restreignent pas seulement aux intentions malveillantes et englobent toutes les causes possibles d'un sinistre cyber.

Sources of Cyber Risk (From Swiss Re report "*Cyber Risk : Too Big to Insure ?*")

Non-criminal Sources	
Act of nature	Power outage after a natural catastrophe, destruction of servers or computer facilities by flooding, fire, etc.
Technical defects	Hardware failure, e.g., data loss after a head crash of the hard-drive or a computer crash; bug in software
Human failure	Unintentionally disclosure of information on webpage, false report
Criminal Sources (Cybercrime)	
Physical attacks	Physical data theft, e.g., theft of confidential bank data by an employee
Hacker attacks	Espionage of customer data or sabotage of company processes, e.g., DoS attack, key logger, or malware[5] (virus, worms, spam-mails, Trojan horses)
Extortion	Threats by internet, e.g., Mexican drug cartel

Table I.A.1 – la répartition du risque Cyber en risque criminel et risque non criminel

De leurs côtés, les régulateurs et le marché, catégorisent le risque cyber comme un risque opérationnel. Ainsi, le risque cyber peut se définir comme « *un risque opérationnel portant sur les nouvelles technologies et l'information qu'elles véhiculent, qui affecte la confidentialité, la disponibilité et/ou l'intégrité de l'information ou des systèmes d'information ».*

AU FINAL …

En résumant les différentes définitions proposées ci-dessus, il se dégage que le risque cyber se caractérise avant tout par une atteinte aux systèmes d'information. Cependant ce risque peut s'avérer de deux façons différentes :

[7] Cyber – a risk we need to insure | Swiss Re

- La première intentionnelle car elle fait suite à un acte de malveillance, dans laquelle la notion de volonté de nuire prend tout son sens.
- Mais le risque cyber peut aussi survenir de façon non intentionnelle que ce soit à la suite d'une panne, un défaut technique ou à une erreur humaine.

Selon le courtier Marsh, 20% des sinistres cyber recensés et gérés pour le compte de ses clients grands comptes sont non-intentionnels contre 80% liés à un acte de malveillance.

2. LES DIFFERENTES TYPOLOGIES D'ATTAQUE[8]

Une cyberattaque quant à elle se définit comme tout type d'action offensive qui vise des systèmes, des infrastructures ou des réseaux informatiques, ou encore les ordinateurs personnels, le réseau, les périphériques, la connexion internet etc. Elle s'appuie sur diverses méthodes pour voler, modifier ou détruire des données ou des systèmes informatiques.

Les cyber-attaques ont évolué au cours du temps et ce, au gré de l'imagination débordante des cyber terroristes, qui se poursuivra sûrement dans le futur et nous apportera de mauvaises surprises. Nous donnons ci-dessous la typologie et la définition des différentes attaques perpétrées en 2020.

a. Attaque par Déni de Service (DoS), Attaque par Déni de Service Distribué (DDoS)

Ces attaques visent à rendre indisponible un serveur, un service ou une infrastructure. Ces attaques peuvent prendre différentes formes :

- Saturation des bandes passantes
- Epuisement des ressources du système de la machine, du serveur, du service ou de l'infrastructure concerné(e)

Plus concrètement, ce type de cyberattaque vise à surcharger de requêtes la ressource ciblée, de façon à épuiser la bande passante et provoquer un net ralentissement ou un arrêt total de fonctionnement. Les hackers peuvent également utiliser plusieurs périphériques compromis pour lancer ce type d'attaque, ce sont DDoS (Déni de Service Distribué).

b. Programme malveillant (malware)

Il s'agit d'un logiciel indésirable installé dans votre système sans votre consentement. Il peut se cacher dans un code légitime, dans des applications ou alors se reproduire sur internet. Les malwares attaquent donc par le biais d'une vulnérabilité qui télécharge par la suite un logiciel malveillant. Il en existe plusieurs sous-catégories comme le cheval de Troie, les virus divers. L'annexe A reprend les définitions des typologies de programmes malveillants.

[8] Les 10 types de cyberattaques les plus courants (netwrix.fr)

Durant la pandémie de COVID 19, les rançongiciels (ransomware), qui représentent un type de programme malvaillant, ont explosés. Ils sont devenus la menace informatique qui pèse aujourd'hui le plus sur les entreprises et les institutions.

Ce type d'attaque cyber est donc défini de façon plus détaillée ci-dessous et fera l'objet d'un paragraphe particulier lorsque les différents sinistres historiques seront répertoriés.

Un rançongiciel est un logiciel malveillant qui prend en otage les données dans l'attente du paiement d'une rançon. Le pirate exploite une faille pour bloquer l'accès aux données de sa victime, les contenus sont alors chiffrés totalement ou partiellement, de façon à les rendre inexploitables sans une clé de déchiffrement. Ensuite le pirate demande de verser une somme d'argent en échange de la clé qui permettra de les déchiffrer. En général, le hacker demande à être payé en cryptomonnaie, comme le Bitcoin par exemple.

Les rançongiciels se propagent par des pièces jointes aux messages électroniques, des programmes infectés et des sites Web compromis. Lorsque le destinataire ouvre le lien ou la pièce jointe, le malware crypte les données et monétise l'accès à la clé de déchiffrement.

Un programme malveillant de rançongiciel peut également être appelé cryptovirus ou crypto-cheval de Troie.

c. Hameçonnage (phishing) / ingénierie sociale

Ces types d'attaques combinent **ingénierie sociale** et **compétences techniques**. Elles consistent en l'envoi d'emails qui semblent provenir de sources de confiance dans le but de collecter des données personnelles ou d'inciter les victimes à une action. Ces attaques peuvent se dissimuler dans une pièce jointe de mail, ou bien utiliser un lien pointant vers un site web illégitime pour vous inciter à télécharger des logiciels malveillants ou transmettre certaines données personnelles.

Le hameçonnage fait partie de **l'ingénierie sociale** (social engineering en anglais) qui dans le contexte de la sécurité de l'information, constitue une pratique de manipulation psychologique à des fins d'escroquerie. Cette pratique exploite les faiblesses psychologiques, sociales et plus largement organisationnelles des individus ou organisations pour obtenir quelque chose frauduleusement (un bien, un service, un virement bancaire, un accès physique ou informatique, la divulgation d'informations confidentielles, etc.).

d. Téléchargement furtif (Drive by Download)

Il s'agit d'une méthode courante de propagation de logiciels malveillants. Les cyberattaquants « hackent » des sites web non sécurisés en insérant un script dans le code http ou PHP d'une des pages web. Ainsi ils installent des logiciels malveillants directement sur l'ordinateur d'un visiteur du site, via un téléchargement furtif. Ce dernier peut se faire à l'insu de l'utilisateur ou bien avec son consentement mais sans qu'il n'en comprenne les conséquences : téléchargement de programmes malveillants ou simplement non désirés.

e. Cassage de mot-de-passe

C'est le moyen le plus courant d'authentification pour accéder à un système. Il n'est donc pas surprenant que ce type d'attaque soit repandu.

f. Injection SQL (Structured Query Language)

Problème récurrent affectant les sites web exploitant des bases de données. Ces attaques se produisent lorsque qu'un cybercriminel exécute un morceau de code SQL (langage informatique normalisé) pour manipuler une base de données et accéder à du contenu potentiellement sensible. Ces données sont alors consultables, modifiables et supprimables.

g. Attaque de l'homme au milieu (MitM) / vols d'identifiant

Il s'agit d'une technique de piratage consistant à intercepter des échanges cryptés entre deux personnes ou deux ordinateurs pour en décoder le contenu. Le hacker doit donc réceptionner les messages des deux parties et répondre à chacune se faisant passer pour l'autre. Il en existe plusieurs types parmi lesquels :

- Détournement de session entre un client de confiance et un serveur, grâce à la subtilisation de l'adresse IP du client
- Usurpation d'IP
- Relecture : se produit lorsqu'un attaquant intercepte puis enregistre d'anciens messages, et tente plus tard de les envoyer se faisant ainsi passer pour un des participants à la conversation.

h. Cross-site scripting (XXS)

Le cyberattaquant insère un JavaScript malveillant dans la base de données d'un site web. Quand l'internaute visite une page de ce site web, ce dernier transmet cette page à son navigateur avec le script malveillant intégré au code HTML. Le navigateur de l'internaute exécute alors ce script, envoyant par exemple le cookie de la victime au serveur de l'attaquant, qui l'extrait et peut l'utiliser pour détourner la session.

Ces vulnérabilités peuvent entraîner de plus lourdes conséquences qu'un vol de cookie, comme l'enregistrement des frappes de touches, des captures d'écran, de collecte de contenus sensibles et d'accès et contrôle à distance de l'ordinateur de l'internaute victime.

i. Ecoute clandestine

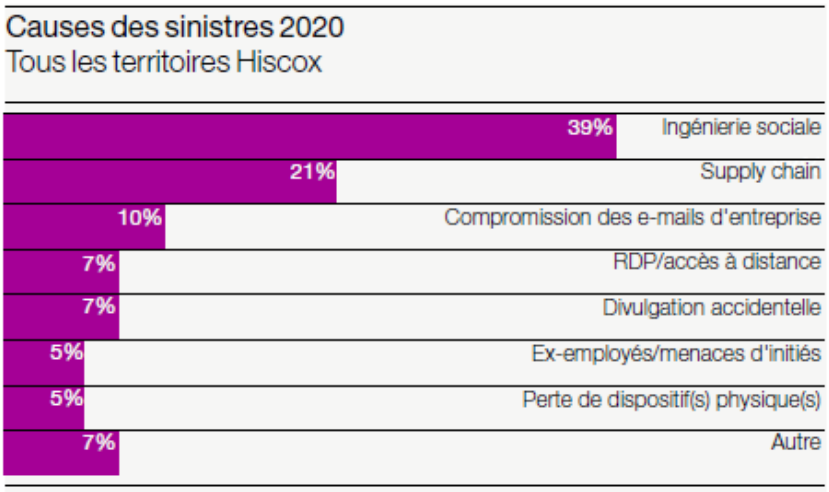
L'écoute clandestine ou illicite est le résultat d'une interception du trafic réseau. Le cyberattaquant peut alors obtenir mot de passe, numéros de cartes bancaires et autres contenus sensibles que l'internaute envoie sur le réseau concerné. Il en existe deux types :

- Ecoute clandestine passive : un pirate intercepte des données en écoutant la transmission de messages sur le réseau
- Ecoute clandestine active : un pirate s'empare activement d'informations en se faisant passer pour une unité amie et en envoyant des requêtes aux transmetteurs.

j. Attaque des anniversaires

Ces cyberattaques sont lancées contre les algorithmes de hachage qui vérifient l'intégrité d'un message, d'une signature numérique ou d'un logiciel. Ce type d'attaque exploite les notions mathématiques équivalentes à celles qu'utilise le paradoxe des anniversaires[9] en théorie des probabilités. Cette attaque est généralement perpétrée pour modifier des communications entre deux personnes ou plus.

A titre illustratif, les graphes ci-dessous répertorient d'un côté les typologies de sinistres enregistrés par l'assureur Hiscox en 2020, sur tous les territoires où il opère. De l'autre, un graphique des cyberattaques les plus courantes contre les entreprises françaises en 2020 relevées par « Statistica » et leurs conséquences[10]



Le graphique ci-contre présente les différentes typologies de sinistres répertoriés en 2020 par l'assureur Hiscox, qui souligne l'importance de la formation des employés puisque l'ingénierie sociale et la sécurité des employés arrivent en tête.

Ceci démontra que les hackers n'hésitent pas à utiliser les employés de l'entreprise pour parvenir à leurs fins.

Graphe I.A.2 – Cause des sinistres 2020 – Rapport Hiscox[11]

[9] Le paradoxe des anniversaires est utilisé en cryptographie pour élaborer des attaques sur les fonctions de hachage. Une des contraintes imposées sur ces fonctions, pour une utilisation cryptographique, est de produire peu de collisions, autrement dit, de rarement prendre la même valeur sur des entrées différentes.

[10] Graphique: Les cyberattaques les plus courantes contre les entreprises françaises | Statista

[11] Rapport_Hiscox_2020_sur_la_gestion_des_cyber_risques.pdf

Au-delà des typologies d'attaques perpétrées en 2020, les conséquence de ces dernières sont également mentionnées avec le vol de données et le deni de service en tête des principales conséquences. Sur ce graphique le rensomware n'arrive qu'en troisième position.

Graphe I.A.3 – Cyberattaques les plus courantes en 2020 contre les entreprises française

3. LES DOMMAGES CAUSES PAR UNE CYBERATTAQUE

Une cyberattaque peut causer une multitude de dommages à l'entreprise. Par exemple :

- Une perte de données ;
- Une dégradation de l'image de marque ;
- Un arrêt du système informatique entraînant un arrêt de l'activité ;
- La responsabilité de l'entreprise vis-à-vis des clients ou partenaires ;
- Une demande de rançon (ransomware).

Selon l'analyse d'Hiscox[12], les conséquences peuvent être dramatiques. Même si les dommages subis ne sont ni matériels, ni corporels, ils peuvent engendrer des frais importants : honoraires pour un expert, coûts pour rétablir la réputation de l'entreprise, perte d'exploitation, le paiement d'une rançon etc.

80% des entreprises ayant perdu leurs données informatiques dans une cyberattaque ont fait faillite dans les 12 mois. L'activité peut en effet se trouver complètement paralysée et l'entreprise aura alors pour objectif de reprendre son activité et de rétablir son image.

Ainsi et nous détaillons ci-dessous les différentes conséquences possibles.

[12] 21486 - Hiscox Cyber Readiness Report 2021 - France.pdf

a. Une perte de chiffre d'affaires

La première conséquence d'une attaque cyber, c'est bien évidemment la conséquence financière. Une attaque cyber entraîne souvent un arrêt ou une perturbation de l'activité de l'entreprise, une indisponibilité de son site web et par conséquent un manque à gagner important.

La perte d'exploitation est la conséquence la plus redoutée par les entreprises, notamment pour les PME et les TPE. Pour rappel, l'entreprise française Saint-Gobain a estimé à **250 millions d'euros** les dommages causés sur son chiffre d'affaires de l'année 2017 par l'attaque cyber du ransomware NotPetya.
Ainsi, dans le cas de lourdes pertes de données comme un fichier client indispensable à l'entreprise, l'activité est alors suspendue et le chiffre d'affaires baisse donc considérablement.

Plus la paralysie de l'activité se prolonge, et plus l'entreprise risque des retards de livraison engendrés également par une augmentation de la charge de travail pouvant aller jusqu'au dépôt de bilan.

Si le coût précis d'une attaque cyber est toujours difficile à quantifier tant l'exercice reste délicat, l'impact sur le chiffre d'affaires n'est plus à prouver et menace les entreprises les plus vulnérables d'un arrêt complet de leurs activités.

b. Une atteinte à l'image de marque de l'entreprise

Une attaque cyber entraînant un vol de données n'a pas que des conséquences financières. En effet, la deuxième conséquence la plus fréquente d'une fuite de donnée : le renvoi d'une mauvaise image de l'entreprise ainsi qu'une baisse de confiance de la part de ses clients. Lorsque les données personnelles des clients sont dérobées, vendues ou exposées publiquement, ces derniers peuvent se montrer réticents à poursuivre une collaboration et se détourner de l'entreprise.

Il en est de même pour les marchés publics qui mettront à l'écart les entreprises victimes d'un vol de données, jugées moins dignes de confiance.

Par ailleurs, avec la mise en place du RGPD en mai 2018, il est désormais obligatoire de notifier aux autorités les fuites de données subies, ainsi que d'en informer ses clients lorsque les données sont jugées sensibles (coordonnées personnelles, n° de carte bancaire, etc.), sous peine de lourdes sanctions. Il est donc indispensable de mettre en place immédiatement un plan de communication de crise efficace.

c. Des coûts de restauration importants

Remettre en route un système infecté, reconstituer les données perdues, remobiliser ses employés après une attaque… Tout cela prend du temps, et coûte de l'argent alors même que l'activité est parfois encore à l'arrêt. Prévoir **un plan de restauration** est alors indispensable pour réagir au plus vite à une attaque et relancer son activité.

Dans certains cas les hackers peuvent demander une rançon pour récupérer les données volées (**ransomware**), mais rien ne garantit la récupération de ces données cryptées ou volées, et pourra exposer l'entreprise au chantage.

d. Des frais juridiques conséquents

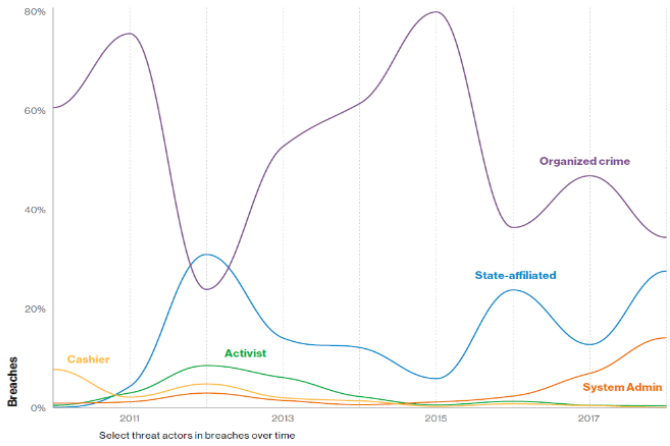
En cas d'attaque ou de piratage des systèmes informatiques ayant permis aux hackers de s'introduire dans ceux des clients ou partenaires par exemple, ces derniers sont en droit d'exiger des dommages et intérêts, notamment dans les cas de perte, extorsion ou détournement de données, d'utilisation frauduleuse d'informations stratégiques, de violation d'accords de confidentialité, d'usurpation d'identité etc.

Plus les conséquences de l'attaque sont lourdes et plus des frais juridiques s'avèreront élevés.

4. QUELQUES EXEMPLES D'INCIDENTS AYANT CONDUIT A DES SINISTRES CYBER

a. Les sinistres d'envergure survenus depuis 10 ans

De nombreux sinistres d'envergure liés à des attaques cyber ont vu le jour depuis une dizaine d'années. Certains, de par leur ampleur et leur étendue géographique ont fait la une des médias. Le plus ancien de ces sinistres est le sinistre **STUXNET** survenu en 2010 et attribué à l'état d'Israël contre le programme nucléaire iranien. L'implication d'Etats dans les sinistres cyber prouve l'étendue possible que peuvent prendre ces types d'attaques. Leurs conséquences s'apparentent dans ces cas à des « guerres informatiques ».



Le graphe présenté et issu du rapport Verizon de 2019 illustre l'activité des Etats et présente les profils des différents attaquants ainsi que l'évolution des violations commises.

Graphe I.A.4 – la répartition du risque Cyber en risque criminel et risque non criminel

Le tableau de l'annexe B donne une description des 10 sinistres les plus importants de l'histoire[13].

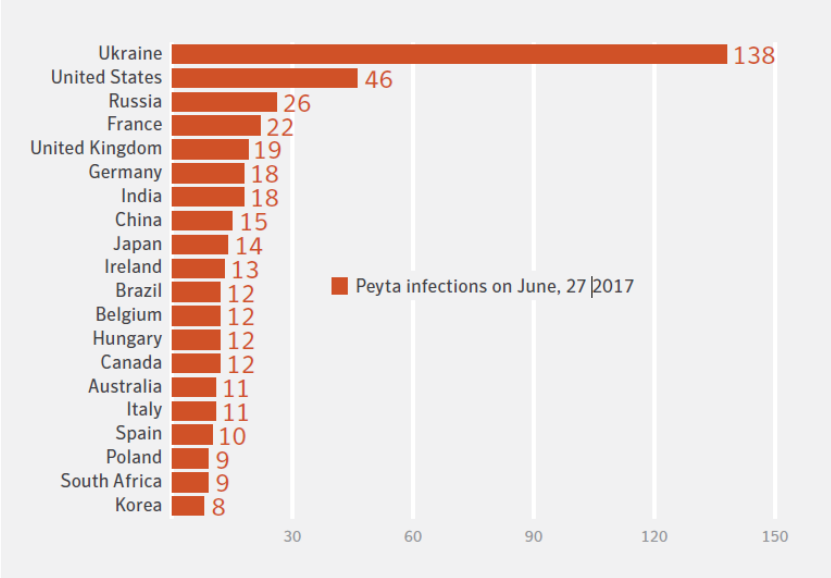
[13] Les 8 plus importantes cyberattaques de l'Histoire, de Stuxnet à Solarwinds (businessinsider.fr)

b. Le cyber, risque systémique ?

Les sinistres **Not Petya** et **Wannnacry** survenus en 2017 et expliquent d'une certaine façon pourquoi le risque cyber peut être qualifié de « systémique ».

En effet, NotPetya est une cyberattaque qui a touché plusieurs pays d'Europe de l'Est (principalement l'Ukraine). Ce virus est un logiciel de type Wiper, c'est-à-dire qui détruit les données du système infecté (malgré une demande de rançon trompeuse). L'objectif de ce virus est donc de provoquer des interruptions d'activité (BI) chez les entreprises infectées.

L'Ukraine est le pays le plus touché par cette attaque puisqu'elle concentre 60% des systèmes endommagés[14].



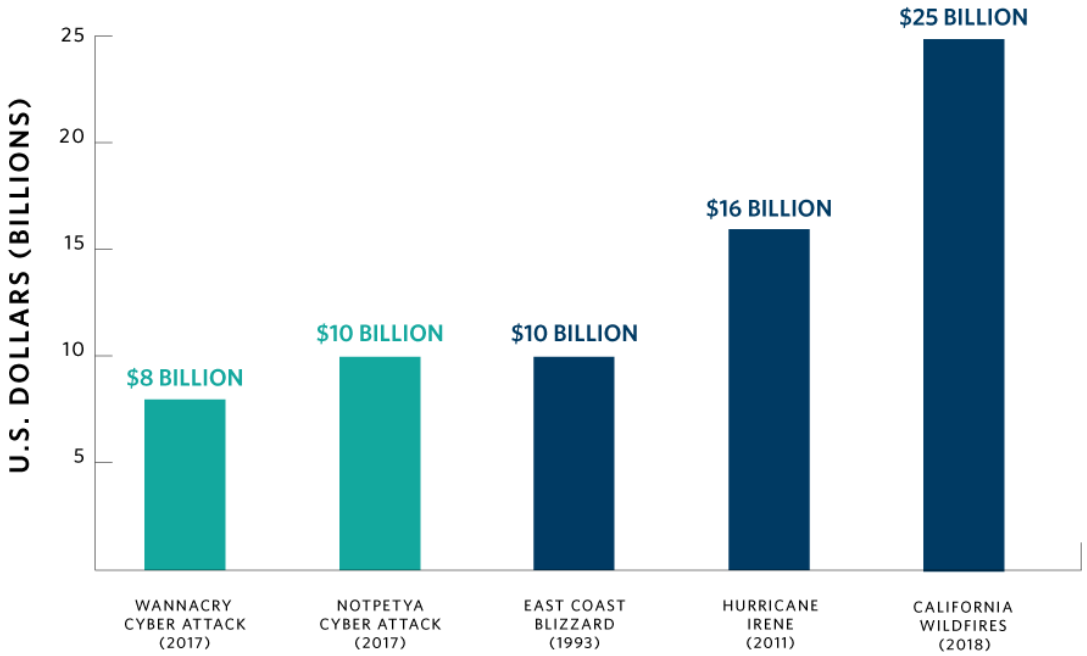
Graphe I.A.5 – Virus Not Petya par pays

Les pertes estimées sont très importantes pour de nombreuses grandes entreprises comme par exemple :

- L'entreprise de matériaux française Saint-Gobain a estimé 250 millions d'euros de pertes.
- L'entreprise de transport maritime par containers, Maersk a estimé 200 millions de dollars de pertes tandis que l'entreprise pharmaceutique Merck a estimé 300 millions de dollars de pertes.

Ces quelques chiffres illustrent l'impact que peut avoir une cyberattaque sur les entreprises et les pays. Le coût de ces attaques a par ailleurs été comparé à quelques événements majeurs survenus aux Etats-Unis suite à des catastrophes naturelles, corroborant le caractère systémique d'un événement cyber.

[14] Rapport tactique NotPetya (menshaway.blogspot.com)



SOURCES: Luke Gallin, "Re/insurance to Take Minimal Share of $8 Billion WannaCry Economic Loss: A.M. Best," Reinsurance News, May 23, 2017, https://www.reinsurancene.ws/reinsurance-take-minimal-share-8-billion-wannacry-economic-loss-m-best/; PCS, "Could NotPetya's Tail Be Growing?," 2019, https://www.verisk.com/siteassets/media/pcs/pcs-cyber-catastrophe-notpetyas-tail.pdf; and National Oceanic and Atmospheric Administration, "Billion-Dollar Weather and Climate Disasters: Events," 2020, https://www.ncdc.noaa.gov/billions/events.

NOTE: The cost of these U.S. disasters is calculated in 2020 dollars.

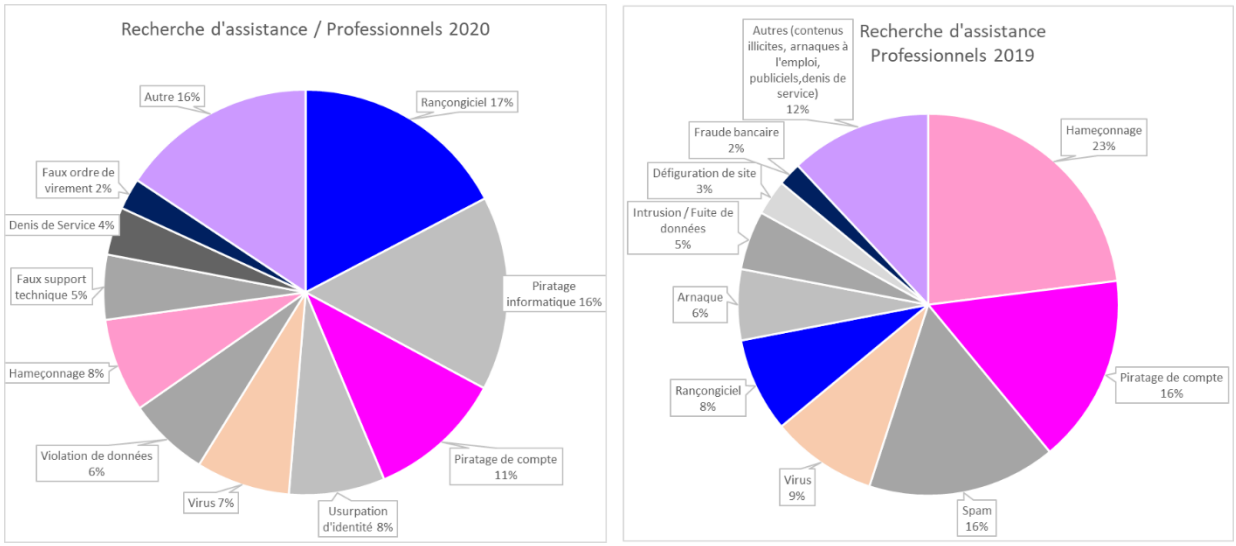
Graphe I.A.6 – Comparaison des coûts de Not Petya et Wanacry par rapport aux sinistres événements naturels US

c. L'explosion des ransomwares avec le COVID 19

La pandémie de COVID 2019, a offert un terrain favorable aux hackers qui ont profité de la crise du fait du développement du télétravail, du commerce électronique et du numérique. Les hackers ont redoublé d'efforts pour lancer pas moins de 5 millions d'attaques au cours du premier semestre 2020. Les rançongiciels ont explosés et sont devenus la menace informatique qui pèse aujourd'hui le plus sur les entreprises et les institutions.

Ainsi depuis 2019, les experts observent une augmentation de la moyenne des paiements de rançon effectués par les grandes entreprises. Les attaques ciblées impliquent principalement du chantage, pour forcer les victimes à payer la rançon. Par exemple, les pirates menacent de stopper les systèmes d'information et les opérations de l'entreprise et de divulguer publiquement les données - données personnelles, données sensibles, données de carte de crédit etc.

Le site cybermalvaillance[15] du gouvernement dont l'objectif est d'assister, d'informer et d'aider les particuliers, entreprises, associations, collectivités et administrations à se protéger en cas de cybermalveillance, a réalisé deux études sur les typologies d'attaques. Ces deux études ont été menées en juin 2019 et en décembre 2020 et recensent selon les différentes catégories d'acteurs et selon la répartition des menaces, les différentes recherches d'assistance. Pour les professionnels (entreprises et collectivités territoriales), nous pouvons noter une évolution des types de menaces, selon les graphiques ci-dessous.



Graphe I.A.7 – Augmentation de la part de rançongiciels entre 2019 et 2020

Par ailleurs, afin de bien comprendre l'évolution des typologies de sinistres liés à des attaques cyber, le tableau de l'annexe C recense, les 10 sinistres les plus importants de 2020. Le développement des sinistres ransomwares s'accentue de façon notable puisque 5 attaques sur 10 sont liées à ce type de menaces.

5. LA REGLEMENTATION

a. Les organismes en charge de la cybersécurité nationale et européenne.

Dès 2006, face à la menace cyber grandissante, la France a publié le décret n°2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale en décrivant le dispositif d'**Opérateurs d'importance vitale** (OIV), codifié en 2007 dans le Code de la Défense.

Une OIV est une organisation identifiée par l'État comme ayant des activités indispensables à la survie de la nation ou dangereuses pour la population et qui exploitent ou utilisent des installations jugées indispensables à la survie de la Nation.

[15] Assistance aux victimes de cybermalveillance

L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) est créée en 2009 (JO du 8 juillet) sous la forme d'un service à compétence nationale est chargée des questions de cyber sécurité. Il s'agit d'une organisation gouvernementale française rattachée au secrétaire général de la défense et de la sécurité nationale (SGDSN), ce dernier étant chargé de conseiller le Premier ministre dans l'exercice de ses fonctions en matière de défense et de sécurité nationale.

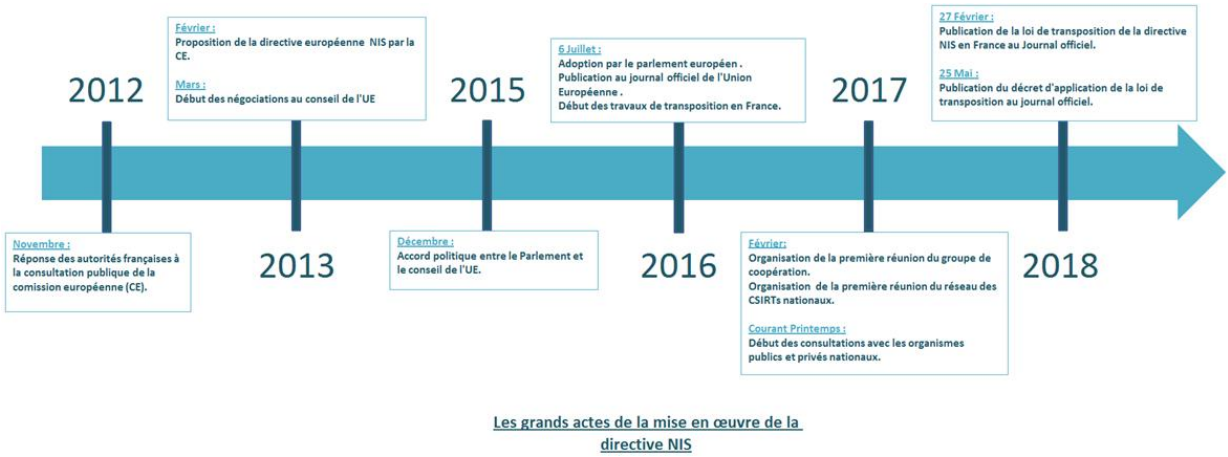
L'ANSSI se voit confier la mission de renforcer de la sécurité des OIV, pour lesquelles au nom du premier ministre, elle pourrait imposer des mesures de sécurité et des contrôles de leurs systèmes d'informations plus critiques.

De son côté l'Union Européenne et les Etats membres se sont organisés pour une meilleure stratégie à adopter contre le risque cyber. En mars 2019, le parlement européen approuve le *Cybersecurity Act* (parution au Journal Officiel de l'Union Européenne le 7 juin 2019). Ce dernier renforce l'Agence européenne pour la cybersécurité (ENISA) et établit un cadre européen de certifications des produits et services de cybersécurité.

b. Les Directives Européennes

i. La Directive NIS

Dans le cadre de la stratégie de renforcement de la cybersécurité dans l'ensemble de l'Union Européenne, la Commission européenne a adopté en Juillet 2016, la directive NIS (**Network and Information System Security**) sur la sécurité des réseaux et de l'information (voir UE 2016/1148).



Graphe I.A.8 – Les étapes de la mise en place de la Directive NIS

Premier texte de loi important à l'échelle de l'Union Européenne sur la cybersécurité, la directive NIS a été transposée en droits nationaux en Mai 2018. En France, cette transposition s'est faite sous l'égide de l'ANSSI qui, forte de son expérience sur les OIV, a capitalisé sur la méthodologie appliquée pour mener les travaux concernant les **opérateurs de services essentiels** au fonctionnement de l'économie et de la société (OSE).

Ces organismes sont majoritairement des grandes entreprises ou des entreprises de taille intermédiaire ainsi que des opérateurs du secteur public (principalement des établissements publics), tributaires des systèmes d'information et dont un arrêt du service aurait un impact disruptif et important pour le fonctionnement de l'économie et la société. Les Etats membres ont dû fournir une liste d'OSE pour le 9 novembre 2018.

Les objectifs de la directive NIS sont les suivants (article 11 de la directive NIS) :

- Le renforcement des capacités nationales des Etats membres ;
- Une meilleure coopération entre les Etats membres ;
- L'instauration d'un cadre réglementaire pour les Opérateurs de Services Essentiels au fonctionnement de l'Economie **(OSE)** ;
- Et pour les Fournisseurs de Services Numériques **(FSN)**

Concrètement les Opérateurs de Services Essentiels et les Fournisseurs de Services Numériques devront garantir un socle minimal de cybersécurité pour se protéger d'une attaque aux conséquences majeures sur le fonctionnement de l'économie et de la société. Ils devront donc suivre certaines règles de sécurité.

ii. Le RGPD

Depuis mai 2018, le nouveau régime juridique en matière de **protection de données (RGPD)** élargit le champ des obligations et de la responsabilité des entreprises. Il prévoit une obligation de notification étendue à toutes les entreprises ayant des activités de traitement de données, tandis qu'auparavant seuls les opérateurs d'importance vitale étaient tenus de notifier les pertes de données. De surcroît, les informations à communiquer dans les notifications ont changées. Désormais, une notification doit comporter : le nombre d'utilisateurs touchés, la durée de l'incident, la portée géographique, la gravité de la perturbation et l'ampleur de l'impact sur les fonctions économiques et sociétales.

Les notifications impliquent donc des expertises qui engendrent des coûts supplémentaires. Ceux-ci s'ajoutent aux coûts relatifs aux mises à jour et mises en conformité des systèmes d'exploitation suite à l'attaque numérique.

Autre implication importante de ces nouvelles obligations de notification, la responsabilité de l'entreprise détenant les données est directement exposée auprès de victimes. Les conséquences pécuniaires liées à la responsabilité juridique de l'entreprise risquent donc de croître dans les prochaines années.

Ce nouveau cadre juridique alourdit donc le coût des attaques et incite les acteurs économiques à transférer ces coûts aux assurances.

B. LES CAPTIVES

1. PREAMBULE

L'objectif de ce mémoire n'est pas de donner les avantages et inconvénients propres à chaque domicile favorable à l'établissement de captives. Ainsi, toute problématique concernant la fiscalité est exclue et les captives sont étudiées d'un point de vue de la GESTION DES RISQUES uniquement.

De plus, seules les captives domiciliées au sein de l'Union Européenne - plutôt que dans une zone Offshore comme les Iles Caïmans, les Bermudes, Guernesey…, rentrent dans le champ de cette étude, de sorte que la réglementation Solvabilité 2 soit applicable.

Seul le risque de souscription du risque cyber est étudié, à l'exclusion d'un éventuel risque opérationnel auquel serait soumis la captive.

Appliquer le modèle développé aux captives (petites compagnies d'assurance ou de réassurance adossées à des Groupes industriels, commerciaux, bancaires etc) permet d'obtenir une vision globale de l'impact de cette modélisation en fonction de la stratégie déjà mise en place par les entreprises, concernant la gestion de leur risque cyber.

2. DEFINITIONS

Selon la Directive 2005/68/CE du Parlement Européen et du Conseil de l'Europe une captive est une société d'assurance (ou de réassurance) appartenant à un groupe industriel, commercial ou de service dont l'activité principale n'est pas l'assurance ou la réassurance.

Une captive constitue un mécanisme formalisé qui permet au groupe propriétaire de s'auto-assurer. Elle prend souvent la forme d'une filiale d'assurance agréée et régulée dans un endroit (domicile) :

- Où la réglementation l'autorise
- Où un réseau de prestataires local spécifique est établi.

La compagnie mère capitalise et contrôle la captive dans le respect du droit du pays d'accueil, les décisions sont prises au cours des Conseils d'administration qui se tiennent dans le domicile. Il définit également direction opérationnelle de la captive, mais la gestion quotidienne est généralement sous-traitée dans le domicile à des prestataires de services spécialisés dans l'activité de gestion de captives.

Le choix de la forme sociale de la captive, qu'il s'agisse d'assurance ou de réassurance, se porte généralement sur une société anonyme.

3. LES TYPES DE CAPTIVES

La **captive d'assurance** (ou captive directe) est une véritable société d'assurance. A ce titre, elle est habilitée à émettre directement des polices d'assurance et à recevoir directement des primes auprès du groupe et de ses filiales opérationnelles, ainsi qu'à indemniser directement ses assurés des sinistres couverts. En fonction du plan d'activités qui aura été défini, la captive directe peut céder tout ou partie des risques souscrits au marché de la réassurance.

Contrairement à la captive directe, la **captive de réassurance** ne peut émettre des polices ni recevoir des primes directement. Elle doit donc faire appel à un assureur tiers, dit « assureur cédant » ou « fronteur », qui se charge de l'émission des polices et de l'encaissement des primes correspondantes, avant de céder les risques à la captive de réassurance. La cédante sera également responsable du règlement des sinistres couverts dont elle collecte le paiement auprès de la captive. En contrepartie de son intervention, le « fronteur » reçoit une commission de fronting payée par la captive et demande généralement des garanties ou collatéraux, susceptibles de revêtir différentes formes (lettres de garanties, nantissement de titres ou d'espèces, …). La captive de réassurance peut également à son tour recéder tout ou partie des risques souscrits au marché de la réassurance (mécanisme de la « rétrocession »).

La gestion de la captive – qu'elle soit d'assurance ou de réassurance – est généralement confiée à une société de gestion, ce qui permet au « sponsor » (l'actionnaire fondateur) de se décharger des activités administratives et comptables afférentes.

Le schéma ci-dessous permet une vision synthétique du mode de fonctionnement de chacun des deux types de structures

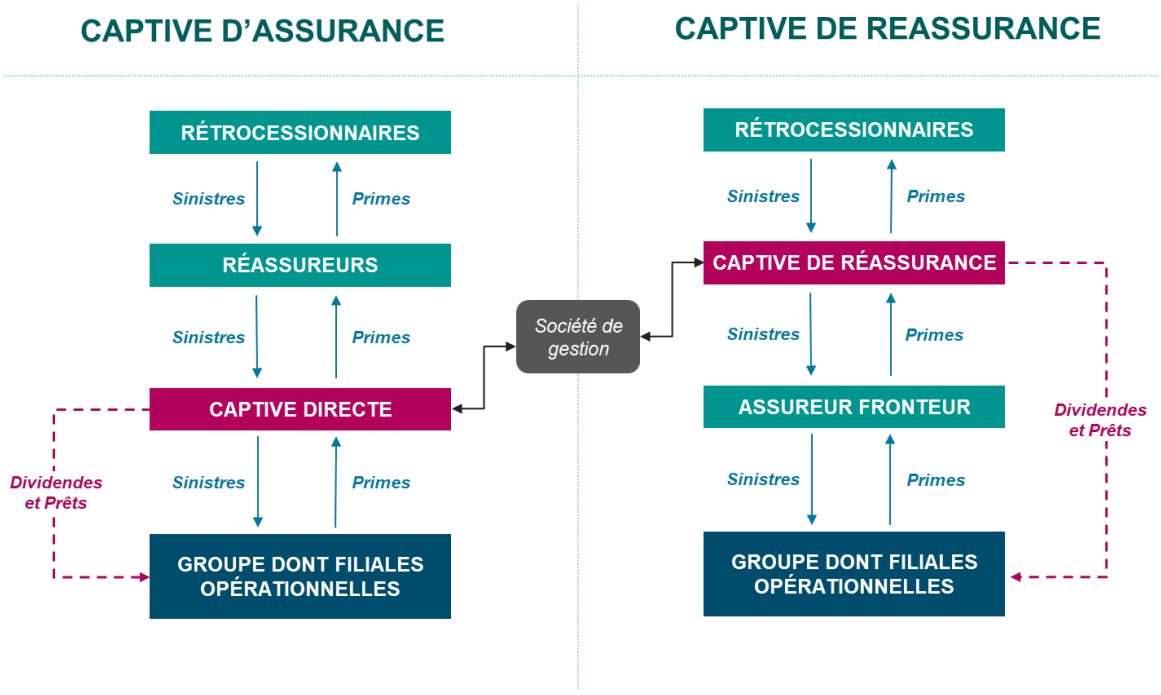


Schéma I.B.1 – Schémas des flux pour une captive d'assurance et une captive de réassurance

4. LA CAPTIVE, UN OUTIL DE GESTION DES RISQUES

a. Les avantages de la captive

La captive est avant tout un outil de *Risk Management*, intégré dans la politique de gestion des risques du groupe, dont les principaux atouts peuvent être résumés comme suit :

- **Optimisation de la rétention des risques**, en adéquation avec les seuils de tolérance financière des entités du groupe. La captive permet en effet aux filiales opérationnelles de bénéficier de franchises basses tout en aménageant une rétention au niveau du groupe lui permettant de bénéficier de conditions de transfert plus favorables sur le marché d'assurance.

- **Solution de couverture pour des risques non assurables** (ou insuffisamment assurés) ou couverts à des coûts prohibitifs par les assureurs traditionnels (ces solutions restent limitées par les moyens financiers alloués par le groupe à la captive)**.**

- **Compréhension et contrôle des risques.** La captive permet de renforcer le contrôle de l'ensemble des programmes d'assurance de l'entreprise, via la centralisation et l'harmonisation des couvertures au sein d'un programme cohérent, qui favorise également la prévention, l'évaluation des risques et la mise en place d'un système de remontée d'information efficace.

- **Stabilisation et/ou réduction du coût de la gestion des risques à moyen / long terme.** Le recours à une captive offre une plus grande capacité d'arbitrage vis-à-vis des offres des assureurs, permettant de moduler de manière réactive la rétention de l'entreprise et de ses filiales au rythme des cycles de marché. Ainsi, les réserves constituées au fil du temps au sein de la captive constituent un « matelas », susceptible d'amortir les variations subies sur le marché : évolutions tarifaires, restrictions de capacités, changements de périmètre, …

- **Constitution de réserves pour le financement d'un sinistre majeur potentiel**

Au-delà des gains en autonomie et flexibilité du groupe fondateur, la mise en place d'une captive autorise également une gestion différente des risques qui présente un certain nombre d'avantages plus strictement financiers :

- **La conservation des profits de souscription et produits financiers** attachés aux flux de primes transitant par la captive permet d'accroître in fine le niveau d'intervention tout en réduisant et en stabilisant le coût total du risque dans le temps **;**

- A contrario d'une gestion par simple provisionnement comptable dans le cadre de son activité traditionnelle, l'entreprise, grâce à la captive, peut bénéficier de mécanismes de dotation de provisions propres à l'exercice de l'activité d'assurance/réassurance. Ces mécanismes peuvent permettre, suivant le domicile choisi, un traitement fiscal avantageux (tels que par exemple la possibilité de provisionner en différé d'impôts sur plusieurs années, et de disposer ainsi d'un matelas financier permettant de faire face à une sinistralité adverse)**.**

b. Les contraintes de la captive

En contrepartie de ces éléments, la société captive génère un certain nombre de contraintes inhérentes au caractère réglementé de l'activité d'assurance / réassurance, et à la gestion d'une entité juridique à part entière. Les principales contraintes et coûts afférents portent principalement sur :

- Les frais de création et de gestion
- L'obligation de reporting dans le respect de règles comptables, elles-mêmes en constante évolution, puisque se pose actuellement la question du reporting des captives sous la norme IFRS 17. Effectivement, depuis le 1er janvier 2005, les groupes cotés de l'UE doivent préparer leurs comptes suivant les normes IFRS, ce qui oblige très souvent à avoir deux jeux de comptes au niveau de la captive, l'un en conformité avec les règles comptables locales, et l'autre établi selon les normes IFRS.
- Les contraintes relatives à la sortie d'un montage captif, généralement soumise à l'approbation des autorités de contrôle en matière d'assurance, et par conséquent la non-disponibilité immédiate des réserves accumulées dans la captive.
- Le risque de perte due à une sinistralité adverse. A cet égard, l'étude de faisabilité réalisée en amont de la mise en place de la captive est primordiale car elle permet de définir les niveaux de rétention maximum au sein de la captive en fonction du seuil de tolérance de l'entreprise et d'organiser le cas échéant sa protection via des cessions adaptées auprès du marché de la réassurance.
- La conformité à la Directive Européenne Solvabilité 2 et aux différentes actions du projet BEPS (Base Erosion Profit Shifting), notamment la nécessité de justifier le niveau des primes facturées par la captive, par des approches techniques (évaluation actuarielle) et la prise en compte des prix de marché. Ces deux contraintes sont décrites plus en détail dans le paragraphe suivant

c. Les réglementations principales

i. Solvabilité 2

Qu'elles soient d'assurance ou de réassurance, les captives sont soumises aux mêmes contraintes réglementaires qu'un assureur ou réassureur « classique » d'un point de vue des exigences quantitatives, qualitatives, de transparence et de communication.

Certaines domiciliations permettent aux captives de bénéficier du principe de proportionnalité notamment en termes de gouvernance, mais ce n'est pas l'objet de ce mémoire.

Se pliant à la notion d'immédiateté introduite par Solvabilité 2, elles doivent déployer les mêmes moyens pour se conformer au pilier 1 tout comme au pilier 2.

Les captives se doivent donc de répondre à des exigences de fonds propres, à des contraintes d'optimisation du capital et de diversification des risques, donc de réaliser les calculs de SCR / MCR / Capitaux Eligibles etc … (Pilier 1).

Elles doivent également définir leur profil, la nature et la qualité des risques souscrits. Elles doivent formaliser une gouvernance d'entreprise. Dans ce cadre, elles sont tenues de produire un rapport de fonction actuarielle chaque année et de réaliser un exercice ORSA (Pilier 2) de façon à déterminer leurs risques propres et tester des scénarios de stress sur leurs portefeuilles.

Elles doivent également se conformer aux exigences de reporting (pilier 3) comme les QRT, les SFCR annuels, les RSR etc.

ii. BEPS, Base Erosion Profit Shifting

Lancée en 2014, le projet BEPS (Base Erosion and Profit Shifting) a pour objectif de s'attaquer aux stratégies de planification fiscale abusive qui exploitent les failles et les différences dans les règles fiscales nationales et internationales.

Dans ce cadre, un ensemble de recommandations (basé sur 15 actions) a été proposé par l'Organisation de Coopération et de Développement Economiques (OCDE) dans le cadre du Projet OCDE/G20 pour une approche internationale coordonnée de la lutte contre l'évasion fiscale de la part des entreprises multinationales.

Les captives, longtemps perçues comme un potentiel outil d'optimisation fiscale, peuvent faire l'objet d'un examen plus approfondi pour prouver que l'activité qu'elles entreprennent est proportionnelle au risque qu'elles assument et au rendement qui leur est attribué

Les Sociétés détenant des captives doivent être prêtes à démontrer leur alignement aux principes BEPS de transparence et de substance économique sous risque de devoir faire face à des dommages potentiels à la réputation et à des pénalités financières.

Le schéma ci-dessous présente les 15 actions proposées par l'OCDE. Les actions concernant l'économie numérique (Action 1) et celle en rapport avec l'élaboration d'un instrument multilatéral visant à contraindre les Etats à modifier leurs conventions bilatérales (Action 15), sont transversales.

Les 13 autres sont réparties selon 3 piliers :

- **La cohérence** : Les actions couvertes par ce pilier s'attachent principalement à s'assurer que le manque de coordination internationale ne soit pas utilisé à des fins abusives par les entreprises qui pourraient profiter des phénomènes de double non-impositions ou déductions liés à ces actions.

- **La substance** : Ce pilier contient des mesures visant à contrer les instruments juridiques qui permettent de faire transiter des revenus dans d'autres pays afin de bénéficier d'une imposition plus légère.

- **La transparence** : Les actions de ce pilier sont mises en place dans le but de faciliter la détection et le contrôle des mesures dommageables en imposant des obligations et des divulgations obligatoires pour les entreprises.

Les captives sont principalement soumises aux recommandations de transparence et de substance avec un objectif précis de conformité des prix de transfert (actions 8 à 10) des assurances souscrites par la captive, au prix du marché selon le principe de saine concurrence.

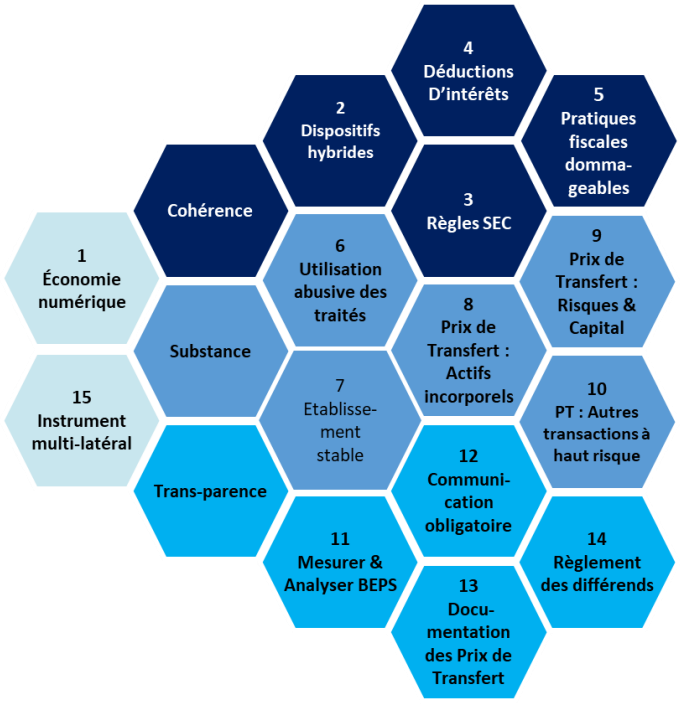
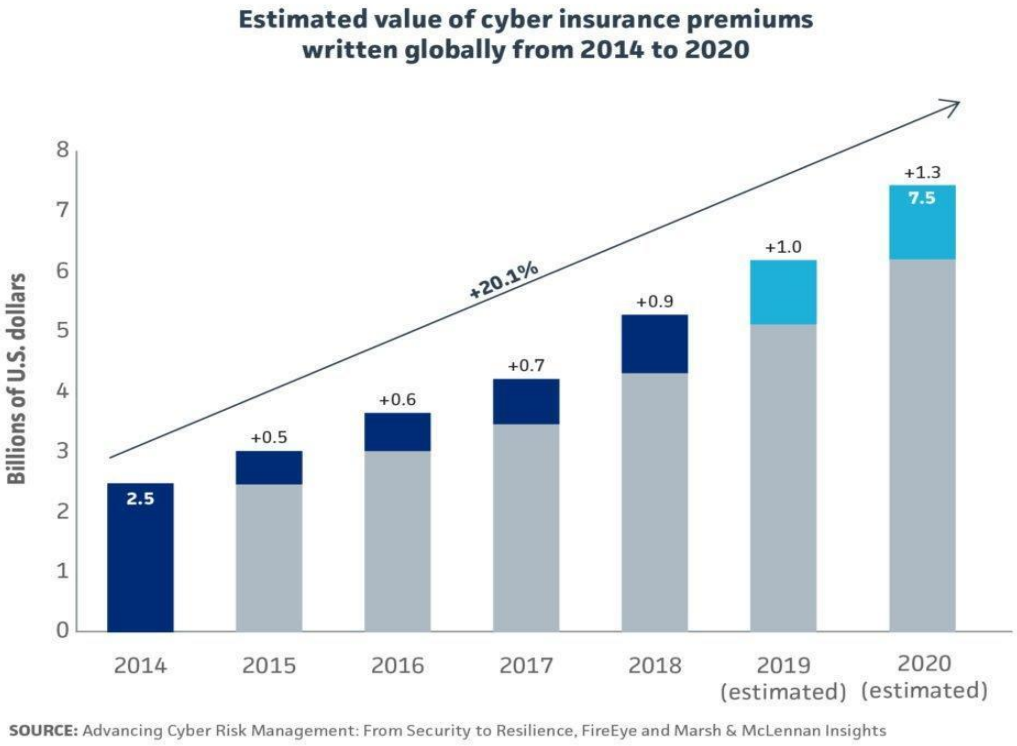


Schéma I.B.2 – Schémas des flux pour une captive d'assurance et une captive de réassurance

C. L'ASSURANCE CYBER

1. LA PRIME D'ASSURANCE ET LA NOTION DE CYBER « SILENCIEUX »

Si la valeur des primes d'assurance cyber ne cesse d'augmenter chaque année, celle-ci ne représente que 0.2% des primes d'assurance Non-Vie sur le marché mondial en 2017 (4.3 miliards de dollars contre 2 234,4).



Graphe I.C.1 – Les évolutions et estimations des primes d'assurance cyber

Pour 2020, la prime cyber mondiale, estimée à 7,5 millards de dollars en 2018 a finalement atteint 7,8 millards de dollars et est estimée à augmenter jusqu'à 20,4 milliards de dollars en 2025 selon Research and market du 27 octobre 2020.

Pourtant les assureurs semblent toujours réticents à développer la cyber-assurance, un marché pourtant en pleine croissance. Ce phénomène est accentué depuis le COVID 19 et l'explosion constatée des ransomwares, qui sont de plus en plus exclus des polices dédiées.

Trouver de la capacité sur les tranches basses des programmes des entreprises devient presque impossible, d'où le rôle grandissant que peuvent avoir les captives pour porter ce risque.

Les raisons pour lesquelles les assureurs ne sont pas « friands » del'assurance cyber sont multiples.

- Tout d'abord, si les sinistres annuels globaux liés au risque cyber sont négligeables du point de vue du bilan des assureurs pour l'instant, c'est la peur d'une méga-attaque ayant un impact

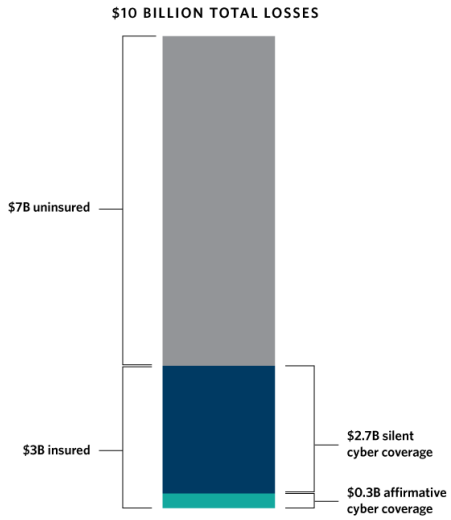
systémique qui les effraie. Effectivement, l'exposition des marchés financiers à ce type de risque expose directement les économies nationales et mondiales.

- De plus, la loi des grands nombre prédit, sous l'hypothèse de non-corrélation des sinistres entre-eux, que l'indemnisation moyenne par assuré est constante. Cependant, les sinistres cyber sont trop corrélés par l'interdépendance des systèmes et acteurs financiers ou bien la suprématie de certains systèmes d'exploitation (Microsoft/Windows), rendant ainsi les prévisions plus difficiles.

La forte corrélation des sinistres complique la stratégie de diversificaton des assureurs et le risque de cumul, menaçant ainsi leur solvabilité. De plus, cette corrélation entre un grand nombre de risques rend la quantification et la définition de la prime d'assurance peu fiables.

De plus, les assureurs ne disposent pas de suffisamment de données statistiques, et donc de recul. Il n'existe donc pas méthodologie pour classer les risques cyber. En outre, les sévérités ne sont pas liées au type de d'attaque, pouvant être intangibles : c'est le cas des dommages à la réputation.

L'exemple de Not Petya est encore une fois révélateur et permet d'introduire la notion de cyber « silencieux ».



Si le sinistre au global a été estimé à 10 milliards de dollars[16],

- seuls 3 milliards ont fait l'objet d'une indemnisation par l'assurance
- dont 2,7 milliards au titre de couvertures silencieuses

Ainsi les compagnies d'assurance n'ont jamais collecté de primes sur la part des couvertures qui ont permis l'indemnisation des 2,7 milliards de dollars.

Graphe I.C.2 – Décomposition du sinistre Not Petya

[16] https://carnegieendowment.org/2020/10/05/war-terrorism-and-catastrophe-in-cyber-insurance-understanding-and-reforming-exclusions-pub-82819

2. LES CONTRATS D'ASSURANCE TRADITIONNELS ET LE CYBER « SILENCIEUX »

Certaines polices d'assurance traditionnelles couvrent une partie des sinistres causés par une attaque cyber :

- **Contrats dommage aux biens :** couvre les conséquences matérielles de l'attaque cyber, qu'elle soit due à une erreur humaine ou à un acte malveillant. Si l'attaque ne provoque pas de dommages matériels, les pertes d'exploitation ne sont pas couvertes.

  A titre d'exemple, ce type d'assurance a couvert l'explosion d'un pipeline de BTC Turquie en Août 2008 : les attaquants avaient pris le contrôle du système d'exploitation et ont déréglé les calculs de pressions, provoquant ainsi une explosion.

- **Contrats responsabilité civile (RC) :** couvre les dommages causés aux Tiers de type corporel, matériel ou immatériel, à la suite d'une attaque malveillante et/ou une erreur humaine.

  Ce type de contrat intervient principalement pour couvrir le risque cyber dans le cas d'un vol de données ou d'une atteinte aux données qui constitue un dommage aux tiers car affectant leur vie privée (dommage immatériel) ou encore la transmission d'un virus dirigé contre l'assuré à des tiers (dommage matériel et/ou immatériel consécutif ou non). Cependant, les garanties des contrats classiques de RC ne s'appliquent pas toujours dans le cas cyber (dépend des exclusions).

- **Contrats Directors and Officers Liability (D&O) :** couvre la responsabilité des dirigeants si leur responsabilité est retenue à la suite d'une attaque cyber.

  C'est le cas, par exemple, si les dirigeants n'ont pas pris suffisamment pris en compte le risque cyber ou bien n'ont pas investi raisonnablement dans les systèmes de cybersécurité connaissant leur risque.

- **Contrats Fraude :** couvre les dommages causés par les fraudes, notamment celles perpétrées par avec un ordinateur.

3. LES CONTRATS D'ASSURANCE DEDIES AU RISQUE CYBER

Les polices spécifiques de cyber assurance sont apparues notamment parce que les polices d'assurance traditionnelles n'apportent qu'une réponse partielle au cyber risque, ne couvrant que la responsabilité civile ou les dommages ou n'en couvrant pas les conséquences immatérielles ou de manière sous-limitée.

Ainsi le contrat d'assurance cyber est une couverture en « périls dénommés », il prend en charge uniquement les risques qui sont explicitement définis en excluant tout le reste.

Généralement une police d'assurance cyber dispose de plusieurs volets pour appréhender ses typologies spécifiques ainsi que ses conséquences propres.

Dans une assurance cyber figure deux types de garanties et notamment des garanties « assurantielles »

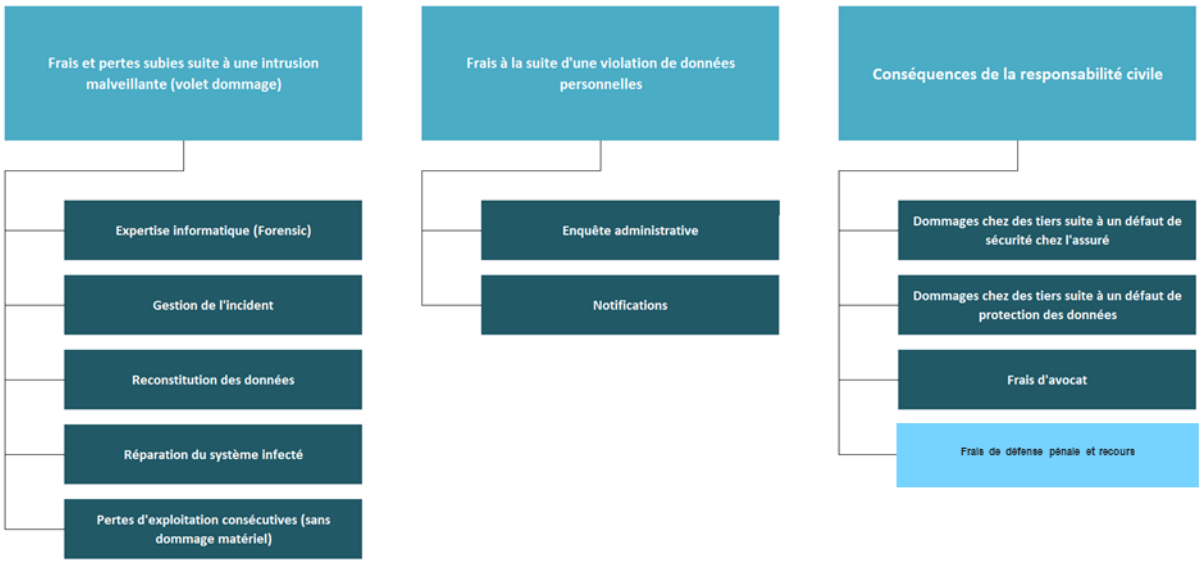
1. Les dommages subis par les assurés comprenant notamment les pertes de revenus suite au sinistre et éventuellement les frais de cyber extorsion qui s'avèrent être optionnels
2. Les dommages subis par les tiers à savoir les conséquences pécuniaires et frais de défense résultant de toute réclamation de tiers pour atteinte à la sécurité du réseau ou du système d'information et/ou aux données.

Par ailleurs, les polices d'assurance cyber bénéficient d'un volet comprenant des prestations de « gestion de crise et d'assistance », qui représentent un atout certain en complément des assurances traditionnelles. Ce volet va permettre d'activer des **garanties d'assistance en urgence**, car la rapidité de traitement en cas d'une attaque cyber représente un facteur important de diminution de la charge du sinistre.

Les prestations d'assistance conclues avec des prestataires de services informatiques, juridiques, de relations publiques et de communication sont mises à disposition de l'assuré. Elles vont permettre de prendre en charge rapidement les éléments ci-dessous :

- Frais de recherche de la cause du sinistre et du rétablissement du système d'information
- Frais de communication et de relations publiques, de restauration des données et de notification.
- *Frais de monitoring* lorsque les données bancaires sont impliquées

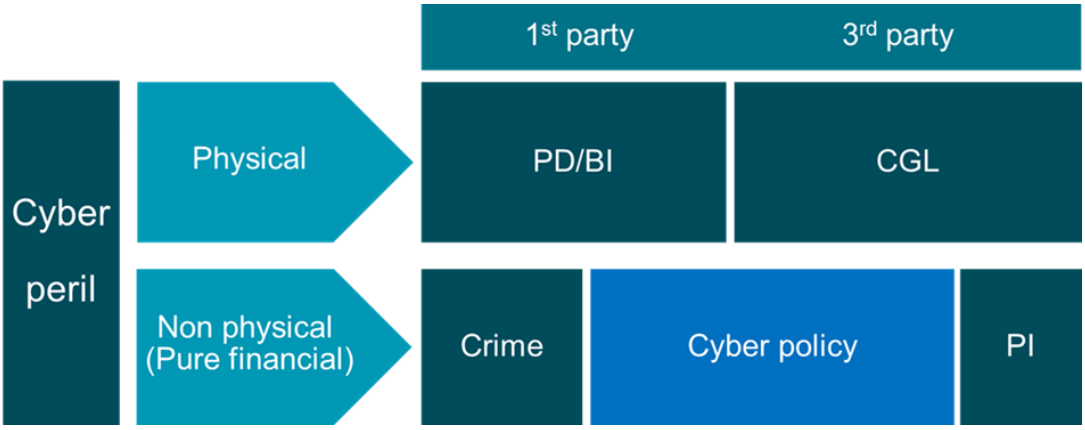
La figure ci-dessous représente l'ensemble des garanties assurantielles et des prestations complémentaires intégrées dans les polices d'assurance dédiées.



Graphe I.C.3 – MARSH – Garanties et prestations complémentaires d'une police d'assurance cyber dédiée

A RETENIR …

Les polices d'assurance traditionnelles peuvent être utilisées par les entreprises lorsqu'elles subissent une cyberattaque. Cependant ces contrats n'apportent pas de prestations de gestion de crise adaptées au risque cyber, ni d'intermédiaire spécialisé. De plus, lors de la tarification de ces contrats, le risque cyber n'a généralement pas été considéré. En conséquence ces polices ne sont pas adaptées à ce risque.



Graphe I.C.4 – MARSH - Couverture du risque cyber selon les types de périls et de garantie

PARTIE II – CARACTERISATION DU RISQUE CYBER

A. LES DONNEES

1. LE RAPPORT CYENCE ET LA MESURE DU CYENCE SCORE

Cyence est un fournisseur tiers, expert en sécurité numérique, en assurance et en modélisation économique qui a trouvé un moyen de quantifier les facteurs qui influencent le comportement des acteurs de la menace.

Grâce à sa capacité d'analyse de données volumineuses (big data) l'outil Cyence mesure le cyber-risque comme un problème de comportement humain, et pas uniquement comme une technologie.

Cyence fournit une mesure de l'environnement de cybermenaces d'une entreprise en tenant compte des facteurs ci-dessous :

- **Les adversaires actifs** : Le comportement et les caractéristiques des « mauvais acteurs intelligents » qui lancent des cyberattaques contre une organisation doivent être pris en compte.
- **La volatilité des risques** : La modélisation traditionnelle des risques va utiliser les événements passés pour projeter l'avenir. Dans le cyberespace, les événements passés ne peuvent pas à eux seuls, constituer une base suffisante du fait du paysage dynamique et en constante évolution des menaces.
- **Les limites des données** : Les événements cyber sont fréquents, mais ne sont pas souvent publiés, ce qui rend difficile l'obtention de données détaillées sur les facteurs de risque potentiels.

L'outil Cyence permet en outre d'agréger divers indicateurs de menaces prédictives à l'aide d'un regard extérieur non invasif.

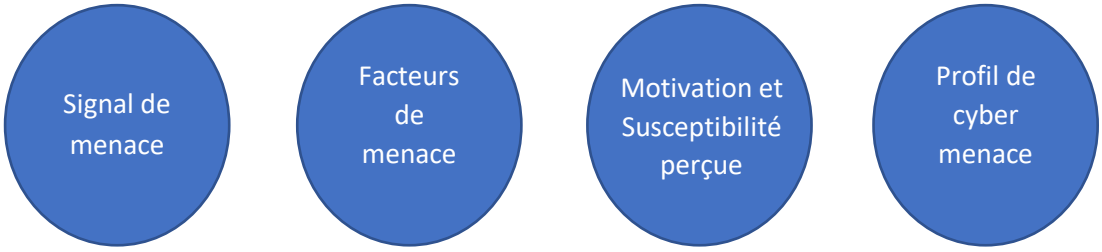


Figure II.A.1 – Les indicateurs du modèle Cyence

Ces indicateurs de menace peuvent être de nature technique (comme l'activité de botnet ou l'hébergement de sites Web) ou non techniques (comme le sentiment des consommateurs public ou la position concurrentielle de l'organisation au sein de l'industrie).

Les indicateurs techniques de menace fournissent une « mesure » de la sécurité apparente des systèmes d'une entreprise par rapport à ses pairs en examinant les vulnérabilités visibles de l'extérieur, les menaces, les activités des mauvais acteurs et l'analyse de l'infrastructure. Les indicateurs de menace non techniques comprennent les signaux liés aux personnes, aux processus, aux politiques, aux contrôles, à la formation, aux titres de compétences et à la préparation.

Le modèle analyse de nombreuses sources de données pour chaque organisation, qui fournissent individuellement des indices auxiliaires sur l'entreprise, mais lorsqu'elles sont considérées dans leur ensemble, elles fournissent des indications sur la maturité et la résilience relatives à la posture (attitude) de cybersécurité d'une entreprise.

Les nombreux indicateurs sont rassemblés dans huit catégories de menaces (dark web, organisation interne, impact externe, mauvaise activité, technologie, périmètre de sécurité et incidents récents).

L'annexe D détaille la définition des huit catégories de menaces prises en compte dans l'analyse.

LE CYENCE SCORE, L'INDICATEUR DE MOTIVATION ET SUSCEPTIBILITE

Cyence synthétise les milliers de sources de données rassemblées en une seule mesure du risque de cybermenace pour une entreprise donnée et attribue une note faisant état de la menace cyber qui pèse sur l'entreprise, le **Cyence Score.**

Ce score fournit des informations sur la motivation qu'un acteur de la menace peut avoir à cibler une entreprise et la susceptibilité perçue d'une entreprise à se défendre contre une attaque.

La motivation mesure le côté offensif des cybermenaces. Les pirates informatiques criminels, les employés malhonnêtes et les employés négligents sont à l'origine de la majorité des violations de la confidentialité des données.

La susceptibilité perçue mesure la posture de l'entreprise au regard de sa cybersécurité apparente à travers la technologie qu'elle utilise, ses employés et les processus mis en place.

Le graphe ci-dessous illustre le principe utilisé pour déterminer le Cyence score. Il se base sur le parallèle avec cambrioleur à l'affût d'une maison à dévaliser. Il analyse

- La motivation qu'aurait le cambrioleur à choisir telle ou telle maison et
- La perception qu'il a de l'environnement susceptible de contribuer à la réussite de son larcin

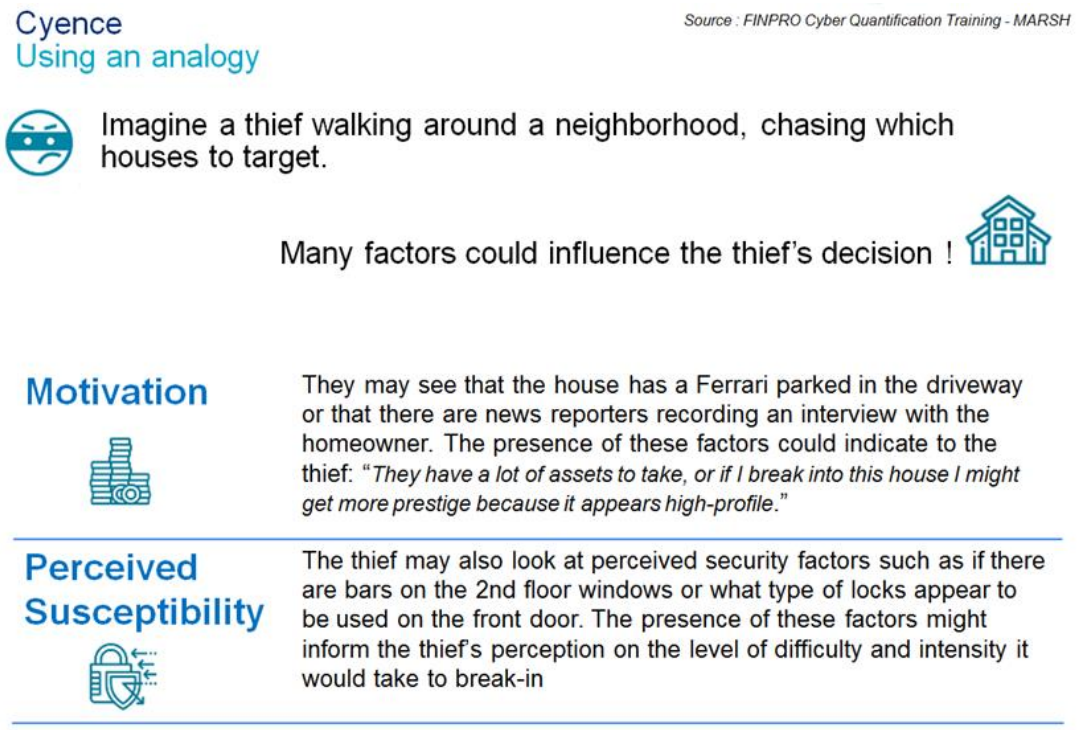
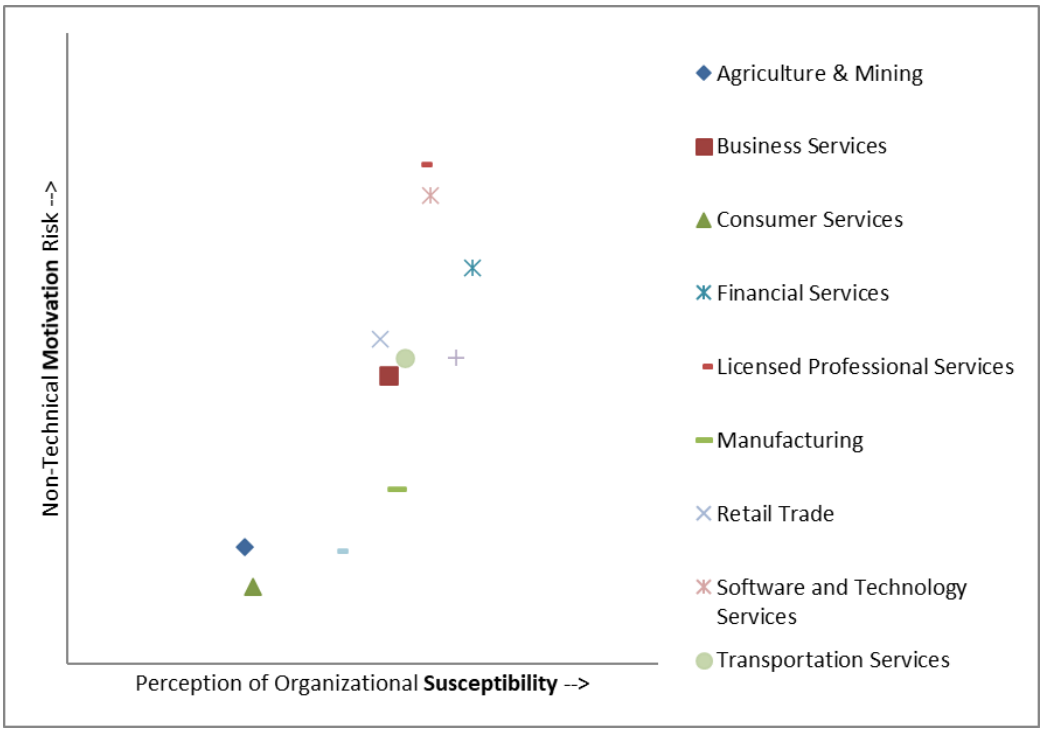


Figure II.A.2 – Concept utilisé par l'outil Cyence

Cyence se positionne comme « un miroir » à une organisation pour voir comment elle peut être vue par les attaquants potentiels, et traduire les connaissances en une meilleure compréhension de la façon de hiérarchiser de manière proactive les préoccupations du marché de l'assurance.



Graphe II.A.3 – Motivation et Susceptibilité par secteur d'activité

2. LES GENERATEURS DE SCENARIOS

Les générateurs de scénarios ont été développés par Marsh afin de modéliser et d'analyser l'exposition au risque cyber de ses clients, et leur permettre d'estimer l'impact financier d'une cyberattaque.

a. L'Exposition à la perte d'exploitation – Ideal BI

Ce générateur quantifie la perte de revenus (perte d'exploitation) qu'une entreprise pourrait subir à la suite d'événements cyber.

- Il modélise l'impact des interruptions d'activité basée sur l'approche données.
- Il simule une gamme de scénarios critiques avec plusieurs niveaux graduels de conséquences de mise à l'arrêt de l'entreprise.
- Il permet de garder une visibilité sur la durée totale de l'événement et de déterminer l'impact sur les revenus.

Le générateur de Perte d'exploitation combine des flux de données sur des données cybernétiques quantitatives spécifiques à l'industrie avec un étalonnage spécifique à l'entreprise. Ces données vont concerner les menaces, les contrôles et la résilience mais également des données plus traditionnelles comme le chiffre d'affaires, le nombre d'employés et le secteur d'activité.

Les données concernant les menaces et les tendances au niveau de l'industrie proviennent de sources externes comme VERISON et Advisen.

L'étalonnage spécifique à l'entreprise est réalisé, pour cette étude, à l'aide de :

- Cyence Score qui apporte une vue améliorée des vecteurs de menace pour le système d'information de l'entreprise considérée.
- Commentaires spécifiques à l'entreprise sur ses opérations, ses paramètres financiers et ses pratiques de résilience vis-à-vis des cyber événements.

Afin de construire une distribution de scénarios fréquence et intensité, 4 types d'incidents recensés entre 2014 et 2017 sont considérés dans le modèle.

- Les piratages (hacker)
- Les logiciels malveillants (malware)
- Les rançongiciels (Ransom / Extorsion)
- Les fraudes internes (Rogue employee)

Chacune de ces typologies d'attaques est étudiée en fonction de 3 niveaux de gravité, ce qui conduit à la construction de 12 scénarios.

L'analyse de ces scénarios va permettre d'estimer la répartition du temps de chacune des étapes de la violation : détection, panne, récupération et phase de restauration prolongée.

Enfin, les scénarios vont être générés selon 3 hypothèses de perte d'exploitation possibles selon le pourcentage de chiffre d'affaires affecté par l'incident

- Hypothèse 1 : 90 % du chiffre d'affaires affecté par l'événement cyber – Autrement dit, si une telle hypothèse se produisait, le client serait en mesure de maintenir jusqu'à 10 % de ses opérations génératrices de revenus, et ce grâce à des opérations manuelles ou à d'autres facteurs atténuants
- Hypothèse 2 : 50 % du chiffre d'affaires affecté par un événement cyber.
- Hypothèse 3 : 10 % du chiffre d'affaires affecté par un événement cyber.

b. L'Exposition au Vol de données – Ideal Privacy

Ce générateur va produire des scénarios susceptibles de donner une estimation de la perte liée à un événement cyber (fréquence et sévérité) relative à une violation de données personnelles.

Cette approche est basée sur un benchmark de réclamation qui a été construit selon le secteur d'activités par observation de données qui proviennent de différentes sources comme :

- Les bases de données cyber des clients de Marsh
- "Privacy Rights Clearinghouse Chronology of Data Breaches",
- "Advisen MSCAd Large Loss Database".

Les données requises sur lesquelles se basent les scénarios sont :

- Les **PCI** : Données bancaires relative aux cartes de paiement (information d'authentification comme le nom, l'adresse, numéro de téléphone, question de sécurité, …°.

- Les **PHI** : Données sensibles, notamment les données de santé protégées (prestation de soins de santé, paiement des soins de santé pouvant être associé à une personne en particulier. Ceci inclut toute ou partie du dossier médical ou de l'historique de paiement d'un patient mais également le nom, le numéro de téléphone, le nom de l'employeur et des membres de la famille, le numéro de sécurité sociale, les informations concernant la mutuelle etc).

- Les **PII** : Informations Personnellement Identifiables. Les données personnelles font référence aux informations qui peuvent être utilisées pour caractériser ou retrouver l'identité d'une personne, telles que son nom, son numéro de sécurité sociale, ses dossiers biométriques, etc., seules, ou lorsqu'elles sont combinées avec d'autres informations personnelles ou d'identification qui sont liées ou liées à une personne spécifique, telles que la date et le lieu de naissance, le nom de jeune fille de la mère, etc.

La probabilité de survenance d'un événement cyber dans les 12 mois à venir – La fréquence de ce type d'événements dépend du secteur d'activité, du chiffre d'affaires de l'entreprise, des incidents passés et du niveau de sécurité mis en place dans l'entreprise (Cyence Score).

La sévérité est fonction du type de données que possède l'entreprise (PII, PCI et/ou PHI) ainsi que du nombre de ces données. Elle est mesurée en considérant deux types de coûts :

- Des coûts liés aux dommages subis par l'entreprise (*First Party*), comme

  Les coûts d'enquêtes judiciaires, les coûts relatifs au centre d'appel, à la notification sur la confidentialité, au contrôle des crédits).

- Des coûts liés aux dommages subis par des tiers (*Third Party*), tels que les frais de litige, mais aussi pour les **PHI** notamment, les actions éventuelles auprès du régulateur. Pour les données sur les cartes de paiement (PCI), les coûts liés aux fraudes sur les cartes bancaires, à la réémission des cartes bancaires ou encore à la vérification des réseaux de cartes de paiement.

Ces concepts de coûts de « *First party* » et « *Third party* » seront particulièrement utiles lors de l'estimation de l'exposition et le calcul des primes pour la quantification du risque cyber silencieux.

A RETENIR …

Les deux générateurs de scénarios ainsi que le rapport Cyence utilisent les données financières des entreprises tel que le chiffre d'affaires et le nombre d'employés. Le secteur d'activité principal de l'entreprise est également un facteur commun aux trois modèles.

3. LES DONNEES PUBLIQUES SUR LES CAPTIVES – LES SFCR

Les SFCR (*Solvency and Financial Conditions Reports*) font partie des rapports narratifs exigés dans le cadre du pilier 3 du régime de Solvabilité 2. Ce **rapport sur la solvabilité et la situation financière** doit être publié tous les ans auprès du régulateur, mais il est aussi à destination du marché. Il s'agit d'un rapport public.

Au contraire du SFCR, l'autre rapport narratif, le RSR (Regular Supervisory Report), **rapport régulier au contrôleur** est à destination exclusive du régulateur.

Le SFCR et RSR ont le même plan, qui est donné dans l'annexe 20 du règlement délégué de la Commission européenne. En revanche le RSR, destiné au superviseur, est plus détaillé.

Le contenu du SFCR et du RSR est décrit dans les articles 290 à 298 (pour le SFCR) et 307 à 311 (pour le RSR) du règlement délégué. Les articles 299 à 303 (pour le SFCR) et 312 à 314 (pour le RSR) traitent des délais et modalités de communication. Ces dispositions sont complétées par des orientations de l'EIOPA (EIOPA-CP-14/047) qui couvrent le RSR et le SFCR.

Le SFCR *« s'inscrit dans un contexte croissant d'exigence, de transparence et de protection de la clientèle* [17] *»*. L'objectif est d'harmoniser la publication d'informations à l'échelle de l'Union Européenne Il s'organise autour de trois principes :

- Les publications comptable, réglementaire et pour le superviseur doivent être cohérentes ;
- La publication d'information pour le régulateur européen doit être harmonisée à l'échelle de l'UE (le but ultime étant la création d'un fichier européen à remplir par les entreprises) ;
- Les mêmes règles doivent s'appliquer à tous les assureurs et aux captives.

Le SFCR doit comporter les éléments suivants :

- Présentation de l'activité et les résultats en décrivant les performances techniques et financières de l'entreprise d'assurance ou de réassurance.
- Information sur le système de gouvernance en particulier sur leur système de gestion des risques et leur gestion des fonctions clés.
- Identification sur le profil de risque et en particulier des risques inhérents à l'activité de l'entreprise (souscription, crédit, marché …)
- Valorisation à des fins de solvabilité des actifs, des provisions techniques et autres passifs.
- Gestion du capital y compris la gestion des fonds propres économiques, du SCR du MCR et du ratio de couverture.

Les éléments sur l'activité communiquent des informations sur les activités souscrites par la captive (LoB) et les états des QRT en annexe, des éléments chiffrés sur les primes, les sinistres, les réserves, les Best Estimate et les calculs des différents modules et sous-modules des SCR.

[17] *Catherine Soulard, associée, responsable du pôle actuariat – Galéa et associés*

4. LE BENCHMARK DE SINISTRES

La société Advisen[18] a répertorié les sinistres survenus aux Etats-Unis depuis 2002 avec des montants conséquents de parfois plusieurs millions de dollars.

Parmi ces sinistres américains, les sinistres Target survenu en 2013 et Wells Fargo survenu en 2011, reportés dans le tableau ci-dessous, chacun avec un montant supériéur à 180 m€.

Les sinistres répertoriés par Advisen sont reportés ci-dessous en USD :

Année de Sinistre	Nom de la compagnie	Montant
2002	Choicepoint Inc	15 500 000
2005	Fifth Third Bancorp	655 000
2005	The Tjx Companies Inc	64 788 000
2009	Heartland Payment Systems Inc	63 761 192
2011	Wells Fargo & Co	185 000 000
2013	Facebook Inc	11 357 600
2013	Target Corp	181 009 948
2013	Yahoo Inc	50 334 000
2014	The Home Depot Inc	46 343 818
2015	The Wendy'S Co	50 000 000
2017	Equifax Limited	657 561
2017	Sonic Corp	4 325 000
2018	Facebook Inc	645 000

Figure II.A.4 – Répartition des sinistres majeurs américains depuis 2002

Les attaques malveillantes, dont le sinistre Target représentent la majorité des sinistres observés avec en 2013 un montant total de 231 m$ soit un tiers de la totalité des sinistres du tableau.

Le vol d'identité avec le sinistre Wells Fargo en 2011 pour un montant de 185 m$ constitue une autre cause de sinistre important.

Sur la zone Europe, un benchmark répertoriant des sinistres notifiés à Marsh par des clients ou prospects sont analysés.

Il permet de modéliser le risque à partir de l'historique de la statistique sinistre et de vérifier la pertinence de ce modèle sur les programmes des captives qui souscrivent du risque cyber.

[18] Cyber Loss Data - Advisen Ltd.

La base étudiée est composée de 209 sinistres survenus entre 2016 et 2019 et répartis de la façon suivante :

- 62 sinistres sont ouverts mais aucun montant n'est indiqué. Il parait donc difficile de tenir compte de ces sinistres dans la suite de l'analyse.

Année	Sinistres reportés	Ouvert sans évaluation	Pourcentage
2016	7	3	42,9%
2017	17	4	23,5%
2018	36	9	25,0%
2019	58	24	41,4%
2020	91	22	24,2%
Total sans évaluation	209	62	29,7%

Figure II.A.5 – Ouverts sans évaluation

Selon les années, nous constatons un nombre de sinistres « sans montant » relativement important avec une forte proportion pour l'année 2019.

Nous en déduisons que sur cette année 2019, il manque peut-être encore des estimations précises sur certains sinistres.

Quoi qu'il en soit, le nombre de sinistres « sans suite » semble non négligeable (autour de 30%).
Par ailleurs, l'année 2016 semble peu représentative.

- 89 sinistres sont ouverts avec une estimation d'évaluation. Nous prenons ces sinistres en compte dans nos analyses déterministes et stochastiques.

- 41 sinistres sont clos et sans suite. Nous les retirons de notre base statistique.

- 17 sinistres sont clos avec un montant non nul, nous les prenons en compte dans nos analyses déterministes et stochastiques.

La base se réduit donc à 106 sinistres répartis sur 5 ans.

a. Commentaires sur l'intensité

Les sinistres sont ensuite analysés selon les secteurs d'activités des entreprises qui ont subi les attaques. En effet, dans la suite de l'étude cette caractéristique est déterminante dans le calcul de la fréquence. Comme indiqué précédemment, les générateurs de scénarios utilisés pour modéliser les risques considèrent que la fréquence des attaques est dépendante, du secteur d'activité de l'entreprise ainsi que de sa taille.

	Institutions Financières	Industrie	Services	Services publics (Energie / Telecom)	Commerce	Global
Moyenne	392 884	235 513	1 112 811	203 460	209 807	449 786
Ecart type	961 115	449 302	4 353 889	545 190	222 833	2 100 356
25%	1 254	3 402	7 915	126	1 491	1 157
50%	73 374	50 001	22 033	44 165	109 862	50 001
75%	280 051	300 001	189 513	103 568	358 314	259 100
90%	1 195 364	570 814	614 000	358 377	542 813	549 108
99%	3 768 286	1 620 325	16 867 591	2 258 056	548 198	4 336 982
Montant total des sinistres	**9 429 208**	**4 003 718**	**25 594 654**	**5 289 960**	**3 776 526**	**47 677 313**

Figure II.A.6 – Sinistres par secteur retenu

Le montant total des sinistres par secteur varie entre 3,7 m€ et 25,6 m€. Cette différence est principalement due à un sinistre de 21 m€ sur une entreprise du secteur des « Services ».
Le sinistre moyen global s'élève quant à lui à 449k€ mais sans le sinistre de 21 m€, cette moyenne baisse à 284 k€.

Toujours en excluant le sinistre de 21 m€, nous déterminons avec le test de Student, l'intervalle de confiance à 95% des moyennes par secteur par rapport à la moyenne globale. Seule la moyenne estimée pour le secteur des Institutions Financières est plus importante que la borne supérieure. Cette constatation est corroborée par le test de Student pour les 90ème et 99ème percentile.

A l'inverse nous constatons que pour le secteur du « Commerce » (Trade), le 99ème percentile avec 548 k€ représente le secteur dont l'intensité de sinistres est la plus faible. Effectivement, les deux sinistres les plus importants pour ce secteur d'activités se situent tous les deux autour d'un montant de 548 k€.

b. Commentaires sur la Fréquence

Le graphe ci-dessous montre une évolution du nombre de sinistres selon les années et les secteurs d'activités.
Quel que soit le secteur d'activités, la fréquence depuis 2016 « explose » et est quasiment multipliée par 10 en 5 ans.

	Institutions Financières	Industrie	Services	Commerce	Service public
2 016	-	-	1	-	-
2 017	2	1	2	1	1
2 018	5	1	4	5	1
2 019	9	2	5	6	6
2 020	8	13	11	6	16
Total	**24**	**17**	**23**	**18**	**24**

Figure II.A.7 – Evolution du nombre de sinistre par secteur

Cette augmentation est à nuancer car le nombre de sinistres devrait être rapporté à la croissance du nombre de nouvelles affaires Cyber placées, qui a elle-même fortement augmenté. Cependant, nous n'avons pas d'indication concernant cette évolution du portefeuille.

POINT IMPORTANT SUR L'UTILISATION DU BENCHMARK …

La modélisation via le benchmark est utilisée dans la suite de cette étude pour comparer la tarification réalisée sur la base des scénarios avec celle réalisée sur la base du benchmark pour les captives qui souscrivent du risque cyber.

Pour les captives qui ne souscrivent pas du risque Cyber mais qui peuvent avoir des expositions silencieuses, le benchmark ne peut pas être utilisé car il ne donne pas d'information concernant la répartition du sinistre en risque « dommage » ou en risque « de tiers ».

Les sinistres provenant du benchmark des sinistres des sociétés européennes sont considérés sans distinction du secteur d'activité dans la tarification.

Les sinistres « Target » de 2013 et « Wells Fargo de 2011 » constitueront la référence des sinistres CAT événementiels avec des montants totaux avoisinant pour chacun d'eux 180 m USD

A noter que les captives souscrivent généralement des tranches basses (dites tranches travaillantes) sur les programmes des entreprises ; le maximum observé étant de 50 m€ de capacité.

B. ETUDE DE L'EXPOSITION AU RISQUE CYBER

Cette partie de l'étude est destinée à mesurer et analyser l'exposition des entreprises au risque Cyber en étudiant les scénarios obtenus par les générateurs. Dans un deuxième temps, nous décrirons comment ces derniers sont utilisés pour modéliser les programmes des captives afin de proposer un modèle de tarification pour le risque cyber.

Les résultats de la tarification réalisée à l'aide des scénarios seront également comparés à une tarification réalisée à l'aide d'un benchmark des sinistres cyber issu de la base de données (LDL) de Marsh.

Concernant l'application aux programmes portés par les captives, plusieurs cas seront étudiés :

- La captive souscrit déjà du risque cyber. Dans ce cas, nous vérifions si la tarification donnée par le modèle est en ligne avec la prime souscrite dans la captive. Pour rappel, la tarification du modèle est basée uniquement sur les expositions aux pertes d'exploitation et aux vols de données personnelles. D'autres types d'exposition ne sont pas prises en compte dans la tarification à partir des scénarios.

- La captive ne souscrit pas de risque cyber mais souscrit du risque dommage et/ou de la RC. Dans ce cas, les polices « Dommage » et/ou « RC » pourraient être appelées dans le cas d'un sinistre cyber. Les polices « Dommage » et/ou « RC » couvriraient du risque cyber silencieux. Nous examinerons la prime qu'il aurait fallu charger si de telles polices étaient activées.

- La captive souscrit des typologies de risques autres que le Cyber, le Dommage ou la RC. Dans ce cas, nous considérons que ces polices n'exposent pas la captive n'est pas exposée au risque cyber.

A noter que le risque cyber associé au risque opérationnel de la captive ne rentre pas dans l'objet de ce mémoire.

1. LA CONSTRUCTION DES SCENARIOS

Les générateurs de scénarios utilisés vont nous permettre d'obtenir deux types d'exposition :

- La première concerne la perte d'exploitation de l'entreprise à la suite d'une attaque Cyber. Elle est déterminée en utilisant les données suivantes :
    - Chiffre d'affaires, nombre d'employés, secteur d'activité mais également
    - Données d'incidents passés et le délai pendant lequel l'activité de l'entreprise a été interrompue.

- La deuxième concerne le vol et la perte des données personnelles, déterminée en utilisant les données suivantes :
    - Chiffre d'affaires, secteur d'activité
    - Nombre de données personnelles, données sensibles et données de cartes de crédit.

Ce générateur de scénarios va également permettre de faire la différence entre les expositions relatives aux dommages subis par l'entreprise elle-même (First party) et les expositions des tiers.

a. Hypothèses et Remarques préliminaires

Les deux générateurs de scénarios permettent de donner une estimation de la fréquence de survenance d'un sinistre et simulent une distribution de l'intensité des scénarios.

b. Scénarios de Perte d'Exploitation

i. Intensité / sévérité – calcul de la sévérité pour une fréquence donnée

Le générateur de scénarios de perte d'exploitation réalise des tirages aléatoires sur un loi uniforme de 0 à 1.
Tout tirage i différent de 0, est attribué à l'un des 12 scénarios définis dans le chapitre A.2.a (*L'exposition à la perte d'exploitation – Ideal BI*) selon la typologie de l'entreprise et sa sévérité correspondante. Le scénario retenu est noté S_i

ii. Fréquence – calcul de la fréquence d'une sévérité donnée

Le modèle réalise A=200 000 simulations pour déterminer ces scénarios S_i relatifs à la perte d'exploitation,

- Soit X_i = 1 quand le scénario simulé est différent de 0

$$N = \sum_{i=1}^{A} X_i$$

- La variable Xi est une variable de Bernoulli de paramètre p « scénario non nul » à savoir la proportion de scénarios non nul dans le nombre de scénarios total (A=200 000). On aura donc :

$$\mathbb{E}\,[N] = \sum_{1 \le i \le A} P(X_i = 1) = A*p$$

$$\mathbb{E}\,[\frac{N}{A}] = p = \frac{N}{200\,000}$$

Pour chaque entreprise, p correspond à la fréquence d'occurrence de scénarios non nuls dont l'intensité est définie par $S_{i\ (i=1\ à\ N)}$

c. Scénarios de Violation des données (vol ou perte)

i. Intensité / sévérité – calcul de la sévérité pour une fréquence donnée

Pour la sévérité, 10 000 simulations sont réalisées pour déterminer les scénarios de vol ou perte de données personnelles.

- Soit n le nombre de scénarios (n = 10 000) recueillis et,
- $I_{i\ (i=1\ à\ n)}$ l'intensité de chaque scénario pour le risque de pertes de données personnelles (PII),
- $H_{i\ (i=1\ à\ n)}$ l'intensité de chaque scénario pour le risque de pertes de données sensibles (PHI – données de santé),
- $C_{i\ (i=1\ à\ n)}$ l'intensité de chaque scénario pour le risque de pertes de données de Carte de crédit (PCI).

ii. Fréquence – calcul de la fréquence d'une sévérité donnée

La fréquence f est calculée de façon globale par le modèle.

Elle est dérivée de la probabilité d'avoir au moins une violation de données par an. Elle est déterminée en utilisant le chiffre d'affaires de l'entreprise, son secteur d'activité. Elle utilise également l'écart du « Cyence Score » de l'entreprise par rapport au « Cyence Score » de son secteur d'activités pondéré par le Chiffre d'affaires.

Une transformation par la fonction logistique permet de borner la probabilité de violation des données entre 0 et 1.

Cette fréquence f est ensuite répartie entre les trois types de données (PII, PCI et PHI) selon un pourcentage défini à dire d'expert et lié au type d'activité de l'entreprise.

A noter …
Des tests de convergence sont réalisées pour les deux générateurs de scénarios.

- Le générateur de perte d'exploitation converge pour 200 000 simulations. Les scénarios générés sont soit des scénarios nuls indiquant qu'il n'y a pas de perte d'exploitation, soit des scénarios non nuls.
- Le générateur de vol ou perte de données converge à 10 000 simulations, mais celui-ci ne produit que des scénarios non nuls.

Les deux générateurs de scénarios sont utilisés sur les données de 55 entreprises qui possèdent une captive afin de créer deux bases de données.

Parmi les 55 entreprises :

- 17 relèvent du secteur de la fabrication « Manufacturing »
- 1 relève du secteur minier « Agriculture & Mining » et pourra être affectée au secteur « Manufacturing » en cas de regroupement
- 9 relèvent du secteur des Services « Services »
- 7 sont des Institutions Financières « Financial Institution »

- 10 relèvent du secteur du Commerce « Trade »
- 11 sont des fournisseurs de services « Utilities »

2. PRESENTATIONS DES SCENARIOS SUR L'EXPOSITION AU RISQUE CYBER

Les résultats des analyses des expositions pour le secteur « Manufacturing » (fabrication) pour les données sensibles (PHI), les données personnelles (PII) et les données de carte de paiement (PCI) sont repris ci-dessous dans le but de présenter les expositions aux typologies de données pour un même secteur d'activité.

Par souci de clarté, les courbes construites pour les autres secteurs d'activité et pour les différents types de données sont reportées dans l'annexe E.

a. Exposition au Vol de Données

i. Intensité

Le générateur de scénarios donne le résultat pour les 3 types de vol de données PHI (données sensibles), PII (données personnelles) et PCI (données de cartes de crédit).

A noter que le nombre de données renseignées par catégorie doit être au minimum de 100 000.

Dans le cas de données comprises entre 50k et 100k pour l'une des catégories, le nombre de donnes est arrondi à 100k. Cette hypothèse est réalisée dans le but de tenir compte du type de données dans l'exposition.

EXPOSITION AUX DONNEES SENSIBLES (PHI)

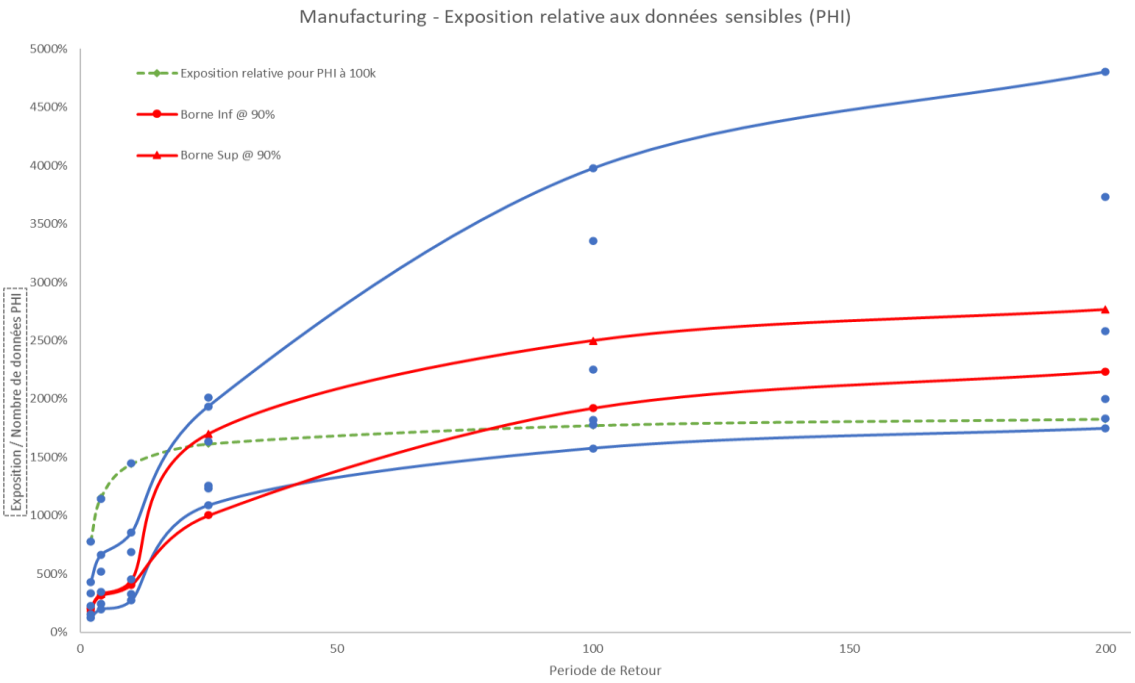
Le graphe ci-dessous représente la courbe de distribution des scénarios des entreprises recensées dans le secteur d'activité « Manufacturing » (fabrication) qui possèdent des données sensibles (PHI). Ces entreprises sont au nombre de 8 (sur 17) dans notre échantillon.

Les scénarios obtenus pour chacune des entreprises aux différentes périodes[19] de retour sont divisés par le nombre de données renseignées pour alimenter le générateur de scénarios. Cet indice ainsi calculé nous permet de comparer les entreprises entre elles.

Dans le graphe ci-dessous, les entreprises ont renseigné un nombre de données sensibles (PHI) qui varie entre 100 000 pour les entreprises les moins exposées à ce type de données et 641 000 pour celles qui sont le plus exposées aux données PHI.

Les entreprises qui évoluent dans ce secteur de la « fabrication » (Manufacturing) sont généralement peu exposées aux données sensibles PHI, qui correspondent plutôt à des données de santé. Ceci explique le manque de représentativité de ces entreprises pour ce type de données.

[19] La période de retour représente l'inverse du percentile et est associée à la fréquence d'un sinistre selon sa sévérité.



Graphe II.B.1 – Exposition des entreprises du secteur de la fabrication aux données sensibles

Ce graphique donne en première approximation une estimation de l'exposition au vol de données sensibles des entreprises du secteur de la fabrication.

Pour les faibles valeurs de périodes de retour (jusqu'à 1 sur 10 ans) les niveaux d'exposition sont équivalents quelle que soit la taille de l'entreprise.

La courbe verte représente les entreprises qui ont renseigné un nombre de données sensibles égal à 100 000 (minimum acceptable pour que le générateur produise des scénarios).

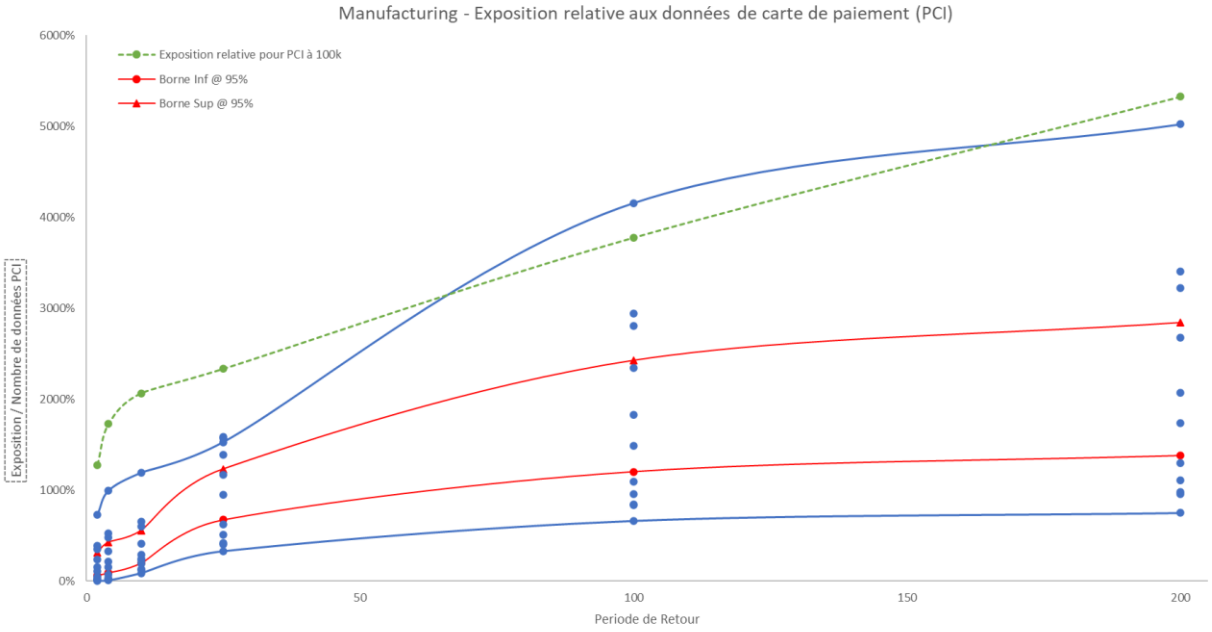
Dans l'estimation de l'intervalle de confiance, ces entreprises ont été retirées, ce qui réduit l'échantillon à 5 entreprises dont les données PHI se trouvent dans l'intervalle [184k ; 641k].

La construction des courbes et les intervalles de confiance ont été déterminées en appliquant le test de Student sur cet échantillon de 5 entreprises en supposant que la moyenne par période de retour suit une loi normale.

Ce test est décrit dans l'annexe F.

EXPOSITION AUX DONNEES DE CARTES DE PAIEMENT (PCI)

Concernant les données de carte de paiement, la même courbe est construite. Dans ce cas, 11 entreprises sur 17 du secteur « Manufacturing » sont concernées et le nombre de PCI renseignées varient de 100 000 à plus de 20 millions de données pour l'une d'entre elle.

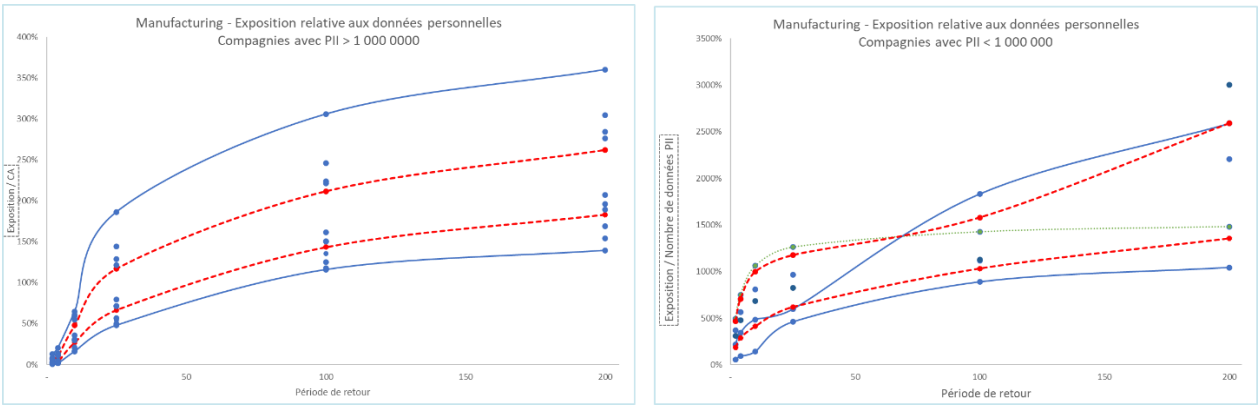


Graphe II.B.2 – Exposition des entreprises du secteur de la fabrication aux données de cartes de paiement

La courbe verte représente les entreprises qui ont renseigné un nombre de données de cartes de paiement égal à 100 000 (minimum acceptable pour que le générateur produise des scénarios).

Cette courbe indique que l'exposition relative aux cartes de paiement est plus élevée que celle obtenue pour les données sensibles puisque pour une période de retour de 200 ans l'exposition atteint 5000% des données renseignées (soit 5 m€ d'exposition) contre environ 1800% pour les PHI.

EXPOSITION AUX DONNEES PERSONNELLES (PII)



Graphe II.B.3 – Exposition des entreprises du secteur de la fabrication aux données personnelles

Toutes les entreprises ont renseigné des données personnelles. Cependant, l'intervalle est très large puisqu'il commence aux 100 000 minimum pour se terminer à près de 60 millions. L'exposition qui en découle varie elle de 1,5 m€ à près de 81 m€.

L'exposition relative est très disparate pour les entreprises qui ont renseigné moins de 1m de données personnelles et celles qui ont renseigné plus d'un million de données.

Afin de faciliter la lecture, deux courbes sont construites.

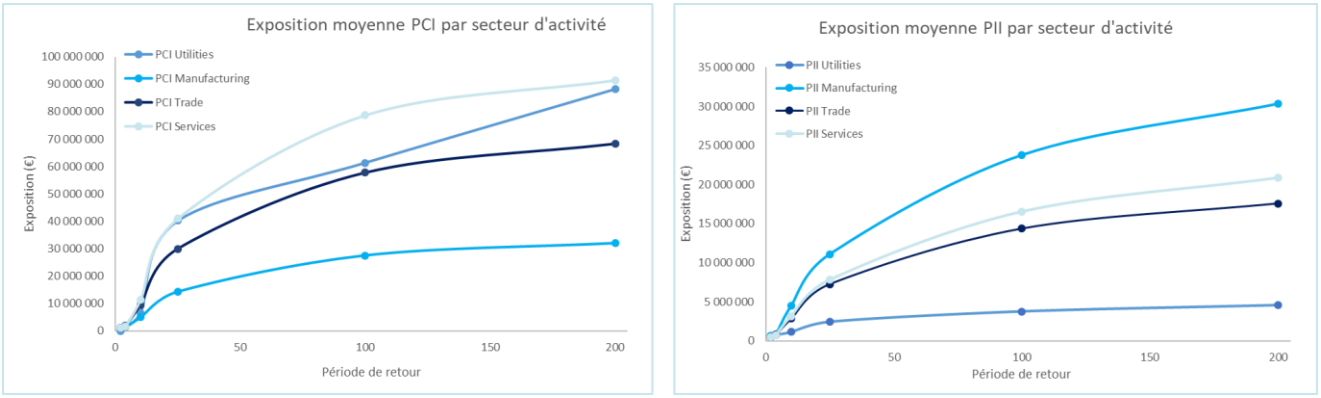
POINTS A RETENIR CONCERNANT L'INTENSITE DES EXPOSITIONS AUX DONNEES …

L'exposition aux données personnelles et aux données de cartes de paiement sont globalement de même niveau moyen. Pour une période de retour de 200 ans, la moyenne se situe autour de 30 m€ et il en est de même pour les autres périodes de retour considérées.

Cependant, l'exposition aux cartes de paiement représente l'exposition la plus importante avec des niveaux pouvant atteindre plus de 150 m€ sur notre échantillon. Cette conclusion corrobore la description réalisée dans le paragraphe (II.A.2.b) qui décrit le générateur de scénarios de vol ou perte de données. En effet, lors du vol ou de la perte de données, il existe des coûts supplémentaires subis par des tiers (fraudes sur les cartes bancaires, réémission de ces cartes, vérification des réseaux de paiement etc.).

Pour conclure, le graphe ci-dessous décrit les moyennes obtenues par secteur d'activité sur l'échantillon de 55 entreprises pour les données personnelles et les données relatives aux cartes de paiement.

L'exposition aux données sensibles n'est pas représentée car de façon logique, peu d'entreprises ont renseigné ce type de données pour les différents secteurs d'activités.



Graphe II.B.4 – Expositions issues du générateur de perte ou vol de données par secteur d'activité

ii. Fréquence

Le graphe ci-dessous représente les fréquences du vol de données comprenant les 3 composantes PII, PCI et PHI.

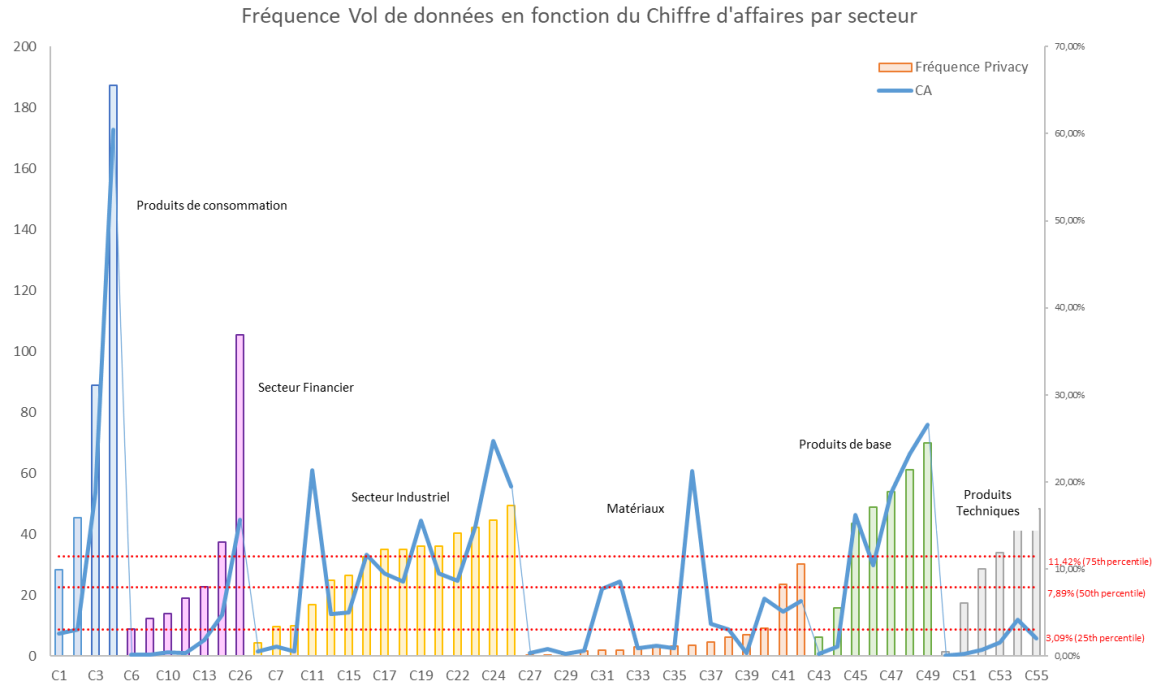
Les secteurs d'activités sont répartis en 6 catégories qui semblent être liées à la nature du produit ou du service fourni.

Les fréquences sont très différentes puisque notre intervalle varie entre 0,1% à 65,54%.

Une régression linéaire est réalisée avec le logiciel R et confirme que les facteurs principaux de détermination de la fréquence sont le **chiffre d'affaires** et les **incidents passés**. Ce résultat est présenté en annexe G.

Pour notre échantillon, la fréquence du vol de données pour les entreprises du secteur des produits de base et des produits de consommation est globalement importante. Par contre, pour les secteurs de l'industrie et des produits ou services techniques, elle est globalement faible.

A noter que le secteur financier présente un cas où la fréquence est très importante mais se situe globalement dans le 75ème percentile.



Graphe II.B.5 – Fréquence issue du générateur de perte ou vol de données par secteur d'activité

b. Exposition à la Perte d'exploitation

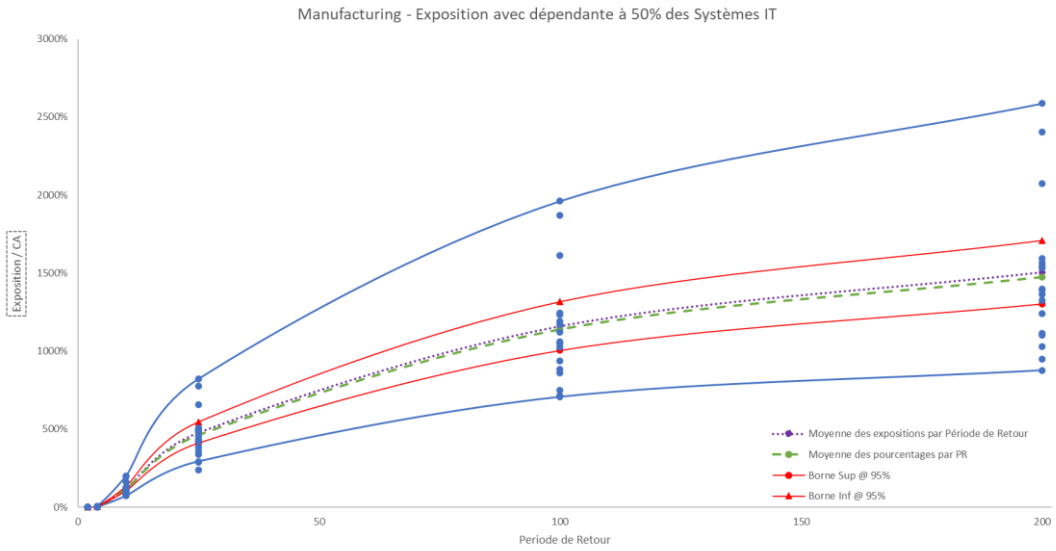
i. Intensité

Le générateur de scénarios donne les résultats pour une exposition de l'entreprise selon 3 scénarios :

- L'entreprise est dépendante de son système d'information (IT) à 10%, ce qui signifie que son activité est réalisée dans la majorité des cas sans avoir recours à ses systèmes d'information
- L'entreprise dépend à 50% de ses systèmes d'information
- L'entreprise dépend à 90% de ses systèmes d'information, ce qui implique que son activité est très liée à ses systèmes informatiques.

Le graphe ci-dessous décrit la courbe de distribution des scénarios des entreprises recensées dans le secteur d'activité « Manufacturing » (fabrication) pour une dépendance moyenne (50%) aux systèmes d'information.

Le graphe est construit en considérant les percentiles et donc les périodes de retour suivantes



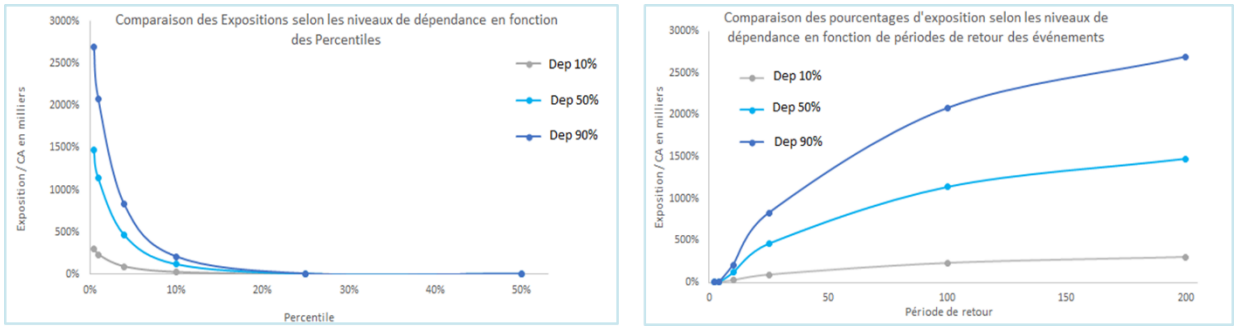
Graphe II.B.6 - Exposition à la PE avec dépendance à 50% de l'IT des entreprises du secteur de la fabrication

- 50% ou un évenement de période de retour de 2 ans
- 25% ou un événement de période de retour de 4 ans
- 10% ou un évenement de période de retour de 10 ans
- 4% ou un évenement de période de retour de 25 ans
- 1% ou un évenement centenaire
- 0,5% ou un événement bicentenaire

Les scénarios aux différentes périodes de retour ont été ramené en pourcentage du chiffre d'affaires de leur groupe respectif. Ceci permet de comparer les entreprises les unes avec les autres. Les chiffres d'affaires sont exprimés en milliers d'euros de façon à favoriser l'aspect visuel du graphique.

Ce résultat permet en première approche pour une entreprise manufacturière dont l'activité dépend à 50% de ses systèmes d'information de connaitre le sinistre perte d'exploitation centenaire moyen auquel elle pourrait faire face connaissant son chiffre d'affaire.

L'annexe H présente les courbes identiques pour les différents secteurs d'activités pour une dépendance 10%, 50% et 90%.



Graphe II.B.7 – Comparaison de l'exposition à la PE des entreprises de la fabrication selon le niveau de dépendance à l'IT

Pour l'étude de l'intensité, une autre information importante lors de la réalisation des courbes d'exposition consiste à comparer les résultats obtenus pour une même entreprise selon sa dépendance au système d'information.

En effet, ce critère est déterminé par l'entreprise elle-même ou par comparaison avec ses pairs et donne une indication sur l'intensité des scénarios générés.

Pour de faibles valeurs des périodes de retour, les scénarios sont relativement proches les uns des autres, la volatilité selon les pourcentage de dépendance aux systèmes d'information devient importante pour des périodes de retour supérieures à 20 ans.

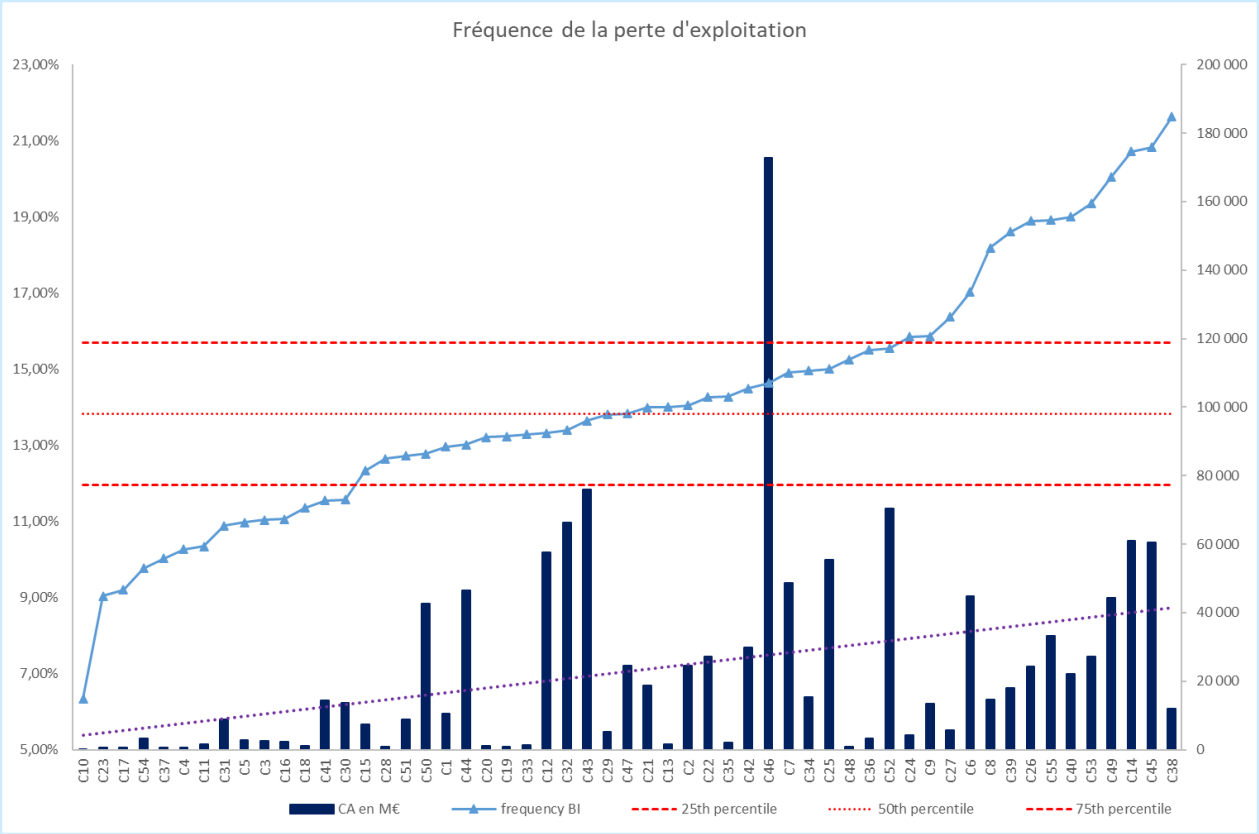
De même quelle que soit la période de retour, le scénario de dépendance à 10% des systèmes d'information est relativement stable jusqu'à 200% de la moyenne.

A l'issue de l'étude de tarification des programmes des captives qui souscrivent du risque Cyber, une hypothèse sur la dépendance aux systèmes d'information sera également réalisée.

ii. Fréquence

Contrairement à la fréquence pour le vol de données, la fréquence pour la perte d'exploitation est plus stable. Les conséquences de la perte d'exploitation dépendent moins du secteur d'activités et touchent toutes les entreprises dans la mesure où le système d'information est affecté par une attaque cyber.

Graphe II.B.8 – Fréquence issue du générateur de Parte d'exploitation



Les fréquences sont comprises entre 6,34% et 21,63%. L'intervalle entre le 25ème percentile et le 75ème percentile est réduit à [11,95% et 15,70%]. Elles semblent logiquement suivre l'évolution du chiffre d'affaires.

Elle se situe en moyenne autour de 14%.

C. METHODE DE CLASSIFICATION A PRIORI DES ENTREPRISES

Pour rechercher des critères de classement des entreprises, autre que la taille et le secteur d'activité, une classification a priori est envisagée.

1. DONNEES

Les données utilisées pour réaliser cette première classification proviennent de plusieurs sources :

- Les rapports édités par **CYENCE** pour les différentes entreprises pour lesquels est réalisée cette étude. De ces rapports, les informations quantitatives suivantes sont utilisées :
  - Le **Cyence** score et ses deux composantes **Susceptibility** et **Motivation.**

    Du fait de la forte dépendance entre ces 3 variables, **Susceptibility** et **Motivation** seront utilisées comme des **variables quantitatives supplémentaires**.

  - Le nombre d'incidents récents reportant les incidents sur les 2 dernières années et le nombre d'incidents passés. Les variables relatives à ces données sont **Recent_Event** et **Earlier_Incident**.

  - Les données de chiffre d'affaires (**CA**), nombre d'employés (**Staff**), nombre de données personnelles (**Nb_Pers**) sont également considérées.

    La variable **Staff** semble corrélée avec la variable CA, nous la considérons comme une **variable quantitative supplémentaire.**

Variable	Type	Commentaire
Cyence Score	Quantitative	
Motivation	Quantitative supplémentaire	Composante de Cyence Score
Susceptibility	Quantitative supplémentaire	Composante de Cyence Score
Recent_Event	Quantitative	Incidents subis sur les 2 dernières années
Earlier_Incident	Quantitative	Incidents subis depuis 3 ans et plus
Chiffre d'affaires	Quantitative	
Staff	Quantitative supplémentaire	Corrélée avec CA
Nb_Pers	Quantitative	Nombre de données personnelles (PII, PCI, PHI)

Figure II.C.1 – Variables quantitatives issues du rapport Cyence

  - La probabilité de violation de données (Data Breach), la probabilité de violation de données des pairs. Afin de comparer l'entreprise par rapport à ses pairs, nous construisons deux variables :

- La variable **peers_Impact** qui va indiquer la violation relative de l'entreprise par rapport aux pairs.
  - ✓ Une valeur négative représentera un meilleur « comportement de l'entreprise » par rapport à ses pairs.
  - ✓ Une valeur positive représentera un comportement moins bon.

- D'autres variables concernant les pairs sont également prises en compte. Il s'agit du nombre d'incidents ayant affectés les pairs et le nombre de pairs affectés. Comme ci-dessus, nous construisons la variable **Rapport_Peers** qui va mesurer le nombre moyen d'incident par pair.

Ces 2 variables sont des variables construites à partir de données obtenues dans le rapport Cyence, aussi nous les considérons comme des **variables quantitatives supplémentaires.**

Variable	Type	Commentaire
Peers_Impact	Quantitative supplémentaire	Violation des données de l'entreprise par rapport à ses pairs
Rapport_Peers	Quantitative supplémentaire	Nombre moyen d'incidents subis par les pairs

Figure II.C.2 – Variables quantitatives supplémentaires construites avec les données du rapport Cyence

- La variable qualitative relative au secteur d'activité de l'entreprise est également prise en compte et est considérée comme une **variable qualitative supplémentaire.**

Variable	Type	Commentaire
Activity_Cyence	Qualitative supplémentaire	Secteur d'activité défini dans Cyence

Figure II.C.3 – Variables qualitative supplémentaire issue du rapport Cyence

- D'autres variables permettant de prendre en compte le secteur d'activité du groupe dans les générateurs de scénarios sont également prises en compte. Il s'agit des variables :
  - **Net_Margin** et **BI-Value** pour le modèle BI. Ces paramètres sont soit propres à chaque entreprise (si l'entreprise est recensée dans la base) soit déterminée par un benchmark réalisé selon le secteur d'activité de l'entreprise.
    - **Net_Margin** permet de mesurer le revenu / bénéfice net
    - **BI_value** permet de mesurer la perte assurable.

  - **Spread** et **Cyber_Class** pour le modèle Privacy. Ces paramètres sont propres à chaque secteur d'activité et permettent de mesurer :
    - **Spread :** Variable construite sur le croisement entre le secteur d'activité et le type de violation de données.

- **Cyber_Class** paramètre déterminé selon un benchmark permettant de calculer la fréquence selon le secteur d'activité. Ainsi nous considérons cette variable comme une **variable quantitative supplémentaire**.

Variable	Type	Commentaire
Net_Margin	Quantitative	Générateur de Perte d'exploitation
BI_value	Quantitative	Générateur de Perte d'exploitation
Spread	Quantitative	Générateur de vol ou perte de données
Cyber_Class	Quantitative supplémentaire	Générateur de vol ou perte de données - Issue d'un calcul

Figure II.C.4 – Variables issues des générateurs de scénarios

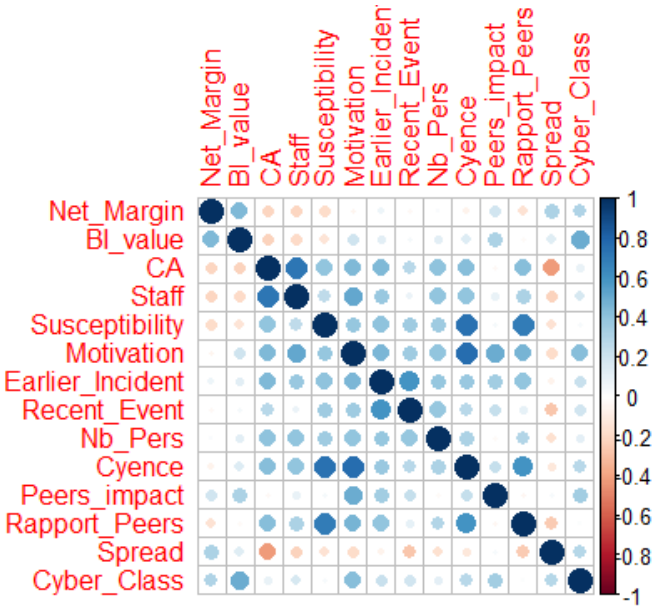
2. ANALYSE EN COMPOSANTES PRINCIPALES (ACP)

Le jeu de données contient 55 individus et 15 variables,

- 6 variables quantitatives sont illustratives,
- 1 variable qualitative est illustrative.

a. Matrice de corrélation

Nous construisons la matrice de corrélation avec les variables retenues ci-dessus.



Graphe II.C.5 – Matrice de corrélation

La matrice de corrélation confirme que les variables **Cyence**, **Susceptibility** et **Motivation** sont corrélées et renforce l'hypothèse de considérer **Susceptibility** et **Motivation** comme des variables quantitatives supplémentaires.

Même constat concernant les variables **CA** et **Staff** et l'hypothèse de considérer **Staff** comme une variable quantitative supplémentaire.

Par ailleurs, **Net_Margin** et **BI_value** sont également corrélées mais elles sont toutes les deux nécessaires au calcul de la fréquence dans le générateur de scénarios du BI (Perte d'Exploitation).

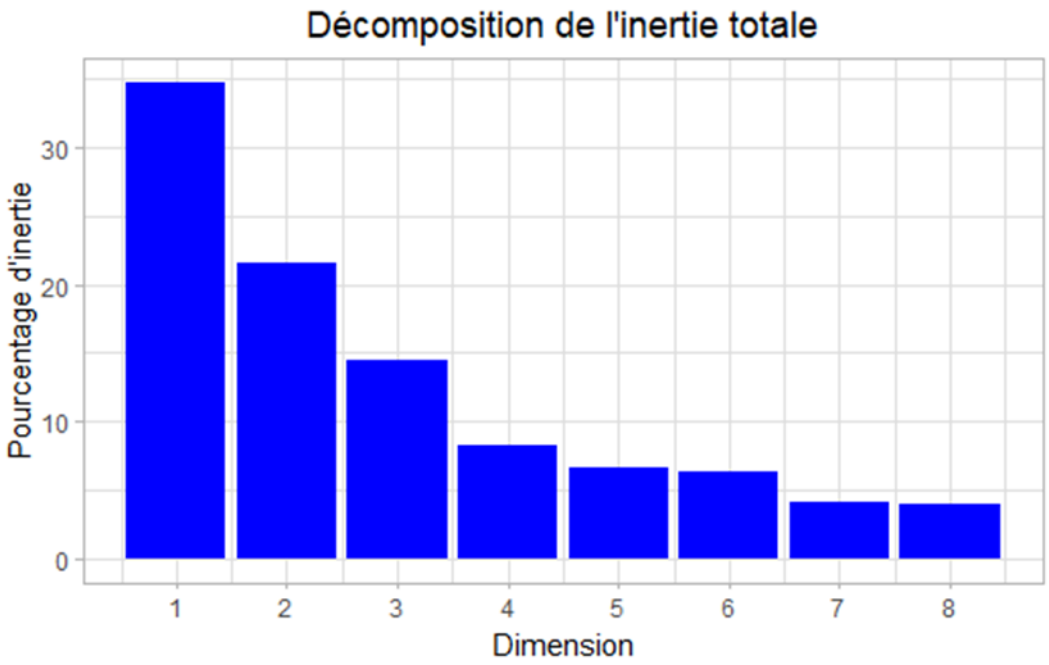
b. L'ACP – Distribution de l'inertie

Afin de réaliser l'ACP, nous utilisons les packages FactoMineR et Factoshiny de R.

L'analyse des graphes ne révèle aucun individu singulier.

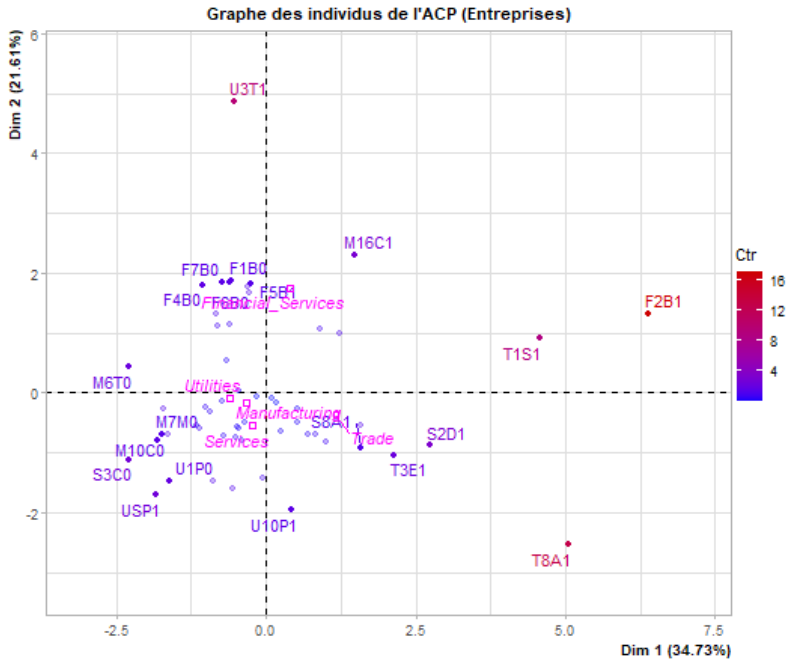
L'inertie des axes factoriels indique d'une part si les variables sont structurées et suggère d'autre part le nombre judicieux de composantes principales à étudier.

Les 2 premiers axes de l'analyse expriment 56.34% de l'inertie totale du jeu de données ; ainsi 56.34% de la variabilité totale du nuage des individus (ou des variables) est représentée dans ce plan. Le pourcentage assez important, et le premier plan représente donc convenablement la variabilité contenue dans une grande part du jeu de données actif.



Graphe II.C.6 – Distribution de l'inertie selon les dimensions

c. Graphes des individus

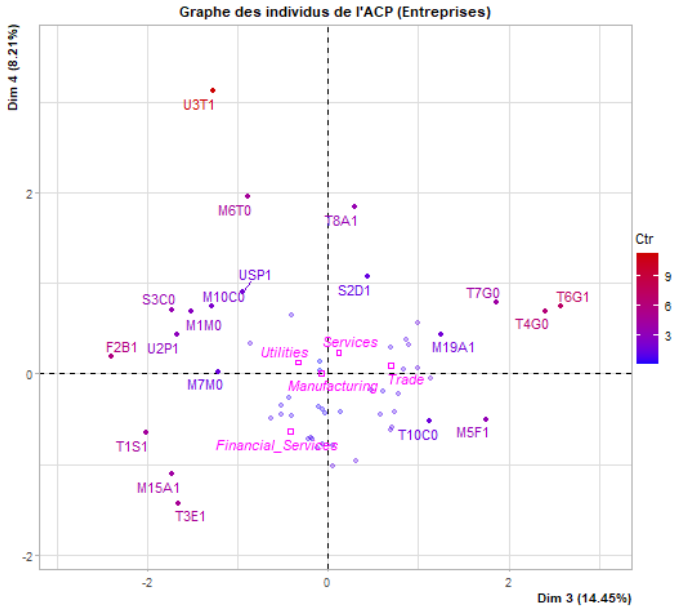


Le graphe des individus représente les entreprises selon les dimensions du plan.

Les 20 premières entreprises sont reportées en termes de contribution.

Les libellés sont colorés en fonction de la contribution à la construction du plan. Ceux représentés en rouge ayant une contribution plus importante.

Graphe II.C.7 - Graphe des Individus de l'ACP selon les dimensions 1 et 2



Les résultats obtenus sur le plan 3 et 4 expriment 22,66% d'inertie supplémentaire.

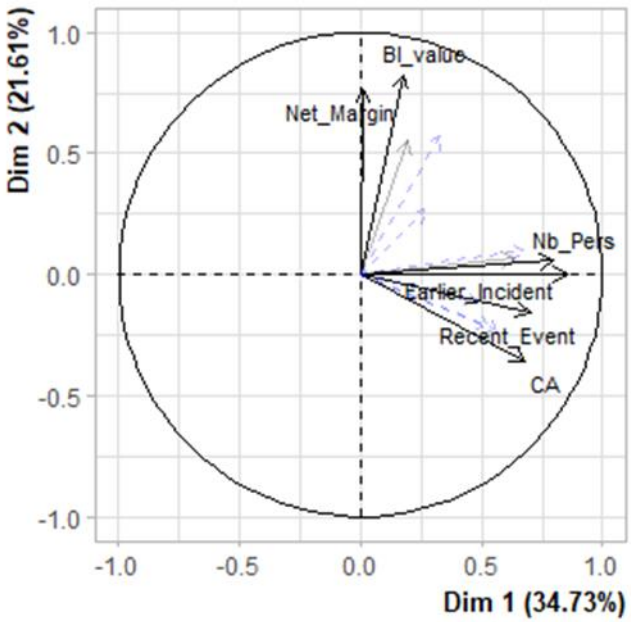
Avec les dimensions 1 et 2, 79% de l'inertie totale est exprimée avec les 4 dimensions.

Comme pour le plan 1 et 2, les libellés sont colorés en fonction de la contribution des entreprises (individus) à la construction du plan.

Sur les deux graphes, les modalités de la variable qualitative supplémentaire **Activity_Cyence** sont positionnées sur le plan.

Graphe II.C.8 - Graphe des Individus de l'ACP selon les dimensions 3 et 4

d. Graphe des variables



Graphe II.C.9 - Graphe des variables de l'ACP selon les dimensions 1 et 2

Les variables représentées par une flèche noire sont les variables actives, celles en bleu sont les variables quantitatives supplémentaires (illustratives). Les 6 variables libellées sont celles les mieux représentées sur le plan. Ce sont les variables qui caractérisent la taille des entreprises (**CA**), l'historique des incidents (**Recent_Event** et **Earlier_Incident**), le nombre de données personnelles (**Nb_Pers)** et la représentation mathématique du secteur d'activité pour le générateur de perte d'exploitation (**Net_Margin** et **BI_value**).

e. Interprétation des dimensions

L'annexe I.1 donne des représentations complémentaires de l'ACP selon les dimensions 3 et 4 et détaille l'interprétation des dimensions 1 et 2. Les résultats principaux sont repris ci-dessous.

La dimension 1 oppose des entreprises ayant déjà subi des attaques cyber avec des entreprises dont l'indice de motivation des hackers est plutôt faible et dont la perte assurable dans le cas de la perte d'exploitation est faible.

La dimension 2 oppose des entreprises pour lesquelles les conséquences d'une attaque cyber pourraient s'avérer plus ou moins importante (valeur de **BI_value** importante selon l'axe positif et **BI_value** faible selon l'axe négatif).

3. CLASSIFICATION

Avec les résultats de l'ACP, nous réalisons une classification. Le package Factoshiny de R, propose directement la réalisation de la classification par la méthode de classification ascendante hiérarchique.

L'annexe I.2 détaille les classes selon les dimensions 3 et 4.

a. Arbre hiérarchique et plan factoriel

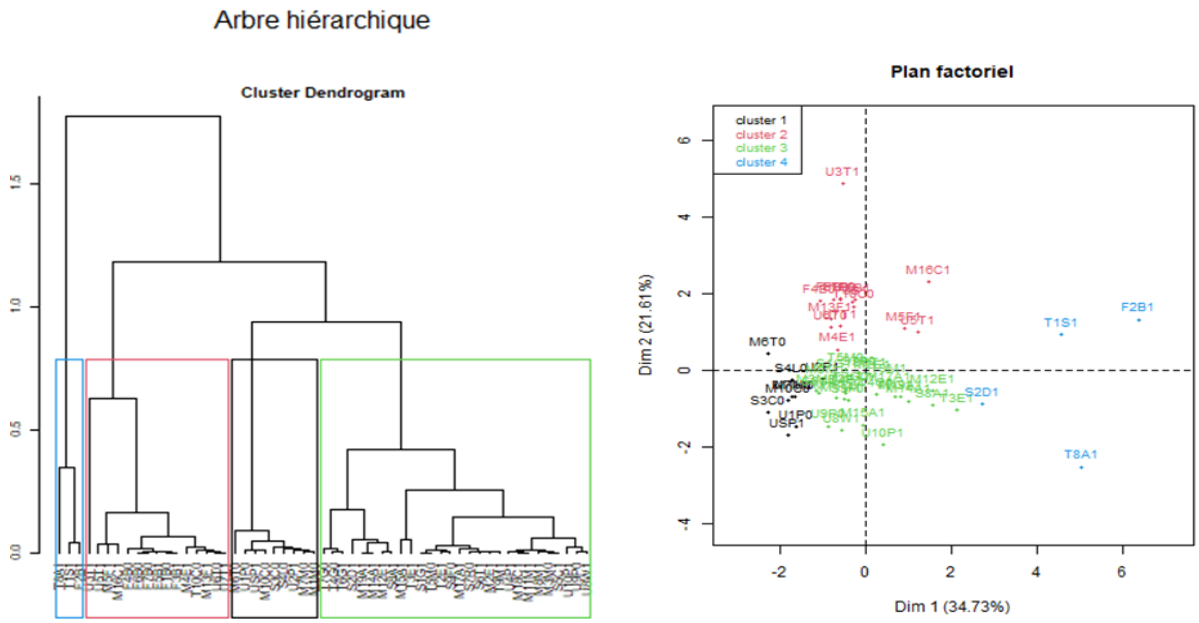
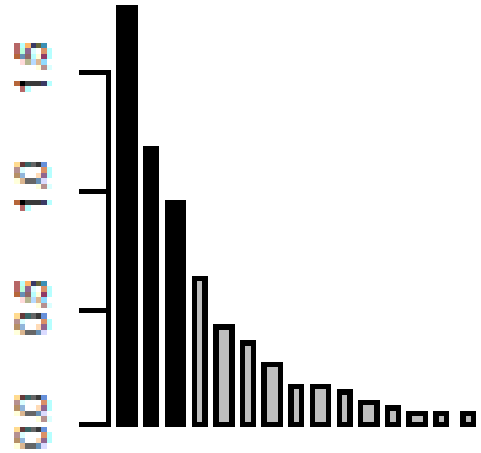


Figure II.C.10 – Arbre hiérarchique et plan factoriel, classification Ascendante Hierarchique des Individus

b. Distribution de l'inertie et choix des dimensions



Graphe II.C.11 – Distribution de l'inertie

L'utilisation du diagramme de distribution de l'inertie permet d'aider au choix du nombre de classes à sélectionner.

Généralement, le choix s'effectue dès que le « saut » observé est faible. Ceci indique que le niveau d'information suivant à récupérer est faible et qu'il n'est plus vraiment utile de regrouper les classes suivantes.

La classification réalisée sur les individus fait apparaître 4 classes corroborée par le graphe de gain d'inertie où la perte d'inertie est importante entre la troisième et la quatrième classe puis le « saut » devient faible.

c. Interprétation des classes

i. La classe 1

Elle est composée d'individus tels que *U1P0*, *M6T0*, *USP1* et *S3C0*. Ce groupe est caractérisé par de faibles valeurs pour les variables *Cyence, Motivation, Susceptibility, peers_Impact, Cyber_Class, Spread, Staff, CA et BI_value* (de la plus extrême à la moins extrême).

Elle représente des entreprises comportant des facteurs de menaces forts

ii. La classe 2

Elle est composée d'individus tels que *F1B0*, *F3B1*, *F4B0*, *U3T1*, *F5B1*, *F6B0*, *M16C1*, *F7B0* et *T10C0*. Ce groupe est caractérisé par :

- de fortes valeurs pour les variables *BI_value, Spread, Cyber_Class et Net_Margin* (de la plus extrême à la moins extrême).
- de faibles valeurs pour les variables CA (de la plus extrême à la moins extrême).

Elle représente des entreprises de taille faible avec une exposition au risque cyber important.

iii. La classe 3

Elle est composée d'individus tels que *S2D1*, *T3E1*, *U8W1* et *U10P1*. Ce groupe est caractérisé par :

- de fortes valeurs pour les variables *Cyence*, *Susceptibility*, *Staff*, *peers_Impact* (de la plus extrême à la moins extrême).
- de faibles valeurs pour les variables BI_value et Net_Margin (de la plus extrême à la moins extrême).

A l'inverse la classe 3 représente des entreprises de taille assez importante avec une exposition au risque cyber contenue mais qui a été la cible d'incidents passés plus nombreux que ses pairs.

iv. La classe 4

Elle est composée d'individus tels que *F2B1*, *T1S1* et *T8A1*. Ce groupe est caractérisé par :

- de fortes valeurs pour les variables *Nb_Pers*, *Earlier_Incident*, *Recent_Event*, *CA*, *Motivation* et *Staff* (de la plus extrême à la moins extrême).
- de faibles valeurs pour la variable Spread.

Cette classe regroupe les entreprises importantes avec un nombre de données élevées et qui ont subis des incidents cyber dans le passé.

4. CONCLUSION

Cette étape de classification met en évidence 4 classes d'entreprises essentiellement selon la taille, le secteur d'activité, l'intensité de la menace et l'historique des incidents passés.

D. TARIFICATION DU RISQUE CYBER DENOMME

Les scénarios simulés par les générateurs nous permettent d'établir un modèle de tarification. En effet, en l'absence de données sinistres exhaustives, le modèle Fréquence-Sévérité développé ci-dessous utilisera les montants des scénarios.
Le benchmark de sinistres permettra de faire un *back testing*.

1. METHODES

a. Construction du Modèle de Tarification à partir des scénarios

Sous l'hypothèse d'indépendance entre les montants des scénarios (coûts) et les fréquences, l'espérance de la charge sinistre ou prime pure est déterminée par

$$\mathbb{E}[S] = fréquence\ moyenne * coût\ moyen.$$

La composante coût moyen va être modélisée avec l'utilisation des montants des scénarios générés.
Comme décrit dans le chapitre sur « L'étude de l'exposition au risque cyber », la fréquence est issue des générateurs de scénarios.
Pour rappel, elle correspond au nombre de scénarios non nuls pour la perte d'exploitation.

i. Hypothèses

La fréquence des sinistres suit une loi de poisson : la probabilité $(p_n)_{n\geq 0}$ qu'une variable aléatoire N (nombre de sinistres cyber annuels) prenne la valeur n_i (n_i = 0,1, 2…) pour un scénario i est distribuée par la loi de Poisson P($\boldsymbol{\lambda}$) avec $\boldsymbol{\lambda}$ >0 si pour tout n_i positif, n_i entier :

$$\boldsymbol{P(N = n) = \frac{e^{-\lambda}\lambda^{n}}{n\,!}}$$

$$\boldsymbol{E[N] = \lambda} \text{ et } \boldsymbol{\sigma^2[N] = \lambda}$$

La loi de poisson utilisée pour la perte d'exploitation est différente de celle utilisée pour le vol de données pour chacune des entreprises considérées. De même pour les scénarios perte d'exploitation, exposition aux données personnelles PII, exposition aux données cartes de crédit PCI et exposition aux données sensibles PHI.

Les scénarios (sinistres) relatifs à la perte d'exploitation et au vol de données sont indépendants

Pour simuler chaque sinistre, un scénario est tiré (choisi aléatoirement) dans la base des scénarios correspondante selon l'hypothèse que tous les scénarios ont la même probabilité de survenance. De ce fait, la probabilité de tirage d'un scénario perte d'exploitation (respectivement vol de données) ne dépend pas du montant du scénario.

ii. Utilisation des fonctions @Risk

Le logiciel @Risk contient un ensemble de lois mathématiques utilisables pour modéliser le risque.

- La fonction RiskPoisson est utilisée pour modéliser la fréquence calculée par les deux générateurs de scénarios.

- La fonction RiskDiscrete ({X_1, X_2, …, X_n}, {p_1, p_2, …, p_n}) permet de réaliser des « tirages » de scénarios. Chaque résultat a une valeur de X et un poids p qui peut être différent. Dans notre cas, nous faisons l'hypothèse que la probabilité d'occurrence d'un scénario est identique quel que soit le scénario et celle-ci est égale à p, définie ainsi :

    - p_n = 0,01% pour les scénarios de vol et perte de données personnelles que ce soit les scénarios PII, PHI ou PCI
    - $p_N = \frac{1}{N}$ pour les scénarios de perte d'exploitation

iii. Illustration

L'extrait ci-dessous illustre la base de données utilisées pour chaque entreprise.

POUR LA PERTE D'EXPLOITATION

Severity distribution for Business Interruption

Hypothèse:

Les revenus de l'entreprise sont à 10%, 50% ou 90% dépendant des systèmes informatiques

10%	50%	90%	Probabilité		
			10%	50%	90%
216 201	277 860	288 382 184	0,00324%	0,00323%	0,00320%
10 432 613	1 478 736	1 583 935	0,00324%	0,00323%	0,00320%
9 046 684	587 256	1 176 121	0,00324%	0,00323%	0,00320%
775 032	387 353	41 184 457	0,00324%	0,00323%	0,00320%
16 595 740	398 002	975 436	0,00324%	0,00323%	0,00320%
576 485	1 437 931	214 431 668	0,00324%	0,00323%	0,00320%
29 659 012	1 506 106	51 615 778	0,00324%	0,00323%	0,00320%
1 150 849	753 419	1 606 198	0,00324%	0,00323%	0,00320%

Dans cet exemple, 8 résultats de scénarios sont reportés pour chaque dépendance au système d'information

Le deuxième scénario pour une entreprise dépendante à 50% de son système d'information équivaut à un sinistre de 1 478 736€.

Il survient avec une probabilité de 0,00323%

Figure II.D.1 – Illustration des scénarios de perte d'exploitation

POUR LE VOL DE DONNEES

Severity distribution for Data Breach

Numéro de scénario	Proba	PCI	PHI	PII
1	0,01%	1 143 943	719 744	385 663
2	0,01%	1 321 739	1 158 819	668 180
3	0,01%	482 761	482 224	651 311
4	0,01%	251 699	810 267	345 278
5	0,01%	750 073	582 186	583 769
6	0,01%	790 805	1 075 929	1 251 994

6 scénarios de vols de données sont reportés pour chaque type de données.

Le deuxième scénario pour le vol de données sur les cartes de crédit s'élève à 1 321 739€.

Sa probabilité de survenance est de 0,01% puisque 10 000 scénarios ont été simulés, la fréquence d'occurrence étant directement déterminée par le générateur.

Figure II.D.2 – Illustration des scénarios pour le vol de données

b. Utilisation d'un benchmark sinistres

L'utilisation du benchmark sinistres permet de modéliser le risque cyber en construisant un modèle qui utilise un historique de sinistres. Une tarification des programmes des captives qui souscrivent du risque cyber est également réalisée et comparée avec les résultats obtenus lors de la tarification avec les scénarios.
Afin de déterminer les paramètres de fréquence et sévérité de ce modèle, les hypothèses suivantes sont proposées :

i. Sévérité

Pour déterminer la sévérité, nous faisons l'hypothèse que la typologie des sinistres du benchmark est représentative des sinistres éventuels de l'échantillon des captives étudiées quel que soit son secteur d'activités, comme présenté lors de la présentation des données du benchmark (Chapitre II.A.4). Cette hypothèse permet d'utiliser un échantillon de sinistre suffisant afin de ne pas trop introduire de volatilité selon les secteurs d'activité.

Le modèle est décomposé en trois catégories de sinistres :

- Les sinistres récurrents
- Les graves
- Les sinistres CAT

L'annexe J expose la méthodologie utilisée pour déterminer le seuil de sinistres graves et l'annexe K celui des sinistres catastrophiques.

Pour chaque composante, une courbe de distribution est ajustée sur l'échantillon de sinistres de la catégorie considérée.

Chaque sinistre $X_{i\ (i = 1\ à\ n)}$ est supposé indépendant et identiquement distribué.

Les sinistres Xi sont représentés par la fonction de répartition F de X qui donne pour toute valeur de x choisie la probabilité que la variable aléatoire X soit inférieure ou égale à x. C'est cette courbe de distribution connue continue qui modélise la sévérité.

Par ailleurs, l'espérance mathématique des sinistres qui permet de calculer la prime pure du contrat est donnée par

$$E[X] = \int_{x \in R_+} x dF(x) = \int_{x \in R_+} P(X > x)\, dx$$

Avec P(X > x) la probabilité qu'un sinistre soit supérieur à x et f(x) = $\frac{dF(x)}{dx}$ la fonction densité de probabilité, dérivée de F.

Avec le logiciel @Risk, la courbe observée est approchée par des courbes de distribution connues avec lesquelles il sera aisé de calculer les moments, notamment l'espérance de X. L'utilisation de ces lois connues permettra d'estimer les paramètres des lois choisies en maximisant la fonction de vraisemblance *L* qui s'écrit pour un ensemble de sinistres X_i dont la fonction de densité de probabilité, si elle existe, est notée f_x

$$L = \prod_{i=1}^{n} f_x(x_i)$$

La fonction « logvraisemblance » représentée par le logarithme népérien de L plus facile à mettre en œuvre est plus couramment utilisée et s'écrit :

$$l = \sum_{i=1}^{n} \ln [f_x(x_i)]$$

Le logiciel @risk utilise des lois dont l'estimateur du maximum de vraisemblance est dans la plupart des cas, unique et se calcule de façon explicite. Il est démontré que cet estimateur est asymptotiquement sans biais et convergent et que sa variance est minimale.

Dès que les paramètres de la loi sont estimés, des tests sont réalisés afin de savoir quel ajustement choisir.
Le logiciel @Risk donne plusieurs tests d'adéquation comme le test AIC … Chi2, Kolmogorov-Smirnov et Anderson-Darling.
Par habitude, le test du Chi^2 sera privilégié puis le test de Kolmogorov-Smirnov

ii. Fréquence

Comme le benchmark utilisé répertorie des sinistres cyber européens et américains, la fréquence déterminées par les échantillons n'est pas exploitable. Pour les entreprises considérées dans cette étude, la fréquence utilisée dans ce modèle de tarification est la même que celle dérivée des générateurs de scénarios.

2. TARIFICATION

a. Application du programme d'assurance, limites de garantie

Pour chaque risque, le nombre de sinistres survenus dans une année est déterminé par la courbe de fréquence puis la valeur de chacun de ces sinistres par la courbe de sévérité. Une simulation correspondra à la situation d'une année pour l'entreprise.

Pour chaque sinistre de chaque simulation, la franchise puis la limite d'acceptation du programme de l'entreprise sont appliquées de la façon suivante :

Soit S_i le montant d'un scénario i issu du générateur de scénarios du modèle BI. En cas d'application d'une franchise f_m et d'une limite l_m le coût du sinistre S_{ifl} sera :

$$S_{ifl} = (min(max(0\ ; S_i - f_m)\ ; l_m)$$

Le total de la charge sinistre acceptée par l'entreprise sur une année est ensuite « capée » à la limite annuelle l_a du programme de l'entreprise.

Soit n_a le nombre de sinistres simulés pour l'année a

$$S_a = max(\sum_{i=1}^{na} S_{ifl}\ ; l_a)$$

b. Simulation de la sinistralité et test de convergence

Nous effectuons 50 000 simulations en utilisant le logiciel @Risk. Sur cette base, les statistiques peuvent être dérivées, comme la moyenne, l'écart-type, les percentiles.

Le choix de 50 000 simulations est obtenu après un test de convergence réalisé sur un échantillon de 2 captives par secteur d'activité.

@Risk propose également une option selon laquelle le nombre de simulations est déterminé automatiquement par l'outil. Pour les captives de l'échantillon ce nombre de simulations est en ligne avec le choix des 50 000 simulations.

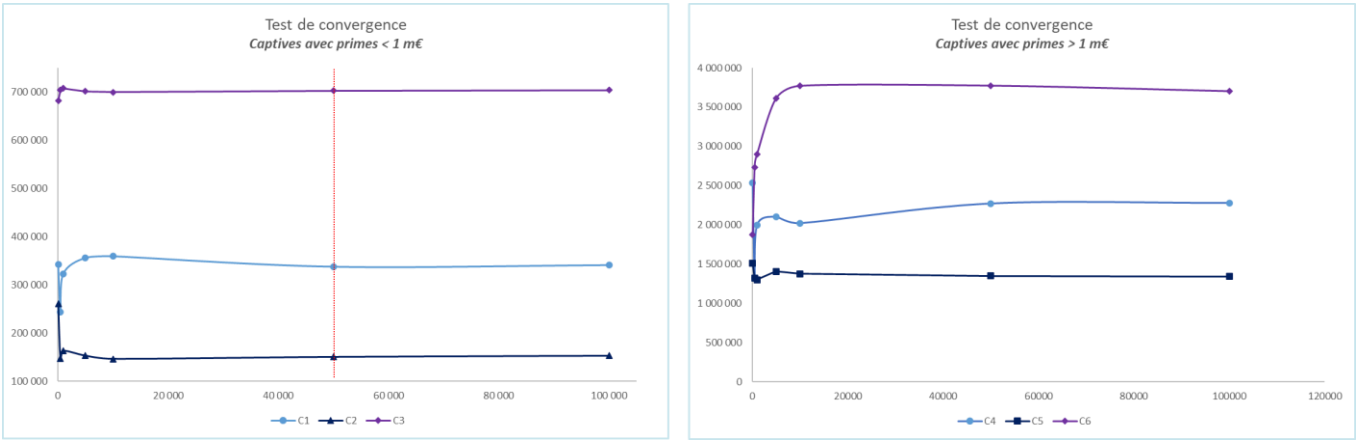


Figure II.D.3 – Test de convergence

c. Calcul de la prime technique

La prime est dérivée à partir des 50 000 simulations effectuées :

- La prime pure correspond à la moyenne des sinistres issus des 50 000 simulations ;
- La prime technique correspond à la prime pure auquel s'ajoute un chargement de sécurité déterminé en ajoutant un pourcentage de l'écart type des sinistres autour de la moyenne

$$\boldsymbol{Prime\ Pure = charge\ moyenne + écart\ type \times \alpha}$$

La pratique du marché des grands risques considère habituellement un $\boldsymbol{\alpha}$ de 25%.

A cette prime technique il faudrait théoriquement rajouter des frais généraux et les marges de réassurance pour obtenir la prime nette, laquelle est déterminée hors frais de courtage et autres commissions (« frais d'acquisition »).

C'est cette prime technique qui sera comparée à la prime souscrite dans la captive.

Ainsi les primes calculées par le modèle de tarification développé ci-dessous pourront être comparées aux primes réelles. Le modèle permettra vérifier la pertinence de la prime calculée par rapport à la prime qu'a payé la captive en 2020 – dans l'état actuel des connaissances du risque cyber.

3. RESULTATS ET VALIDATION DU MODELE

Les tableaux suivants présentent les résultats obtenus pour la partie modélisation et pour la partie tarification pour les différentes captives qui souscrivent du risque cyber. Elles sont au nombre de 14.

D'autres captives qui ne souscrivent pas de risque cyber mais qui acceptent des risques liés à des polices « Dommage aux biens », « Responsabilité Civile », « Responsabilité Civile des Mandataires Sociaux »

(risque peu ou pas souscrit habituellement dans les captives) et « Fraude » (notamment pour les banques), sont également étudiées. En effet, elles peuvent être exposées à un risque de « cyber silencieux » et exposer la captive à des sinistres qui n'ont pas été pris en compte dans la tarification.
La « prime manquante » pour ces 36 captives est déterminée selon le modèle de tarification développé.

A noter que 7 captives sont identifiées comme n'étant pas exposées au risque de souscription cyber. Ces dernières souscrivent d'autres types de police comme du crédit, de la RC décennale, du transport, de l'Employee Benefit etc.

a. Captives qui souscrivent du risque Cyber

50 000 simulations sont réalisées sur les 14 captives qui souscrivent du risque cyber et la courbe de distribution est déterminée sur le programme de la captive.

L'annexe L présente l'exemple d'une année de simulation

- Avec le détail des sinistres individuels pour la perte d'exploitation, le vol ou la perte de données (PCI et PII – le PHI est supposé nul dans cet exemple)
- L'application du programme de réassurance sur chaque sinistre individuel
- L'application de l'aggregate limite annuel (AAL) sur l'ensemble des sinistres simulés par l'année concernée.

Le tableau ci-dessous récapitule les distributions obtenues pour chacune des expositions de l'entreprise et les résultats appliqués au programme de réassurance de la captive.

En Euros			Au Premier Euro					Tarification Captive			
			PE (50%)	PCI	PHI	PII	Total	Programme 2020	Programme 2020 sans AAL	Programme 2021	Programme 2021 sans AAL
Moyenne			4 887 391	829 899	-	134 361	5 851 652	1 212 001	1 221 869	1 849 991	1 861 885
Ecart type			63 005 686	6 063 473	-	1 701 463	63 317 779	7 092 398	7 187 916	11 902 587	12 032 995
Percentile	1%	1,01	-	-	-	-	-	-	-	-	-
	10%	1,11	-	-	-	-	-	-	-	-	-
	50%	**2**	-	-	-	-	-	-	-	-	-
	80%	5,0	-	-	-	-	603 093	-	-	-	-
	90%	10,0	-	871 746	-	-	1 703 819	-	-	-	-
	95%	20,0	1 059 321	1 831 509	-	-	3 762 843	-	-	-	-
	96%	25,0	1 251 822	2 058 612	-	309 694	5 876 988	85 012	85 012	85 012	85 012
	97,0%	33,3	2 082 925	2 366 144	-	447 916	14 995 123	9 803 879	9 803 879	9 803 879	9 803 879
	99,0%	100,0	102 540 693	24 174 264	-	1 158 808	109 337 830	50 000 000	50 000 000	100 000 000	100 000 000
	99,5%	200,0	286 861 313	46 114 399	-	7 712 080	288 156 792	50 000 000	50 000 000	100 000 000	100 000 000
	99,9%	1 000	976 956 528	91 273 484	-	27 035 133	976 956 528	50 000 000	50 000 000	100 000 000	100 000 000

Table II.D.4 – Courbe de distribution des résultats des simulations pour une captive

Pour chaque captive, les trois hypothèses de dépendance aux systèmes d'information (respectivement 10%, 50% et 90%) ont été testées.

Pour certaines captives (3 sur les 14 considérées), ce modèle a servi à la tarification du programme cyber et a été paramétré en utilisant une dépendance au système d'information de 50% en accord avec l'entreprise qui a commandé la mission.

Pour les autres tarifications, la dépendance aux systèmes d'information de 90% a été *a priori* privilégié. De de fait, en combinant la sévérité ainsi déterminée à la fréquence estimée par les générateurs de scénarios, les résultats obtenus sont conformes aux tarifications des assureurs. Ce niveau de dépendance est retenu pour 8 captives sur les 14 qui souscrivent du risque cyber. Il permet de rester plus conservateur dans l'approche.

Sur les captives restantes (3 sur les 14 considérées), la dépendance de 10% aux systèmes d'information a été retenue pour 2 captives du secteur industriel. Ce résultat semble cohérent puisque l'activité manufacturière de ces entreprises ne requiert pas que des activités numériques.
La dépendance de 50% aux systèmes d'information a été retenue pour les captives du secteur des institutions financières.

En Euros	Tarification			
	Programme 2020	Programme 2020 sans AAL	Programme 2021	Programme 2021 sans AAL
Prime pure	**1 212 001**	**1 221 869**	**1 849 991**	**1 861 885**
% Ecart type	1 418 480	1 437 583	2 380 517	2 406 599
Ecart Type	7 092 398	7 187 916	11 902 587	12 032 995
Prime Technique	**2 630 481**	**2 659 452**	**4 230 509**	**4 268 484**
Rate On Line (ROL)	**5,26%**	**5,32%**	**4,23%**	**4,27%**
Frais généraux	526 096	531 890	263 048	263 048
Marge de réassurance	60 000	60 000	30 000	30 000
Prime nette	**3 216 577**	**3 251 343**	**4 523 557**	**4 561 532**
% Ecart type	20%	20%	20%	20%
% frais (si disponible)	20%			
Part client dans le programme	100%	100%	50%	50%
Prime Technique (hors tout)	**2 630 481**	**2 659 452**	**2 115 254**	**2 134 242**
Prime 2020	**2 470 125**			
Prime 2021			**1 714 867**	

A partir des estimations de charge moyenne et d'écart type sur le programme de la captive, la prime nette et la prime chargée sont calculées puis comparées à la prime que paie la captive aujourd'hui.

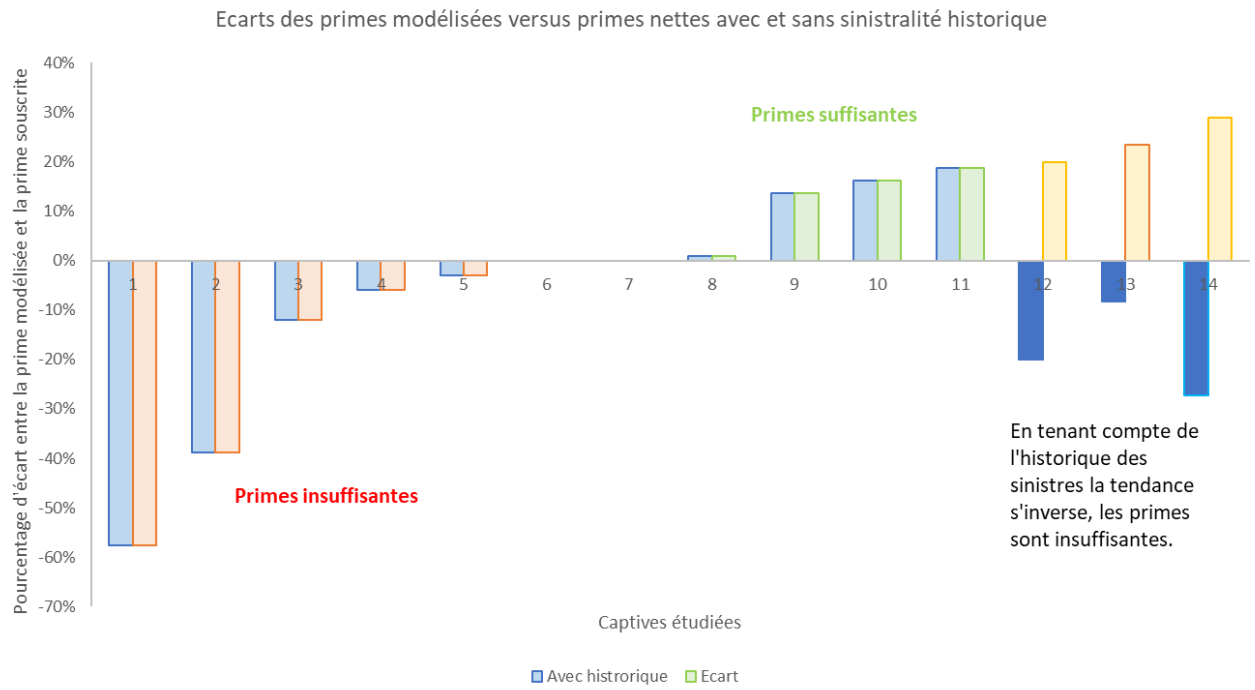
A noter que les primes de captive indiquées sont les primes nettes hors tout.

Table II.D.5 – Tarification avec la méthode des scénarios

b. Validation du modèle

Le graphe ci-dessous représente les écarts entre la tarification réalisée avec les scénarios et la prime réellement souscrite par la captive.
Les captives 6 et 7 ne montrent pas d'écart avec le modèle puisque la tarification a été réalisée avec le modèle.

Les primes sont insuffisantes pour 5 captives et semblent suffisantes pour 6 autres captives. Cependant les captives 12, 13 et 14 ont souffert de sinistres ce qui explique une prime plus importante souscrite par la captive.
En tenant compte de cet historique de sinistres, les primes souscrites sont en ligne (voire insuffisantes) par rapport au modèle.



Graphe II.D.6 – Ecart entre la prime souscrite et la prime estimée avec le modèle des scénarios

Le modèle de tarification à l'exposition tel que nous l'avons étudié semble sous-estimer la prise en charge de la sinistralité passée. A noter que cette information n'était pas connue au moment où les générateurs de scénarios ont été compilés, ce qui explique les résultats.

Il est donc primordial de bien renseigner les événements passés dans les générateurs de scénarios pour que ceux-ci tiennent bien compte de ces éléments lors de la génération de scénarios.

c. Comparaison avec le modèle qui utilise le benchmark

Comme indiqué lors de la présentation du modèle, la tarification se fait en plusieurs temps étapes car les modélisations des sinistres attritionnels (récurrents), des sinistres graves (large) et des sinistres catastrophiques (CAT) se font de manière séparée.

SINISTRES RECURRENTS

Sévérité

Ajustement

Limites	*De*	1
	A	1,00E+06

Table ajustement	Rec_Sev	
Distribution 1	BetaGeneral	*75 379*
Distribution 2	Gamma	*33*

Percentiles	Input	BetaGeneral	Gamma	Selection
0,000001	1	1	1	1
0,0001	1	1	1	1
0,001	1	1	1	1
0,002	1	1	1	1
0,003	1	1	1	1
0,004	1	1	1	1
0,005	1	1	1	1
0,006	1	1	1	1
0,007	1	1	1	1
0,008	1	1	1	1
0,009	1	1	1	1
0,01	1	1	1	1
0,015	1	1	1	1
0,02	1	1	1	1
0,025	1	1	1	1
0,03	1	1	1	1
0,035	1	1	1	1
0,04	1	1	2	1
0,045	1	1	3	1
0,05	1	1	4	1
0,055	33	2	5	2
0,06	81	3	7	3
0,065	98	4	10	4
0,07	99	5	13	5
0,075	99	7	17	7

Résultat ajustement

Distribution	BetaGeneral	*75 379*
Description	RiskBetaGeneral(0,22404;0,96512;0;677034)	

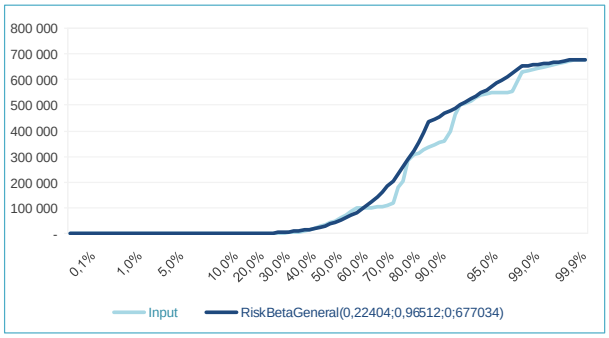


Table II.D.7 – Ajustements des distributions issues du benchmark sinistres – sinistres récurrents

Le modèle développé permet d'ajuster 2 courbes de distribution au benchmark des sinistres et d'en choisir une en fonction de l'erreur d'ajustement calculé selon différentes méthodes.

Le cas ci-dessus présente un ajustement pour les sinistres attritionnels avec une loi de Pearson, alors que la loi bêta donnait également un bon ajustement de la sinistralité.

L'annexe M présente un échantillon de courbes d'ajustement obtenu pour les sinistres attritionnels et pour les sinistres graves avec les paramètres ayant permis de réaliser le choix entre les courbes.

La loi choisie est ensuite utilisée dans le modèle fréquence sévérité.

1 HYPOTHESE DE SIMULATION

Tous Sinistres

Courbe d'ajustement

Sinistres récurrents	Fréquence	Sévérité
Param 1	5,00	0,22
Param 2	0,04	0,97
Param 3		-
Param 4		6 777 034,00
Shift		
Montant Sinistre max		1,00E+06
Fonction @ Risk	**Poisson**	**Beta General**

Sinistres large	Fréquence	Sévérité
Param 1	18,88	3 740 885,00
Param 2		979 396,00
Param 3		
Param 4		
Shift		807 344,00
Montant Sinistre max		
Fonction @ Risk	**Poisson**	**Invgauss**

Tous les sinistres	Fréquence	Sévérité
Param 1	749,00	0,25
Param 2	1 072,00	1,43
Param 3	32 675,00	797 034,00
Param 4		
Shift		
Montant Sinistre max		
Fonction @ Risk	**Hypergeo**	**Pearson6**

Courbe d'ajustement

Sinistres CAT	Proba	Montant/Nb	
Sévérité	100%	185 000 000	avec franchise
Fréquence	99,80%	-	
	0,20%	1	
Fonction @ Risk	**Discrete**		

Calibration risque	
Prime commerciale	
Prime commerciale estimée	1 610 476
Différence	
Prime technique estimée	1 609 776
Ecart type	8 265 174
Prime pure	370 000

Table II.D.8 – Hypothèse de simulation pour tarification avec le Benchmark sinistres

La table ci-dessus détaille les lois choisies pour les trois catégories de sinistres.

Comme dans le cas du modèle qui utilise les scénarios, 50 000 simulations du couple fréquence / sévérité sont réalisées sur les captives qui souscrivent du cyber.

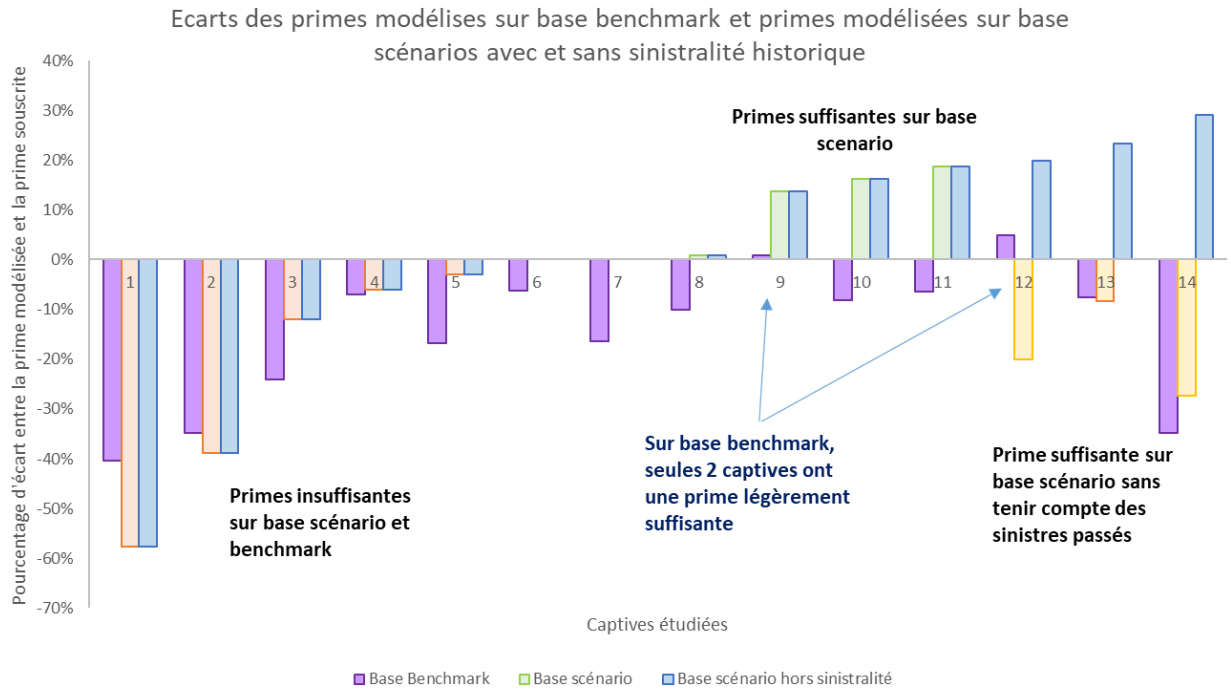
L'utilisation de la composante catastrophique dépend de la capacité souscrite dans chaque captive et de l'exposition globale de l'entreprise.

Dans l'exemple elle correspond à un sinistre de 185 m€ auquel est affecté une période de retour de 500 ans, ce qui ne peut s'appliquer qu'aux entreprises dont l'exposition reste inférieure à 200 m€ sur la globalité des scénarios.

Les résultats obtenus reprennent le graphe II.D.6 sur lequel la composante « Ecart de la prime simulée avec le benchmark versus la prime souscrite » est ajouté (en violet).

Les résultats sont relativement en ligne avec les résultats du modèle avec les scénarios même en ajoutant une composante catastrophique, mais ils sont globalement plus conservateurs. En effet, presque toutes les captives souscrivent une prime inférieure par rapport à la prime modélisée, sauf deux d'entre elles (dont une à la marge).

Le modèle qui utilise le benchmark est globalement plus conservateur et la prime manquante est de l'ordre de 20%.



Graphe II.D.9 – Ecart entre la prime souscrite et la prime estimée avec le benchmark et les scénarios

E. TARIFICATION DU RISQUE CYBER SILENCIEUX

L'un des objectifs de cette étude est de mesurer l'impact qu'aurait un sinistre Cyber sur une captive qui n'en souscrit pas nommément.

En effet, si le cyber n'est pas spécifiquement exclu des polices Dommages, RC, Fraude et D&O, celles-ci peuvent être touchées par un sinistre cyber alors que la prime déterminée lors de la tarification n'a pas tenu compte de cette typologie de sinistre potentiel.

L'idée est donc de mesurer quel est l'ordre de grandeur de cette prime non tarifée.

Dans l'échantillon des 55 captives étudiées, 32 ne souscrivent pas directement de programme cyber mais peuvent être touchées au titre du cyber silencieux du fait d'autres programmes.

La méthode utilisée pour mesurer l'impact de ces couvertures silencieuses dans cette partie de l'étude consiste à

- Décomposer les scénarios obtenus par les générateurs en risque de dommage (nommé *First Party*) et en risque de tiers (nommé *Third Party*).
- Appliquer les scénarios *First Party* et *Third Party* sur les programmes des captives dans les branches considérées et tarifer l'impact de ces scénarios pour la captive.
- Evaluer la prime manquante dans les captives qui ne souscrivent pas du risque Cyber et mesurer son importance au regard de la prime souscrite pour le contrat en question.

La tarification par l'historique n'est pas possible dans ce cas, car les informations sur les sinistres ne permettent pas de distinguer les parties *First* et *Third Party*.

1. LA DECOMPOSITION DE L'EXPOSITION

a. Risque de Dommage

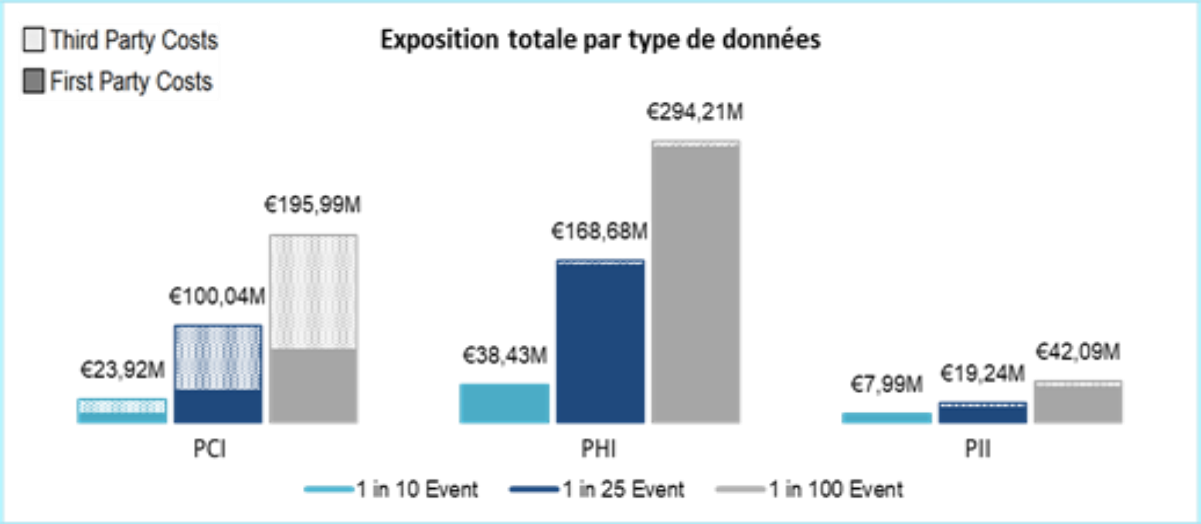
Les pertes d'exploitation sont des garanties typiques de la police Dommage. Ainsi, les scénarios provenant du générateur de perte d'exploitation correspondent à du risque *First party*.

Lors de l'étude de l'exposition, la dépendance aux systèmes d'information a également été abordée. Afin de rester conservateur dans notre approche, nous privilégions une dépendance à 90% des systèmes d'information pour toutes les captives qui ne souscrivent pas du risque cyber mais qui sont susceptibles d'indemniser des dommages résultant de sinistres qui ne sont pas spécifiquement exclus.

Par ailleurs, les scénarios obtenus avec le générateur de vol de données contiennent une part d'exposition au *First party* et une part d'exposition au *Third Party*. Nous scindons ces expositions afin de ne conserver que l'exposition au *First Party* pour la partie de risque liée au « Dommage ».

b. Risque de Tiers

La partie des scénarios *Third Party* du générateur de vol de données vient alimenter les expositions liées au risque de tiers, notamment pour la partie des données relatives aux cartes de crédit (les coûts liés aux fraudes sur les cartes bancaires, à la réémission des cartes bancaires ou encore à la vérification des réseaux de cartes de paiement, mais aussi les frais de litige).



Graphe II.E.1 – Coût total du First Party et du Third Party

Le graphe ci-dessus illustre cette répartition entre *First Party* et *Third Party* d'une entreprise qui possède les 3 types de données (PCI, PII et PHI).

L'exposition au vol de données des cartes de paiement est logiquement la plus contributrice en termes de *Third Party* que les autres typologies de données puisque des frais spécifiques viennent s'ajouter dans cette catégorie.

Pour chaque captive étudiée, 10 000 scénarios sont générés et les données suivantes sont recueillies

c. Impact sur les scénarios

i. Pour le *First Party*

A titre d'exemple, le tableau ci-dessous présente les 12 premiers scénarios *First Party* pour le vol de données d'une des entreprises étudiées, sur les 10 000 simulés.
La partie « Contrôle des crédits » représente l'exposition la plus importante pour cette entreprise.

First Party					
Number of Scenario	Forensics Investigation	Call Center Costs	Privacy Notification Costs	Credit Monitoring	Total 1st Party Costs
Average	285 200	62 416	405 325	8 838 266	9 591 206
1	45 883	24 169	42 115	883 007	995 175
2	49 161	43 679	25 065	37 962	155 866
3	61 165	36 600	39 780	469 425	606 969
4	1 149 064	149 011	4 553 852	121 832 733	127 684 661
5	188 292	25 312	19 318	40 693	273 614
6	1 075 090	143 771	916 170	11 802 060	13 937 092
7	34 926	68 175	16 972	759 370	879 443
8	34 538	34 459	50 039	1 217 367	1 336 404
9	681 606	230 643	484 683	7 374 712	8 771 643
10	101 931	59 965	29 929	751 627	943 452
11	113 965	37 757	30 975	27 796	210 493
12	1 707 565	193 405	4 179 141	76 154 136	82 234 248

Table II.E.2 – First Party – Extrait de la décomposition des scénarios

ii. Pour le *Third Party*

Le tableau ci-dessous représente la partie *Third Party* des mêmes 12 scénarios générés pour l'entreprise présentée ci-dessus.

Third Party PCI						
Numéro de scénario	Litigation Expense	Regulatory Action	Fraud	Card Reissuance	Assessments from Card Networks	Total 3rd Party Liability
Average	764 430	18 089	5 311 719	8 394 143	178 113	14 666 494
1	232 664	0	0	436 679	687 111	1 356 454
2	139 587	0	0	28 885	561 742	730 214
3	155 718	0	0	424 231	2 836 809	3 416 758
4	5 006 961	0	80 088 523	127 187 984	1 123 382	213 406 849
5	152 679	0	0	19 789	111	172 580
6	1 638 581	0	29 242 990	11 644 767	8 802	42 535 141
7	176 417	0	0	422 309	111 347	710 074
8	41 869	0	0	445 414	1 611 822	2 099 106
9	6 519 927	0	16 507 436	5 199 646	16 124	28 243 133
10	223 064	0	0	436 715	758	660 537
11	121 626	0	0	20 338	53 037	195 002
12	2 291 322	0	55 550 029	90 121 096	16 547	147 978 995

Table II.E.3 – Third Party pour le PCI – Extrait des scénarios

Le tableau ci-dessous représente un extrait des 12 premiers scénarios d'une entreprise étudiée pour le PHI (données sensibles) et le PII (données personnelles).

Third Party PII			
Number of scénario	Litigation Expense	Regulatory Action	Total 3rd Party Liability
Average	619 411	15 128	634 539
1	246 115	0	246 115
2	42 722	0	42 722
3	109 519	0	109 519
4	831 766	0	831 766
5	89 092	0	89 092
6	4 217 685	0	4 217 685
7	102 243	0	102 243
8	89 972	0	89 972
9	226 473	0	226 473
10	105 653	0	105 653
11	64 129	0	64 129
12	76 073	0	76 073

Third Party PHI			
Number of Scenario	Litigation Expense	Regulatory Action	Total 3rd Party Liability
Average	472 374	0	472 374
1	5 658 316	0	5 658 316
2	158 220	0	158 220
3	1 272 904	0	1 272 904
4	82 369	0	82 369
5	217 572	0	217 572
6	80 601	0	80 601
7	2 127 212	0	2 127 212
8	1 015 589	0	1 015 589
9	187 008	0	187 008
10	141 314	0	141 314
11	112 331	0	112 331
12	217 704	0	217 704

Table II.E.4 – Third Party PII et PHI – Extrait des scénarios

Pour le PII et le PHI seuls deux composantes font partie des scénarios de *Third Party*, il s'agit des frais de litiges et d'actions auprès du régulateur.

2. LA TARIFICATION DES GARANTIES LIEES AU RISQUE DE DOMMAGE ET AU RISQUE DE TIERS

Le modèle utilisé pour tarifer les programmes Cyber des captives qui ne souscrivent pas de risque cyber est le même que celui utilisé précédemment dans la partie « C. Tarification du risque Cyber dénommé ».

Dans ce cas, la tarification s'applique aux programmes « Dommages », « Responsabilité Civile », « Fraude » et « D&O » des captives qui ne souscrivent pas de Cyber mais qui souscrivent ces branches.

La majorité des captives de notre échantillon souscrivent des programmes « Dommages » et dans une moindre mesure de la « Responsabilité civile ». Les institutions financières qui ne souscrivent pas de Cyber dénommé couvrent des pertes liées aux fraudes dans le cas de police Globale de Banque et de la RC des Mandataires Sociaux (D&O).

Les garanties *First party* et *Third Party* sont traitées séparément. En effet toutes les captives ne souscrivent pas les deux types de garanties et les programmes couverts pour les deux typologies de risque sont différents. Par ailleurs, il parait intéressant d'observer les spécificités de chaque typologie.

a. La régression multiple

La prime manquante est analysée en montant et en pourcentage de la prime acquise pour les garanties *First Party* et *Third Party* des captives.

Pour chacune des deux typologies de risque, une régression multiple est réalisée afin d'expliquer la prime manquante (variable quantitative Y) en fonction de p autres variables quantitatives $X_1,\ldots,X_p$ et prédire de nouvelles valeurs pour Y.

Les autres variables quantitatives utilisées dans l'analyse sont :

- Le chiffre d'affaires de l'entreprise (variable CA)
- Le nombre d'incidents cyber recensés pour l'entreprise par Cyence (Nb_Incident)
- L'exposition moyenne au risque Cyber, déterminée par les scénarios et par le degré de dépendance au système d'information de l'entreprise (variables « moyenne » et « Dep » uniquement pour le *First Party*)
- L'exposition au 99,5^{ème} percentile, déterminée par les scénarios (variable « VAR200 »)
- La fréquence globale (variable Freq) composée par les fréquences pour la perte d'exploitation et pour le vol de données

- La couverture souscrite par la captive (variable « Limite_1st » ou « Limite_3rd » et prédire de nouvelles valeurs pour Y.

L'objectif est de déterminer le meilleur modèle représentant la prime manquante.

D'un point de vue théorique celui-ci s'écrit

$$y = \beta_0 + \sum_{j=1}^{p} \beta_j \, x_j + \varepsilon$$

Avec

- y la variable à expliquer, $x_1 \dots x_p$ les variables explicatives,
- ε le terme d'erreur aléatoire du modèle et
- $\beta_0, \beta_{1, \dots} \beta_p$ les paramètres à estimer

Pour chaque i observation sur n, le modèle s'écrit

$$y_i = \beta_0 + \sum_{i=1}^{p} \beta_j \, x_{ij} + \varepsilon_i$$

Avec ∀ i = 1, ..., n ε_i i.i.d, $\mathbb{E}(\varepsilon i) = 0$, $\mathbb{V}(\varepsilon i) = \sigma^2$ et ∀ i ≠ k $Cov(\varepsilon_i , \varepsilon_k) = 0$.

Les erreurs sont centrées, leurs variances homogènes et constantes et les ε_i ne sont pas corrélés.

Pour estimer les coefficients β la méthode des moindres carrés est utilisée. Elle consiste à minimiser pour chaque observation, l'écart entre l'observation et la prévision par le modèle. Cet écart est déterminé pour toutes les observations, l'estimation de β correspond donc minimiser la somme des carrés des erreurs (résidus) soit :

$$\hat{\beta} = \min_{\beta_0 \beta_1 \dots \beta_p} \sum_{i=1}^{n} (y_i - (\beta_0 + \beta_1 \, x_{i1} + \dots + \beta_p \, x_{ip}))^2$$

En écriture matricielle

$$\hat{\beta} = \min_{\beta} \|Y - X\beta\|^2$$

Et en développant

$$\hat{\beta} = (X'X)^{-1} X'Y$$

Avec X'X inversible, ce qui est globalement le cas si n > p + 1

Il reste à estimer la variance des résidus en calculant dans un premier temps les valeurs prédites puis en calculant les résidus.

$$\hat{y}_i = \hat{\beta}_0 + \sum_{i=1}^{p} \hat{\beta}_j \, x_{ij}$$

$$e_i = y_i - \hat{y}_i$$

L'estimateur de la variabilité résiduelle $\sigma^2 = \frac{\sum_i (Y_i - \widehat{Y_i})^2}{n-p-1}$ avec $\mathbb{E}(\sigma^2) = \hat{\sigma}^2$ estimateur est sans biais

La variabilité totale des y est décomposée entre une variabilité dûe au modèle et à une variabilité résiduelle.

$$\underbrace{\sum_i (y_i - \bar{y})^2}_{} = \underbrace{\sum_i (\hat{y}_i - \bar{y})^2}_{} + \underbrace{\sum_i (y_i - \hat{y}_i)^2}_{}$$

Variabilité	Totale	Modèle	Résiduelle
Degré de Liberté	n -1	p	n – p – 1
Carré moyen	$\frac{SCM}{p}$	$\frac{SCR}{n-p-1}$	

Avec *SCM* Somme des Carrés du modèles et *SCR* Somme des carrés des résidus

i. Test Global

Afin de décider si le modèle est significatif, les hypothèses suivantes sont testées

- $H_0 : \beta_j = 0 \; \forall \; j = 1 \ldots p$
- H_1 Il existe j = 1 … p tel que $\beta_j \neq 0$

Il existe au moins un β_j différent de 0 grâce auquel le modèle devient intéressant donc significatif. Le rejet de H_0 entraine que le modèle est significatif.

Un test de Fisher est réalisé avec la statistique du test suivante

$$F_{obs} = \frac{SCM/p}{SCR/(n-p-1)}$$

Loi de la statistique du test :

- Sous H_0, F_{obs} suit une loi de Fisher $\mathcal{F}_{n-p-1}^{p}$
- Si $F_{obs} > \mathcal{F}_{n-p-1}^{p}\,(1-\alpha)$ alors rejet de H_0 au seuil α

Avec le logiciel R, le test de Fisher est réalisé directement la p-value (probabilité critique du modèle) est calculée et la décision est prise pour un seuil de 5%

ii. Test sur chaque β

Pour tester quels sont les coefficients β à retenir, il faut tester chaque β_j séparément.

La loi de $\widehat{\beta}_j$ est une loi normale $\mathcal{N}\,(\beta_j\,, {\sigma_{\widehat{\beta}_j}}^2)$ et la loi de $\frac{\widehat{\beta}_j - \beta_j}{\sigma_{\widehat{\beta}_j}}$ est une loi normale centrée réduite mais $\sigma_{\widehat{\beta}_j}$ est la vraie valeur de l'écart type de de $\hat{\beta}_j$.

En remplaçant $\sigma_{\hat{\beta}_j}$ par $\hat{\sigma}_{\hat{\beta}_j}$ la loi $\mathcal{L}$ ($\frac{\hat{\beta}_j - \beta_j}{\hat{\sigma}_{\hat{\beta}_j}}$) devient une loi de Student T_{n-p-1}

Les hypothèses du test sont donc :

- H_0 : $\beta_j = 0$ contre
- H_1 : $\beta_j \neq 0$

Sous H_0 la variable j n'apporte pas d'information supplémentaire intéressante sachant que les autres variables sont déjà dans le modèle.

La statistique du test $T_{obs} = \frac{\hat{\beta}_j}{\hat{\sigma}_{\hat{\beta}_j}}$ est réalisé par le logiciel R sachant que les valeurs généralement prises par le test T_{obs} sont comprises entre -2 et 2 au seuil de 5%.

- Si $|T_{obs}| > t_{n-p-1}\left(1 - {}^{\alpha}/_{2}\right)$ alors rejet de H_0 au seuil $\alpha = 5\%$

b. Courbe de marché

Une « courbe de marché » représentant les « primes manquantes » est construite. Elle doit comparer les primes obtenues pour le risque Cyber aux couvertures prises en compte dans la tarification. Les coordonnées sont déterminées de la façon suivante :

- **L'abscisse** va représenter un point de la couverture à tarifer. Elle est déterminée par le calcul du *Thirdpoint* ramené au chiffre d'affaires de l'entreprise. Cette valeur relative permet de tenir compte de l'étendue de la couverture par rapport à sa taille.

  Le *Thirdpoint* correspond au point représentant le premier tiers de la couverture, il vaut donc :

  $$Thirdpoint = Rétention + \frac{Garantie}{3}$$

  A noter que le chiffre d'affaires est en milliers d'euros afin de faciliter la lecture sur le graphe.

- **L'ordonnée** va représenter le prix de la couverture à tarifer en fonction de la capacité achetée. Cette valeur correspond au *Rate On Line (ROL).*

3. ANALYSE DES RESULTATS

a. Risque lié au Dommage – First Party

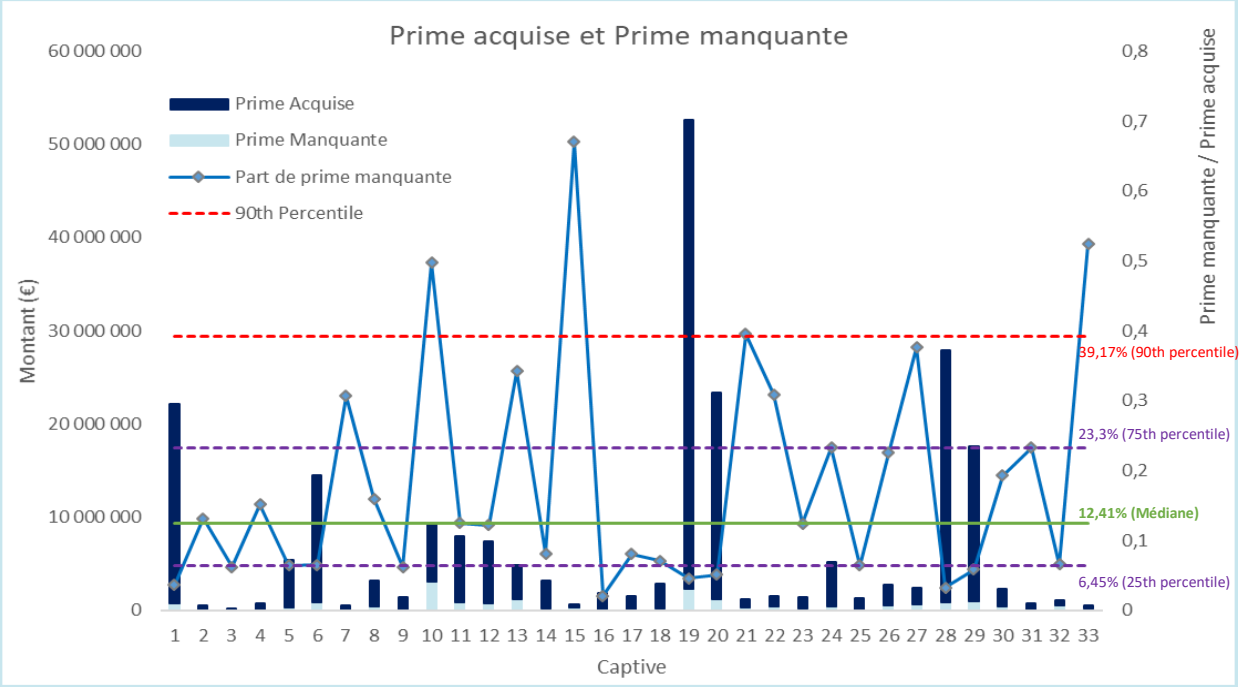
i. Graphe descriptif

L'observation des pourcentages de prime manquante par rapport à la prime acquise pour couvrir le programme souscrit par la captive est reporté dans le graphe ci-dessous.

Pour 25% des captives le manque de prime est inférieur à 6,23% alors qu'il est supérieur à 21,5% pour le dernier quart. La médiane se situe à 10,53% et pour 10% des captives le manque de prime est supérieur à 37,24%.

Le modèle produit un effet non négligeable de manque de prime sur les polices *First Party* pour près de la moitié des captives. Il s'agit majoritairement de captives dont la prime acquise pour les garanties *First party* est relativement faible. Le graphe de l'annexe N propose le même graphique avec les captives dont les primes acquises en *First Party* sont inférieures à 5m€.

Même si les conséquences de ce résultat ne sont pas particulièrement impactantes sur la prime, elles démontrent qu'avec encore beaucoup d'incertitudes sur le modèle de tarification du risque Cyber, certaines captives pourraient se retrouver en difficulté si un sinistre cyber venait impacter leur programme First Party.



Graphe II.E.5 – Prime acquise et prime manquante pour le First Party

ii. Résultat de la régression

Avec le logiciel R, nous réalisons la régression multiple calibrée sur les 33 programmes précédents.
La variable qualitative Activity_Cyence est renommée en Activity et rendue quantitative de la façon suivante :

- Secteur 1 - Agriculture & Mining
- Secteur 2 – Financial Institutions
- Secteur 3 – Manufacturing
- Secteur 4 – Services
- Secteur 5 – Trade
- Secteur 6 – Utilities

Le meilleur modèle semble être le modèle où la prime manquante est fonction de l'écart type de la moyenne de l'exposition, du pourcentage de dépendance de l'entreprise à ses systèmes d'information, du Cyence Score et de la capacité achetée par la captive pour ses garanties *First Party*.

Coefficients:

	Estimate	Std. Error	t value	Pr(>|t|)
(Intercept)	-7.857e+0	4.616e+05	-0.170	0.866061
SD	1.148e-02	2.563e-03	4.479	0.000115 ***
Dep	-1.174e+06	3.553e+05	-3.305	0.002606 **
Cyence	3.172e+03	1.167e+03	2.719	0.011126 *
Limite_1st	3.199e-02	4.404e-03	7.264	6.58e-08 ***

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 287700 on 28 degrees of freedom
Multiple R-squared: 0.8342, Adjusted R-squared: 0.8105
F-statistic: 35.21 on 4 and 28 DF, p-value: 1.51e-10

Figure II.E.6 – Résultat de la régression de la prime manquante First party

Pour cette partie consacrée aux garanties *First party* une classification des captives après estimation de la prime manquante est réalisée avec les variables résultats obtenus ci-dessus et présentée en annexe O.

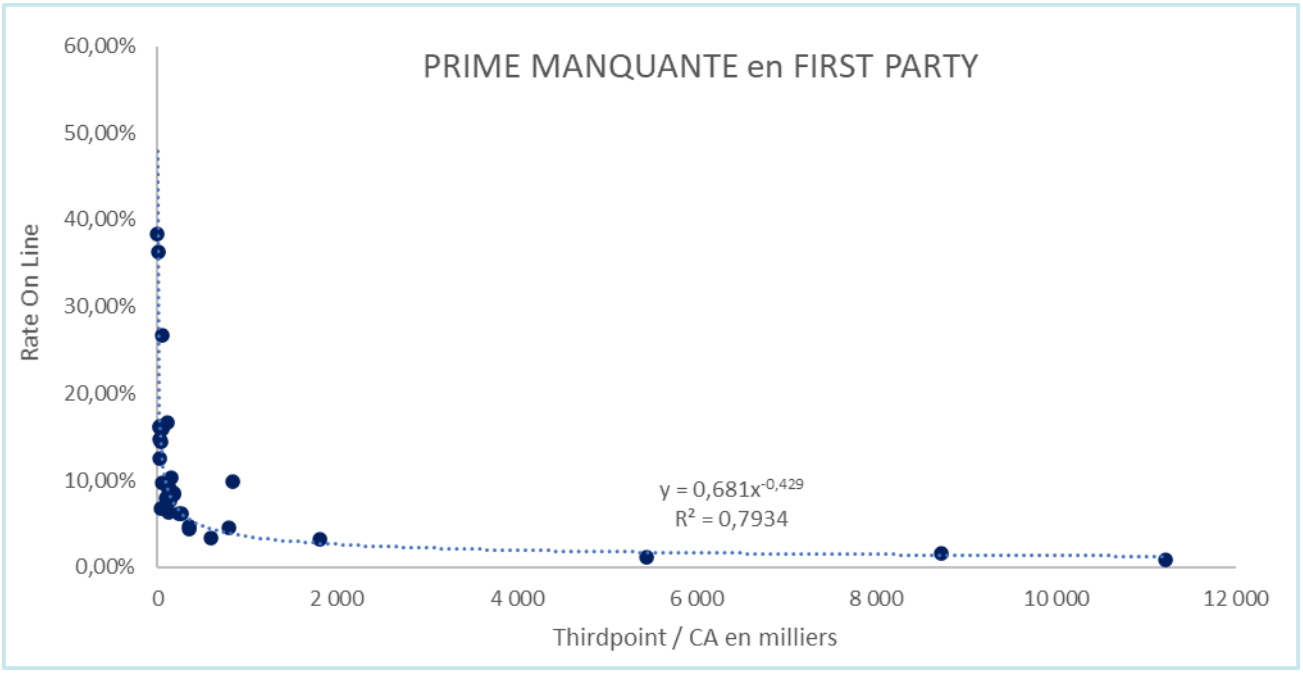
iii. Courbe de marché

Le graphe ci-dessous est construit avec la méthodologie expliquée dans le paragraphe E.2.b. Une tendance se dessine avec l'ajustement d'une courbe de forme « puissance ».

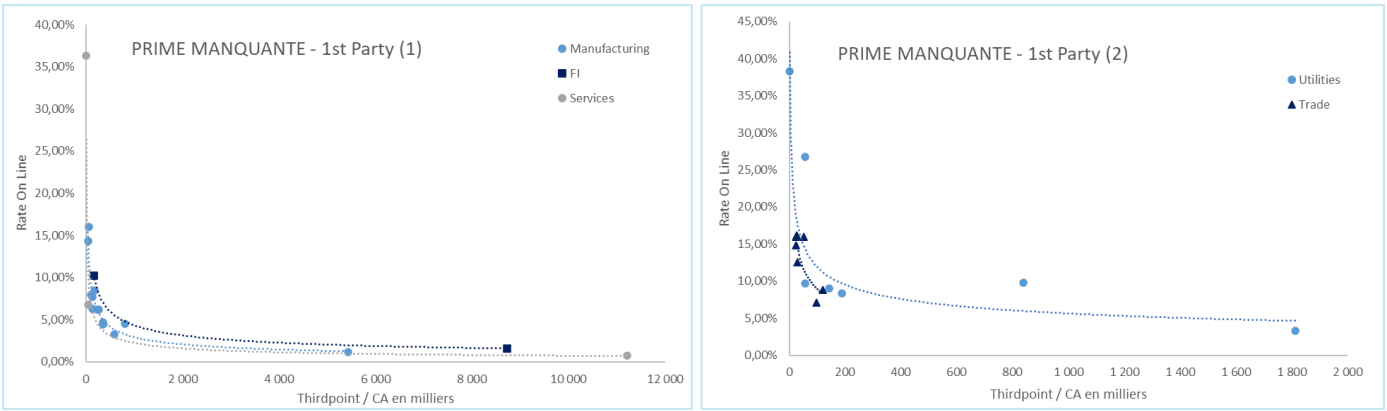
Cette courbe permet de déterminer une valeur « moyenne » de la prime manquante. Elle peut être utilisée quelle que soit la couverture et le secteur d'activités de l'entreprise.

Les courbes de la figure II.E.8 tiennent compte, quant à elles des secteurs d'activités des captives. Pour gagner en clarté visuelle, elles sont construites selon les valeurs de « Thirdpoint / CA en milliers » car pour trois secteurs (Manufacturing, Services et Financial Institutions) ces valeurs peuvent être élevées.

Certains secteurs ne possèdent pas d'échantillon suffisant pour ajuster une courbe de tendance à part entière (Financial services).



Graphe II.E.7 – Courbe de marché globale pour le First Party

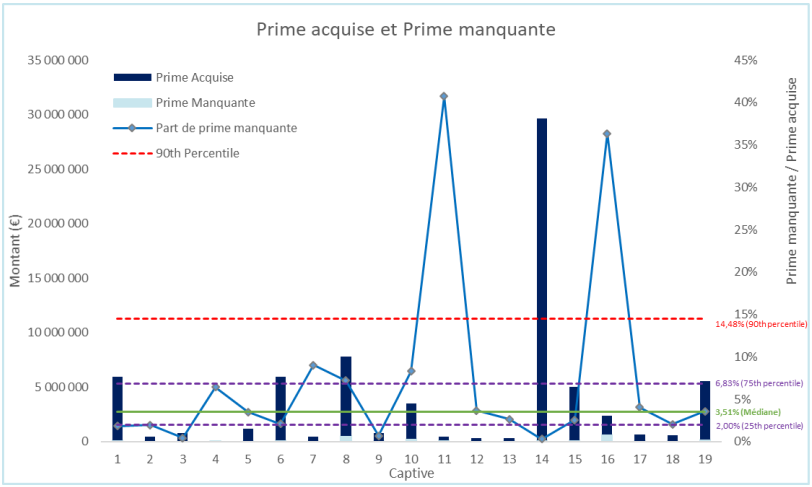


Graphes II.E.8 – Courbe de marché par secteur d'activité

b. Risque lié au Risque de Tiers – *Third Party*

i. Graphe descriptif

Comme pour le risque « dommage » l'observation des pourcentages de prime manquante par rapport à la prime acquise pour couvrir le programme souscrit par la captive est reporté dans le graphe ci-dessous.



Pour 75% des captives le manque de prime est inférieur à 6,83%, ce qui parait très faible. Seule deux captives ont une prime manquante supérieure à 10% de la prime souscrite en responsabilité civile par la captive. Celles-ci ont un nombre de données de cartes de paiement important.

L'impact du modèle sur le risque de tiers n'est pas suffisamment significatif.

Graphe II.E.9 – Prime acquise et prime manquante pour le Third Party

ii. Résultat de la régression

Avec le logiciel R, nous réalisons la régression multiple telle que décrite plus haut.
La variable qualitative Activity_Cyence est renommée en Activity et rendue quantitative de la façon suivante. Pour le risque de tiers, seuls 4 secteurs d'activités sont représentés. Il s'agit :

- Secteur 1 – Financial Institutions
- Secteur 2 – Manufacturing
- Secteur 3 – Trade
- Secteur 4 – Utilities

Le meilleur modèle semble être un modèle à 3 variables explicatives où la prime manquante est fonction de la moyenne de l'exposition, du nombre d'incidents passés subis par l'entreprise et de la capacité achetée par la captive pour ses garanties *Third Party*.
Etonnamment, le nombre de données de cartes de paiement ne constitue pas une variable de ce modèle optimum. Elle est néanmoins la quatrième variable explicative puisqu'avec les variables citées ci-dessus elle fait partie du meilleur modèle à 4 variables.

Coefficients:

	Estimate	Std. Error	t value	Pr(>|t|)
(Intercept)	-2.497e+04	2.060e+04	-1.212	0.244170
Limite_Third	8.020e-03	1.910e-03	4.199	0.000774 ***
Incident	5.503e+04	1.125e+04	4.891	0.000196 ***
Moyenne	2.095e-01	3.818e-02	5.487	6.26e-05 ***

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 62130 on 15 degrees of freedom
Multiple R-squared: 0.8965, Adjusted R-squared: 0.8759
F-statistic: 43.33 on 3 and 15 DF, p-value: 1.261e-07

Figure II.E.10 – Résultats de la régression sur la prime manquante

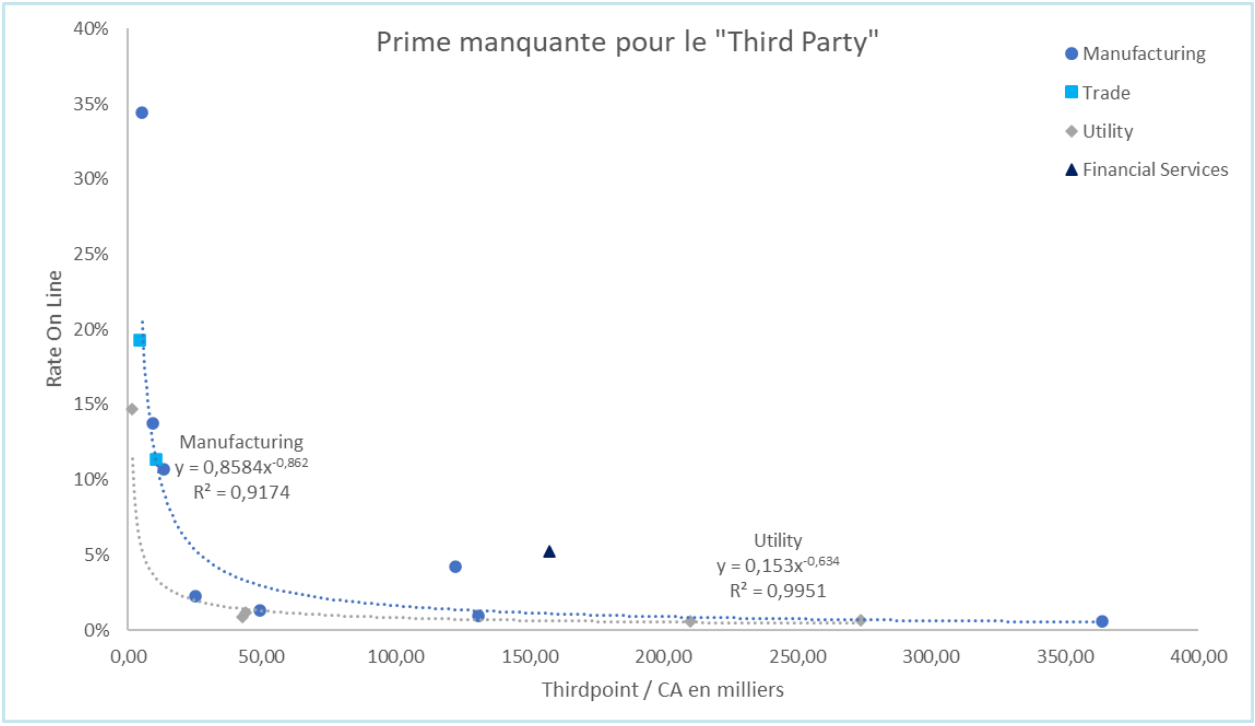
iii. Courbe de marché

Comme pour le *First Party*, une courbe de marché pour les garanties liées au risque de tiers - *Third Party* est construite. Une tendance se dessine avec l'ajustement d'une courbe de forme « puissance ».

Cette courbe permet de déterminer une valeur « moyenne » de la prime manquante. Elle peut être utilisée quelle que soit la couverture et le secteur d'activités de l'entreprise.

Le secteur du « Manufacturing » et des « Utilities » qui regroupent respectivement 8 et 5 entreprises semblent relativement bien s'ajuster, mais l'échantillon reste relativement faible pour donner une conclusion sur la représentativité de cette courbe. Elle permet néanmoins de dégager une idée des ROL et donc des prix applicables.

Les deux captives du secteur du commerce « Trade » s'ajustent sur la courbe du « Manufacturing ».



Graphe II.E.11 – Courbe de marché Third Party

A. LE RISQUE CYBER SOUS SOLVABILITE 2

Pour compléter cette étude, et aller plus loin dans les réflexions concernant le risque Cyber dans les captives, il semblait important de donner quelques pistes de réflexion sur Solvabilité 2.

Le risque cyber peut avoir des effets importants sur la solvabilité de la captive car les sinistres, comme Target ou Not-Petya peuvent être des sinistres d'intensité.

L'objectif de cette partie consiste à proposer quelques pistes d'orientation sur le calcul du SCR (Solvency Capitale Requirement) CAT afin de mieux prendre en compte le cyber.

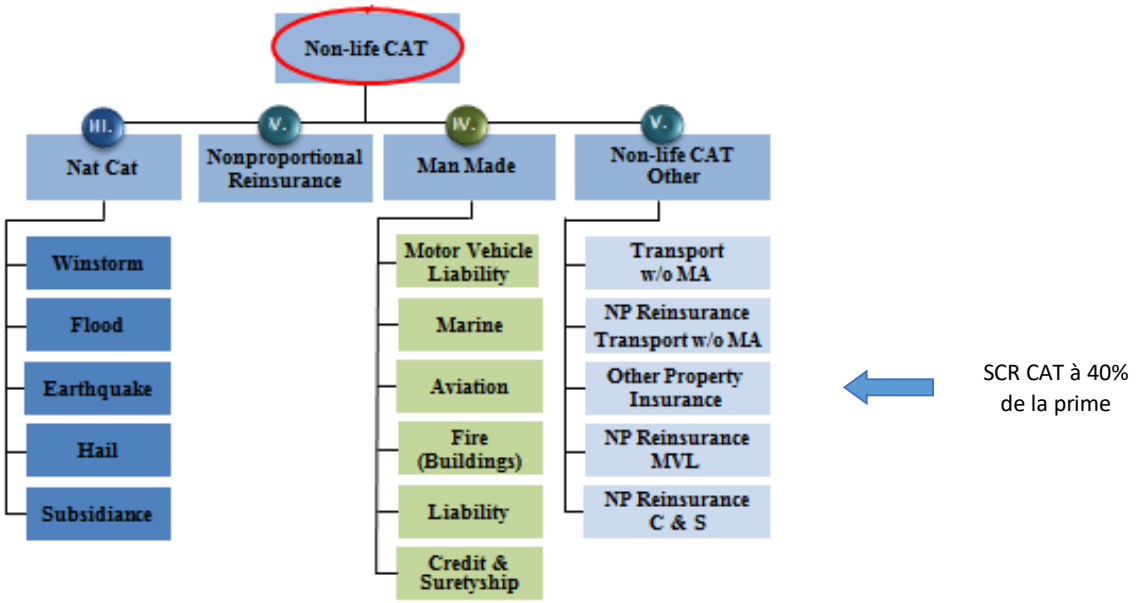


Figure III.A.1 – Modules du calcul du SCR CAT Non Vie

Aujourd'hui, pour les captives qui souscrivent du risque Cyber, le risque est classé dans la LoB des « pertes pécuniaires diverses ». La grande majorité des captives étudiées couvrent la tranche « travaillante » des programmes d'assurance et de réassurance des entreprises. Il s'agit de tranches dont la franchise est généralement faible (quelques milliers d'euros) et retenue par les entreprises et leurs filiales. De ce fait, les programmes souscrits par la captive sont considérés comme des traités proportionnels. Pour cette LoB, le SCR CAT de la formule standard est calculé en utilisant le sous-module « *Other Property Insurance* ».

Dans ce sous-module, le risque CAT est basé sur un pourcentage de 40% de la prime, ce qui semble relativement faible compte-tenu de la « dangerosité » du risque Cyber. En effet, l'étude a montré que la prime n'est, à ce jour pas forcément bien appréhendée et ce risque peut être sous-estimé.

B. PROPOSITIONS DE CALCUL DU SCR CAT CYBER

Nous proposons de réaliser plusieurs types de modifications de la Formule Standard afin de mieux appréhender le risque Cyber.

Le sous module SCR CAT Non-Vie se calcule de la manière suivante :

$$\text{SCR } CAT_{Non-Vie} = \sqrt{(SCR_{natCat} + SCR_{np\ dommage})^2 + SCR^2_{man\ made} + SCR^2_{Other}}$$

Le SCR_{natCat} est nul dans le cadre de cette étude, le calcul du $SCR_{non\ vie}$est simplifié.

Le $SCR_{man\ made}$ est calculé pour chaque branche (Motor, Marine, Aviation, Incendie, RC et Crédit). Dans le cas de cette étude, seule la branche RC est concernée et les coefficients ci-dessous sont appliqués directement sur les primes en fonction des catégories de garanties.

- RC Pro – 100%
- RC générale – 100%
- Et le non proportionnel – 210%

La partie « Dommage » est renseignée avec le SCR_{Other}. C'est le calcul de ce SCR qui implique que la prime soit considérée à 40%.

1. FORMULE STANDARD

Le calcul du $SCR\ CAT_{non\ vie}$ est réalisé selon la méthodologie de la Formule Standard, pour les captives qui ne souscrivent pas de Cyber.

La prime pour la partie du risque « Dommage » est considérée à 40% de la prime estimée, celle pour la partie « Risque de tiers » est prise selon les pourcentages ci-dessus. Dans la majorité des cas, les couvertures sont considérées comme des protections RC générales cédées sous forme de traités proportionnels. Des traités non-proportionnels existent mais uniquement pour 4 captives qui les rétrocèdent entièrement. De ce fait, le choc appliqué à la tranche non-proportionnelle est répercuté pour tenir compte du risque de « mitigation » et le net pour les excess devient nul.

2. CORRECTION DU MODULE MAN MADE

Deux corrections à la Formule Standard sont proposées :

a. Les primes « dommage » et « risque de Tiers » sont considérées à 40% dans le module « Other CAT» ; Cette méthode est nommée « SCR Other revu »
b. Le choc du sous-module « Other CAT » est porté à 100% au lieu de 40%, ceci implique que les primes des deux parties « Dommage » et « Risque de Tiers » sont considérées à 100%. Cette méthode est nommée « SCR Man Made revu ».

3. MODELE INTERNE PARTIEL AVEC LE 99,5EME PERCENTILE

Une vision plus conservatrice est également étudiée.

En effet, le SCR est calibré pour correspondre aux fonds propres nécessaires à l'assureur pour faire face à ses engagements à un horizon un an avec un seuil de confiance de 99,5%.

Lors de la tarification, les simulations réalisées ont permis de déterminer pour chacun des programmes le sinistre correspondant au 99,5ème percentile.

De ce fait, les valeurs obtenues pour ce niveau de percentile sont utilisées pour calculer le $SCR\ CAT_{non\ vie}$ avec cette méthode nommée « MIP ». Les valeurs du 99,5ème percentile sont globalement plus élevées que la prime issue de la tarification, dans la mesure où cette prime est déterminée en tenant compte de la moyenne de la charge des sinistres augmentée d'un coefficient de sécurité basé sur l'écart-type de cette charge autour de la moyenne.

D'un point de vue global nous constatons que le 99,5ème percentile correspond souvent à la capacité souscrite par la captive pour le programme considéré. Ceci semble logique puisque le 99,5ème percentile correspond à un sinistre dont la période de retour est de 200 ans.

C. RESULTATS

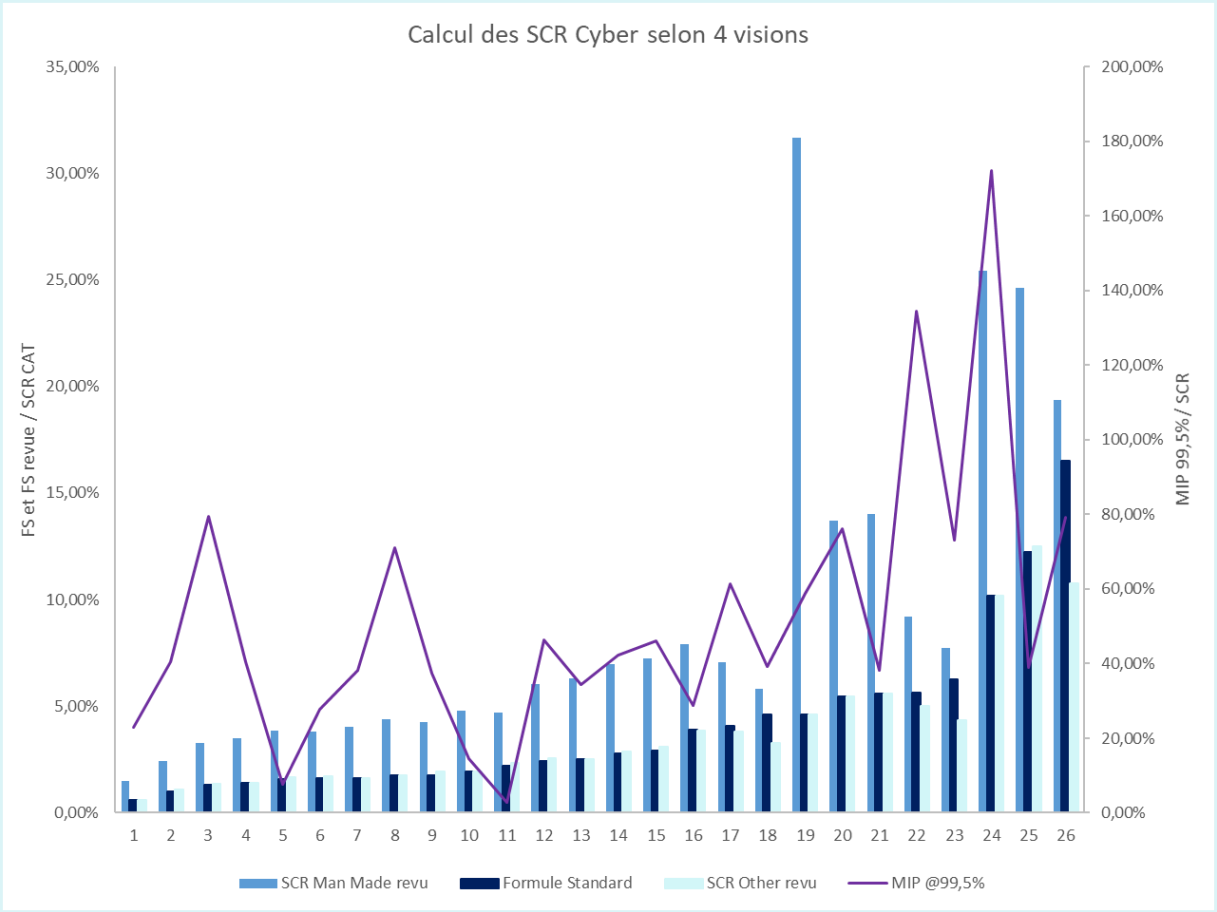
Le graphe ci-dessous récapitule les résultats obtenus pour les différentes captives. Il compare les méthodes « Formule standard », « SCR Man Made revu » et « SCR Other revu » au $SCR\ CAT_{non\ vie}$ déterminé pour chacune des captives lors de la publication des calculs réglementaires en 2020.

3 captives présentent un « SCR CAT cyber » selon la formule standard supérieur à 20% du $SCR\ CAT_{non\ vie}$ calculé. L'impact des méthodes utilisées restent faibles sur l'estimation d'un SCR Cyber.

Le graphe est construit avec les captives dont le SCR Cyber calculé selon la Formule Standard est inférieur à 20% du $SCR\ CAT_{non\ vie}$ publié. Les captives sont classées dans l'ordre croissant de ce $SCR\ CAT_{non\ vie}$. Cette approche permet de visualiser pour chacune des captives considérée, les résultats des autres méthodes de calcul.

A noter que le « MIP » fait apparaitre logiquement des SCR Cyber beaucoup plus élevés. Ceux-ci sont comparés au SCR global publié par la captive et non plus au $SCR\ CAT_{non\ vie}$ uniquement.

Le « SCR Man Made revu » est globalement et logiquement plus important que le SCR Formule Standard. Le « SCR Other revu » est en ligne avec celui de la « Formule Standard » à quelques exceptions près.



Graphe II.C.1 – Comparaison des méthodes de calcul du SCR CAT Cyber

Globalement, Le « SCR Man Made revu » pour le risque cyber correspond au double du SCR relatif au risque cyber calculé avec la Formule Standard. En revanche, le SCR qui utilise le « MIP » a un impact pouvant aller jusqu'au doublement du SCR global.

CONCLUSION

Considéré comme l'un des risques majeurs par de nombreuses organisations, le risque cyber est encore mal maitrisé par les différents acteurs de la chaine assurantielle.

Son apprentissage est difficile à appréhender car c'est un risque qui concentre plusieurs problématiques. Il peut être étendu géographiquement, les entreprises affectées ne souhaitent généralement pas communiquer à son sujet, il est évolutif puisque les hackers débordent d'imagination pour trouver de nouvelles typologies d'attaque, il est potentiellement couvert par des polices traditionnelles qui n'ont pas été tarifées pour le prendre en compte. Tous ces éléments constituent un frein au développement des couvertures assurantielles.

Les entreprises souhaitent néanmoins trouver des protections pour garantir les sinistres qu'elles pourraient subir et utilisent quand elles en ont, leurs sociétés d'assurance captives, dans lesquelles elles centralisent l'information pour participer à l'apprentissage du risque.

L'étude réalisée dans le cadre de ce mémoire apporte des éléments permettant d'aider à la gestion du risque cyber grâce aux captives et dans les captives, avec le développement de quelques « outils » permettant de mieux le cerner et le quantifier. L'idée était de pallier le manque de données historiques en utilisant des scénarios simulés à l'aide de générateurs. Ces derniers constituent une base de données suffisante qui permet ensuite d'utiliser des « méthodes » classiques de modélisation. Parmi celles-ci, nous pouvons citer les modèles fréquence – sévérité ou la construction de courbes de marché pour la tarification, les régressions pour expliquer certains résultats, la construction de courbe d'exposition etc.

Dans l'échantillon de 55 entreprises qui possèdent une captive, les approches suivantes ont donc développées :

- **L'analyse de l'exposition** des entreprises à la perte d'exploitation et à la violation des données déterminée par la construction de courbes déclinées par secteur d'activité. Les pertes éventuelles moyennes par période de retour jusqu'à 200 ans sont mesurées en pourcentage soit du chiffre d'affaires soit du nombre de données renseignées afin de pouvoir comparer les entreprises entre elles.
- **La tarification** des programmes cyber souscrits par les captives, pour donner une indication des primes à transférer en ayant bien conscience des limites du modèle. Pour la majorité des captives étudiées, les primes transférées aujourd'hui semblent insuffisantes que ce soit sur la base du modèle avec les scénarios (10 entreprises sur 14) ou du modèle avec le benchmark (12 sur 14). Les insuffisances de primes peuvent atteindre jusqu'à 60% avec une moyenne de 20% pour le modèle avec le benchmark.
- De cette tarification est dérivée une **courbe de** marché qui permet l'estimation d'une première indication de cette prime à transférer dans la captive pour un programme donné.
- **L'estimation** du cyber dit « silencieux » que les captives pourraient être amenées à couvrir si les programmes relatifs aux garanties dommage (*First party*) et aux risques de tiers (*Third Party*) ne l'excluaient pas. En effet, les scénarios générés sont décomposés selon ces deux typologies de

risque. Le risque de tiers semble peu important lors de décomposition sauf dans le cas de la violation des cartes de paiement. De ce fait, les résultats sur les programmes de type « responsabilité civile » semblent peu significatifs. La prime médiane « manquante » relative reste faible à 3,5% et représente moins de 15% dans 90% des cas. De plus, seules 19 captives (sur les 55 de l'échantillon) souscrivent des programmes couvrant du risque de tiers (responsabilité civile). A l'inverse 32 captives souscrivent des programmes « dommage » et la prime manquante est évaluée à plus de 12,4% pour la moitié d'entre elles.

- **L'évolution du calcul du SCR CAT Non-Vie.** Le calcul avec la formule standard actuelle semble peu adapté à la « dangerosité » du risque cyber et des pistes d'amélioration sont proposées comme le développement d'un Modèle Interne Partiel « MIP » qui considère le 99,5^{ème} percentile de la courbe de distribution simulée lors de la tarification des programmes *First Party* et *Third Party*. La conséquence doit être étudiée de façon raisonnée, car elle peut entrainer un doublement voire plus du SCR global de la captive. Le calcul du SCR CAT Non-Vie en ajustant la partie « Man Made » double déjà l'impact du cyber sur le SCR CAT Non-Vie.

Bien qu'apportant un complément non-négligeable pour les entreprises dans le cadre de leur gestion des risques, les modèles développés présentent plusieurs limites. La première réside dans le fait que le risque cyber est évolutif, les modèles sous-jacents à la génération des scénarios doivent être revus régulièrement. De plus, la modélisation n'est possible que pour la perte d'exploitation et la violation de données. Or il existe d'autres types de risque qui engendrent de nombreux impacts intangibles comme le risque de réputation ou les coûts indirects (chute des ventes, perte de clientèle, baisse de valorisation de l'entreprise sur les marchés, etc.) qui ne peuvent pas être considérées comme des garanties assurables mais que les clients aimeraient couvrir.

Par ailleurs, les primes obtenues avec l'utilisation du benchmark sont un peu plus élevées que celle estimées avec les scénarios alors même que peu de sinistres sont encore disponibles. Le graphique I.C.2 qui décrit le sinistre Not-Petya montre d'ailleurs que ce dernier a été indemnisé uniquement pour 30% de sa valeur et sur ces 30% seulement 10% au titre des polices dédiées.

Ceci laisse à penser que non seulement les polices dédiées actuelles sont loin d'être satisfaisantes pour les clients mais que les tarifications sont également loin d'être à la hauteur du risque potentiel, auquel il faut également rajouter le manque de maîtrise des expositions « silencieuses ».

L'étude du risque cyber en est donc à ces prémices et de nombreuses analyses devront être conduites dans le futur pour apprendre à le maîtriser, comme par exemple un approfondissement des calculs de SCR relatifs au risque cyber ou une approche des sujets concernant les intangibles.

ANNEXES

A. Les différentes typologies de programme malveillant

B. Les 10 plus importants sinistres de l'histoire

C. Les 10 plus importants sinistres de 2020

D. Cyence, définition des 8 catégories de menace

E. Expositions aux violations de données

F. Test de Student

G. Fréquence du générateur de violation de données

H. Courbes d'expositions à la perte d'exploitation selon la dépendance aux systèmes d'information

I. Classification a priori

J. Choix du seuil de sinistres graves

K. Choix du seuil de sinistres catastrophiques

L. Modélisation des programmes des captives

M. Ajustements des sinistres attritionnels et graves

N. Prime "manquante" *First Party* & prime acquise < 5 m€

O. Classification – base prime "manquante"

P. Régression linéaire pour le *Third Party*

A. LES DIFFERENTES TYPOLOGIES DE PROGRAMME MALVEILLANT

Les sous-catégories de programme malveillant (malware en anglais) sont déclinées ci-dessous. Le rançongiciel, du fait de son importance exponentielle, développée pendant la période de COVID 19, est défini plus en détail dans le corps du mémoire.

- **Rançongiciel (ransomware)** : Il s'agit d'un logiciel malveillant qui prend en otage les données dans l'attente du paiement d'une rançon. Le pirate exploite une faille pour bloquer l'accès aux données de sa victime, les contenus sont alors chiffrés totalement ou partiellement, de façon à les rendre inexploitables sans une clé de déchiffrement. Ensuite le pirate demande de verser une somme d'argent en échange de la clé qui permettra de les déchiffrer. En général, le hacker demande à être payé en cryptomonnaie, comme le Bitcoin par exemple.

- **Logiciel espion (spyware) :** Il s'agit de programmes installés pour recueillir des informations sur les utilisateurs, sur leurs habitudes de navigation ou encore sur leur ordinateur. Ces logiciels surveillent à votre insu tous vos faits et gestes et envoient ces données au(x) cyber-attaquant(s). Ils sont généralement mis en place lors du téléchargement d'une application gratuite.

- **Macro-virus :** Ces virus utilisent le langage de programmation d'un logiciel pour en altérer le fonctionnement. Lorsque le logiciel se télécharge, le macro-virus exécute ses instructions avant de laisser le contrôle à l'application en question. Ils s'attaquent principalement aux fichiers des utilisateurs et utilisatrices. Leur expansion est due au fait qu'ils s'intègrent à des fichiers très échangés et que leur programmation est moins complexe que celle des virus.

- **Virus polymorphes :** Il s'agit d'un virus informatique qui modifie sa propre représentation lors de sa réplication. Cette manœuvre empêche alors leur détection par les logiciels antivirus.

- **Virus furtifs :** Ces types de virus prennent le contrôle de certaines fonctionnalités du système pour se dissimuler. Pour ce faire, ils compromettent les logiciels de détection. Ces virus peuvent se propager de la même manière que tout autre virus, par le biais de programmes malveillants, de pièces jointes ou d'installations créées via divers sites internet.

- **Cheval de Troie :** Programme en apparence légitime, mais à vocation malveillante**.** Les cybercriminels usent de techniques dites d'ingénierie sociale pour vous inciter à charger et à exécuter ce Cheval de Troie. Pour plusieurs finalités :
  - Voler, supprimer, bloquer, modifier ou copier des contenus personnels et ou sensibles
  - Espionner,
  - Voler des mots de passe…

- **Bombe logique :** Logiciel malveillant ajouté à une application. Il s'agit de dispositifs programmés dont le déclenchement s'effectue à un moment déterminé. Ce type de virus est capable de se déclencher à un moment précis plus ou moins proche, et sur un grand nombre de machines.

  On se souvient du **virus Tchernobyl**, lancé en 1998 par un étudiant taïwanais… Ce virus était programmé pour se déclencher à la date du 13ème anniversaire de la catastrophe nucléaire, soit le 26 avril 1999. Parti de Taïwan, cette *bombe logique* est donc restée inactive pendant plus d'un an, date à laquelle celle-ci a mis hors service des milliers d'ordinateurs à travers le monde.

- **Ver :** Ce sont des logiciels malveillants qui se reproduisent sur plusieurs ordinateurs en utilisant un réseau informatique. Les *Vers* ont la capacité de se dupliquer une fois qu'ils ont été exécutés. La propagation la plus courante se fait au travers de pièces jointes d'emails.

- **Injecteurs :** Il s'agit d'un programme créé pour *injecter* un logiciel malveillant sur un système cible. Également appelé « programme seringue » ou « virus compte-gouttes ». Une fois le logiciel malveillant activé, il peut arriver que l'injecteur s'autodétruise.

B. LES 10 PLUS IMPORTANTS SINISTRES DE L'HISTOIRE

Année	Nom	Type	Conséquence	Montant / Durée	Nature	Commentaire
2010	STUXNET	Virus - ver informatique Logiciel Malveillant qui utilise la vulnérabilité pour s'introduire dans un ordinateur pour essayer de pirater tous les appareils à proximité	Infection de 30 000 ordinateurs Prise de contrôle de certaines infrastructures informatiques d'une centrale d'enrichissement d'uranium => pannes dans le parc de centrifugeuses Ralentissements / Explosions		Politique	Programme nucléaire iranien. Attaque Interétatique attribuée à Israel avec l'aide des Etats-Unis Pays touchés: Inde, Indonésie, Pakistan, Chine.
2013	TARGET	Compromission de données de carte de crédit Target, l'un des plus importants acteurs de la distribution aux USA, s'est fait subtiliser plus de 40 millions de données bancaires, auxquelles s'ajoutent 70 millions de données personnelles	Perte de chiffre d'affaires / Atteinte à la réputation Montant des sommes dérobées aux clients des magasins est une inconnue – seuls ceux qui se sont identifiés dans les poursuites civiles sont connus 80 poursuites au civil et class actions ont été lancées. Licenciement du DSI, du CEO et de 7 membres du board car des défauts de prévention et de réaction ont été relevées. Plusiuers magasins ont également été contraints de fermer	* Entre le 15 novembre et le 17 décembre 2013 * Pour TARGET pertes estimées à 1 milliard de dollars en chiffre d'affaires et 34 % de baisse des profits pour la seule année 2013, et à 4,2 milliards en perte de valeur boursière.	Entreprise	Les motivations des attaquants sont purement financières. En effet, une donnée personnelle se vend sur le marché noir entre 0,25$ et 2$ environ, tandis qu'une donnée bancaire peut rapporter plusieurs dizaines de dollars. Les données de cartes de crédit ont été utilisées
2014	SONY	ver informatique équipé de 5 composants : un implant d'écoute, une backdoor, un proxy, un outil de destruction massif de disque dur et un outil de nettoyage ciblé	Annulation de la sortie de "l'interview qui tue!" une comédie sur le complot fictif de la CIA pour assassiner le leader nord-coréen Kim Jog-UN	Perte d'un investissement de 80 millions de dollars	Entreprise	Washington attribue cette attaque à Pyongyang, qui dément
2013	CYBERBUNKER	Deni de service (DDoS) Les serveurs de Spamhaus se sont vus confrontés à un nombre incalculable de connexions simultanées	Ralentissement de l'accès à internet en raison d'une brouille entre Spamhaus et Cyberbunker. Cyberbunker placé sur la liste noire de Spamhaus => cybervendetta	Flux de données stratosphériques de 300 Gbits / seconde (contre 50 pour une attaque classique)	Entreprise	Spamhaus: organisation à but non lucratif qui vise à aider les fournisseurs de courrier électronique à filtrer les spams et autres contenus indésirables. Cyberbunker est un hébergeur douteux qui de son propre aveu abritait toutes sortes de contenus "hormis pédopornographie et tout ce qui est lié au TRO.
21-oct-16	MIRAI Société DYN	Botnet créant un Deni de Service distribué de plus d'un tétraoctet par seconde frappe Dyn	10 millions d'objets connectés infectés par le malware Mirai indisponibilité des sites des clients de Dyn dont Twitter, WhatsApp, Netflix, Amazon et Paypal	Indisponibilité pendant 10 heures	Entreprise	Les hackers ont submergé Dyn de requêtes DNS (Domain Name System _ soit un service internet qyu traduit les noms de domaine en adresses IP
2016	PANAMA PAPERS	Vol de données avec Divulgation 11,5 millions de documents confidentiels issus du cabinet d'avocats Mossack Fonseca, qui aurait aidé quelques 200 000 sociétes offshore à se constituer	Atteinte à la réputation Révélation de nombreuses infractions de la part de personnalités politiques mondialement connues, provoquant une bombe autant médiatique que numérique		Politique	Cyberattaque qui a lié les mondes politiques et médiatiques
2017	WANNACRY	Virus - chiffrage des données des appareils touchés Rançongiciel	Infection de 300 000 ordinateurs fonctionnant sous Windows dans 150 pays. La France a été le 4ème pays touché avec 20 000 ordinateurs infectés Perte des données / Demande de rançon	4 jours La rançon s'élève à 4 mds $	Entreprise	Un groupe de pirates prétendait avoir piraté la NSA en dévoilant tous ses outils de l'époque. Et parmi ces outils figuraient une faille de Windows (touchant Windows 10) utilisée pour créer Wanacry Wannacry s'auto-répliquait et se propageait lui-même
2017	NOT PETYA	Rançongiciel chiffrage voire effecement des données	Pertes de données sensibles car même si la rançon était payée les données n'étaient pas restituées	300$ en bitcoin / entreprise avec un total estimé à 10 mds $	Entreprise	Virus orienté vers les Entreprises Propagation moins étendue que Wanacry Infection des ordinateurs grâce à un malware télécharger à l'insu de l'utilisateur en visitant une page Web piratée
juillet 2020	MEOW	Logiciel qui s'attaque aux serveurs mal sécurisés. Des milliers de base de données touchées avec comme victime majoritaire la société UFO qui édite un VPN (Virtual Private Network)	Nuisance aux entreprises / Perte définitive des données 3 000 base de données touchées S'apparente à une leçon pour montrer à quel point il est facile de toucher les entreprises qui négligent leur sécurité informatique		Entreprise	Introduction dans les serveurs pour accéder aux fichiers et les supprimer sans raison apparente en laissant comme message "Meow" (Miaou en anglais)
mars à décembre 2020	SOLARWINDS	Espionnage par attaque via la chaine d'approvisionnement. La chaine logistique de SolarWinds a été visée à l'aide d'une porte dérobée ("bakdoor": ie une fonctionnalité cachée grâce à laquelle les hackers ont pu installer des logiciels malveillants et mener à bien leurs opérations d'espionnage. compromission de mise à jour de la plateforme de gestion et de supervision Orion développé par la Société SolarWinds.	Nuisance aux institutions américaines (Trésor 18 000 clients et plus d'une centaine de sociétés américaines affectées. bases de données touchées S'apparente à une leçon pour montrer à quel point il est facile de toucher les entreprises qui négligent leur sécurité informatique	Difficile mais parmi les clients de SolarWinds figurent 425 des 500 entreprises américaines les plus riches (dont Microsoft)	Politique / Ministères US & Grandes Entreprises touchées Le département du Trésor affirme que l'attaque a visé "le secteur financier, des infrastructures critiques, des réseaux gouvernementaux et de nombreuses autres" victimes. Attribué à la Russie	Des pirates probablement parainés par un Etat Exploitation d'une brèche dans les infrastructures du développeurs de logiciels Solarwinds. Un code malveillant dénommé "Sunburst" a été intégré aux mises à jour de la plateforme permettant aux pirates d'accéder, une fois la mise à jour réalisée sur le matériel des organisations visées, aux systèmes niformatiques et donc de leurs données

C. LES 10 PLUS IMPORTANTS SINISTRES DE 2020

Année	Nom	Type	Conséquence	Montant / Durée	Nature	Commentaire
Avril	LEETCHI	Faille sur le CTA (Call To Action) "je participe" / Phishing	Informations personnelles des utilisateurs (Nom, prénom, date de naissance, adresse email) se sont retrouvés exposés sur la toile. => Perte de confiance des internautes		Particuliers	
	BOUYGUES Construction	Intrusion d'un ransomware dans le système d'information bloquant l'accès aux données internes	Fonctions supports paralysées (activités opérationnelles non concernées par l'attaque)=> Main mise des pirates sur des données confidentielles	Rançon de plusieurs millions de dollars	Entreprise	
Mai	EASYJET	Piratage de 9 millions de données (données clients comme des adresses emails ou des itinéraires de voyage) 2 000 informations bancaires ont été illégalement consultées.	Risque important d'hameçonnage même si la compagnie a prévenu ses clinets. => Pert de confiance de millions d'utilisateurs et plainte collective par plus de 10 000 clients	Cette attaque pourrait coûter plusieurs millions de livre à Easyjet	Entreprise	
30-janv	ESTEE LAUDER	Faille de sécurité où l'accès a été possible sans mot de passe à une base de 440 millions de données	Ralentissement de l'accès à internet en raison d'une brouille entre Spamhaus et Cyberbunker. Cyberbunker placé sur la liste noire de Spamhaus => cybervendetta		Entreprise	Spamhaus: organisation à but non lucratif qui vise à aider les fournisseurs de courrier électronique à filtrer les spams et autres contenus indésirables. Cyberbunker est un hébergeur douteux qui de son propre aveu abritait toutes sortes de contenus "hormis pédopornographie et tout ce qui est lié au TRO.
Juin	Université de Californie San Francisco	Rançongiciel paralysant tout le réseau informatique	Vol de données très sensibles	Paiement de la rançon (environ 1m€)	Université	Rapidité de réaction de l'établissement
Juin	AP HP	Attaque par Déni de Service (DDoS) qui a rendu une partie des serveurs de l'AP-HP inaccessibles a cause d'une surcharge de requêtes inutiles.	Pendant un heure, l'AP-HP a dû couper les accès aux outils internes et aux emails pour les salariés alors en télétravail.		Etablissement Public	Ce n'est pas la première fois que l'hôpital public français est victime d'une cyberattaque. En novembre dernier, l'hôpital-universitaire de Rouen avait été victime d'un ransomware.
Avril	MARRIOTT	**Cassage du mot de passe** Vol de données de 5,2 millions de clients grâce à l'utilisation des identifiants de deux employés pour accéder à l'application de fidélisation	Infection de 300 000 ordinateurs fonctionnant sous Windows dans 150 pays. La France a été le 4ème pays touché avec 20 000 ordinateurs infectés Perte des données / Demande de rançon	4 jours La rançon s'élève à 4 mds $	Entreprise	Le groupe en est à sa **deuxième cyberattaque en seulement 3 ans…** La première ayant donné lieu à une fuite de données ayant affecté **339 millions de clients**… Le groupe Marriott avait alors dû régler **une amende de 18,4 millions de livres**. Cette sanction était diligentée par le gendarme britannique de la protection des données : ICO. Ce dernier avait alors prononcé cette peine au nom de l'Union Européenne. A noter que cette cyberattaque a eu lieu en 2014 et que les contenus sensibles ont été compromises jusqu'à ce que le piratage soit détecté… en 2018 !
2017	GOOGLE	Cyberattaque DDoS (Déni de service distribuée) qui a eu lieu en 2017, mais révélée uniquement en Octobre 2020 Au plus fort du pic, le trafic est monté jusqu'à 2,5 To/seconde	Malgré son envergure inédite, cette cyberattaque n'aura pas eu d'impact.	Cyberattaque DDoS la plus importante car elle a duré 6 mois	Entreprise mais parrainée par un Etat (Chibne)	
mars à décembre 2020	SOLARWINDS & MICROSOFT	Espionnage par attaque via la chaine d'approvisionnement. La chaine logistique de SolarWinds a été visée à l'aide d'une porte dérobée ("bakdoor": ie une fonctionnalité cachée qui permet de passer inaperçu via un logiciel de confiance. Les hackers ont pu installer des logiciels malveillants et mener à bien leurs opérations d'espionnage. Compromission de mise à jour de la plateforme de gestion et de supervision Orion développé par la Société SolarWinds.	Nuisance aux institutions américaines (Département du Trésor et du Commerce américains, l'agence de l'énergie (en charge de la gestion des programmes nucléaires), ministères de l'intérieur et de la Santé 18 000 clients et plus d'une centaine de sociétés américaines affectées. bases de données touchées S'apparente à une leçon pour montrer à quel point il est facile de toucher les entreprises qui négligent leur sécurité informatique	Difficile mais parmi les clients de SolarWinds figurent 425 des 500 entreprises américaines les plus riches (dont Microsoft)	Politique / Ministères US & Grandes Entreprises touchées Le département du Trésor affirme que l'attaque a visé "le secteur financier, des infrastructures critiques, des réseaux gouvernementaux et de nombreuses autres" victimes. Attribué à la Russie	Des pirates probablement parainés par un Etat Exploitation d'une brèche dans les infrastructures du développeurs de logiciels Solarwinds. Un code malveillant dénommé "Sunburst" a été intégré aux mises à jour de la plateforme permettant aux pirates d'accéder, une fois la mise à jour réalisée sur le matériel des organisations visées, aux systèmes niformatiques et donc de leurs données
Septembre	HOPITAL DE DE DÜSSELDORF	Attaque par logiciel malveillant de type « rançongiciel », qui avait bloqué son infrastructure informatique ne laissant au service hospitalier aucun accès aux données médicales des patients.	L'hôpital s'est vu dans l'obligation de transférer des malades vers d'autres hôpitaux de la région, et c'est dans l'ambulance qu'une patiente en état critique n'a pas survécu.	Les pirates ont accepté de fournir des clefs de déchiffrement	Université / Hôpital	Première cyber attaque mortelle en Allemagne Les hackers s'en seraient pris "par erreur" à la clinique - Ils croyaient viser l'Université de la ville.

D. CYENCE - DEFINITION DES 8 CATEGORIES DE MENACES

Les 8 catégories de menace relevées par **Cyence** lors de l'analyse des sources de données des différentes organisations analysées

1. **Bad activity / Mauvaise activité**

Fait référence à la présence et à la durée d'une activité malveillante détectée dans les systèmes de l'entreprise. Une mauvaise activité remontant au réseau de l'entreprise indique généralement une hygiène de sécurité inférieure aux normes ou un réseau infecté / compromis.

2. **Dark web**

Fait référence aux sites Web et aux forums du Deep Web qui ne sont pas accessibles par les navigateurs Web et les moteurs de recherche traditionnels, et qui sont généralement utilisés par les pirates comme un marché clandestin et des sites de discussion pour l'échange de données volées ou de renseignements et services criminels.

Le Dark Web est une ressource populaire utilisée par les acteurs malveillants, leur fournissant les dernières informations sur les innovations de piratage et les vulnérabilités de sécurité. L'activité sur le Dark Web liée à une entreprise montre généralement des preuves d'intérêt de la part des pirates informatiques et pourrait indiquer qu'une violation s'est déjà produite ou qu'il y a une probabilité accrue d'une violation à venir.

3. **Technologie**

Relatif à la technologie matérielle et logicielle attribuée au réseau de l'entreprise. Les technologies qui composent le réseau de l'entreprise peuvent refléter la complexité de ses systèmes, l'exposition générale aux menaces et aux vulnérabilités, ainsi que la sophistication et la posture du personnel informatique de l'entreprise.

4. **Infrastructure**

Caractéristiques techniques des configurations réseau et serveur de l'entreprise. La conception, la configuration et les performances du site Web peuvent refléter la sophistication informatique et la posture de sécurité globale de l'entreprise.

5. **Organisation Interne**

Mesure des systèmes internes, des activités, des politiques et des comportements adoptés par l'administration de l'entreprise. La façon dont une organisation est gérée affecte la conduite, l'efficacité et la fiabilité de son capital humain, qui est un élément essentiel de la défense contre les cyberattaques.

6. **Présence externe**

Mesure de l'opinion, de l'attitude et de l'attrait du public ou d'un tiers à l'égard d'une organisation. Une présence publique omniprésente ou une réputation défavorable peut exposer une entreprise à un risque accru d'être la cible d'une attaque.

7. Périmètre de sécurité

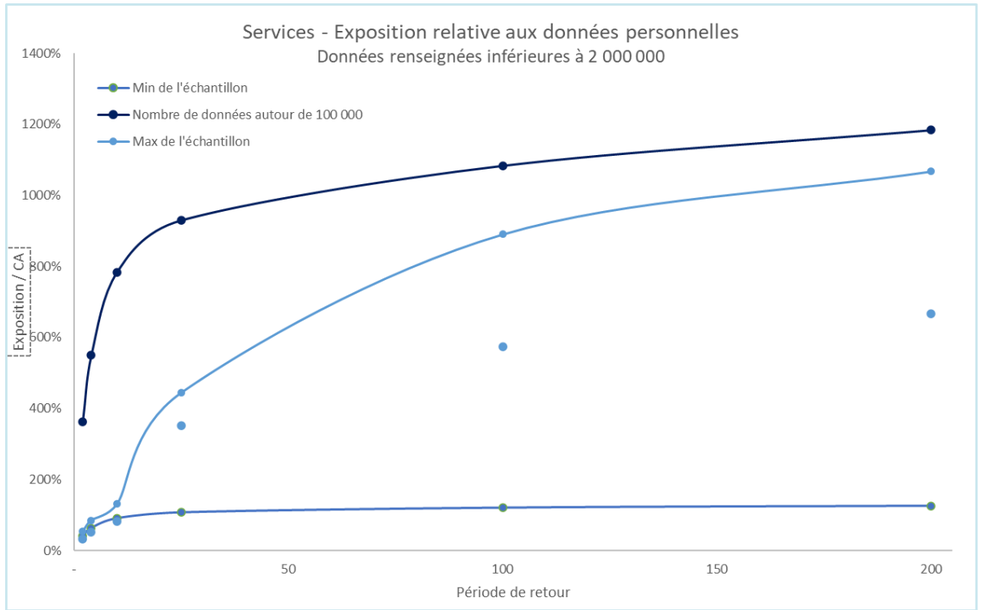
Indicateurs de réseau externes qui reflètent la surface d'attaque de l'entreprise et son exposition aux cyber-risques. Le risque d'une entreprise augmente avec le nombre de vecteurs d'attaque et de vulnérabilités exploitables présents dans le réseau. Les vulnérabilités sur les systèmes Internet de l'entreprise peuvent permettre l'accès à d'autres parties du réseau. Le périmètre de sécurité qui constitue la première couche de défense du réseau d'une entreprise, peut également indiquer l'hygiène de sécurité globale et la force des cyberdéfenses

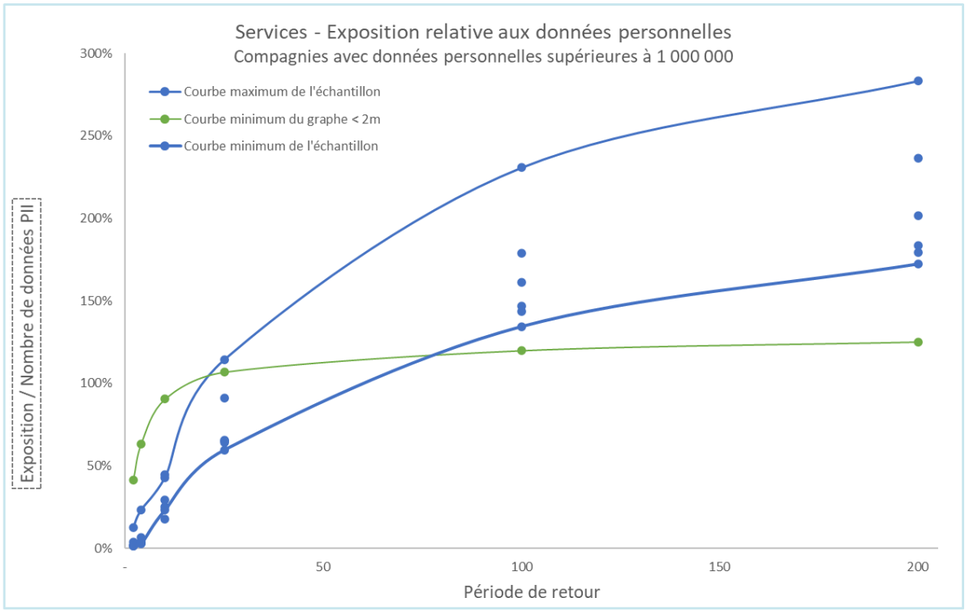
8. Incidents de sécurité

Résumé des événements de sécurité divulgués qui se sont produits au cours des deux dernières années. Les incidents de sécurité passés peuvent refléter l'exposition générale d'une entreprise aux cyber-risques.

E. EXPOSITIONS AUX VIOLATIONS DE DONNEES

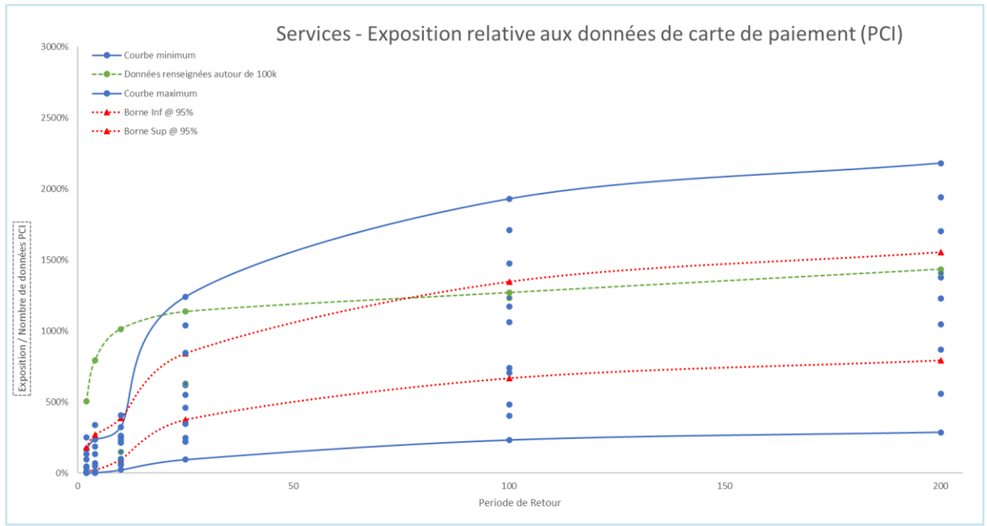
SECTEUR DES SERVICES - PII





2 analyses sont proposées pour les données PII (données personnelles) pour le secteur des services, car les données renseignées sont très disparates selon les compagnies, puisqu'elles s'échelonnent de 138 000 à 31,8 millions.
Un graphe présente les expositions pour des seuils différents (données renseignées inférieures à 2 millions et données personnelles supérieures à 1 million).

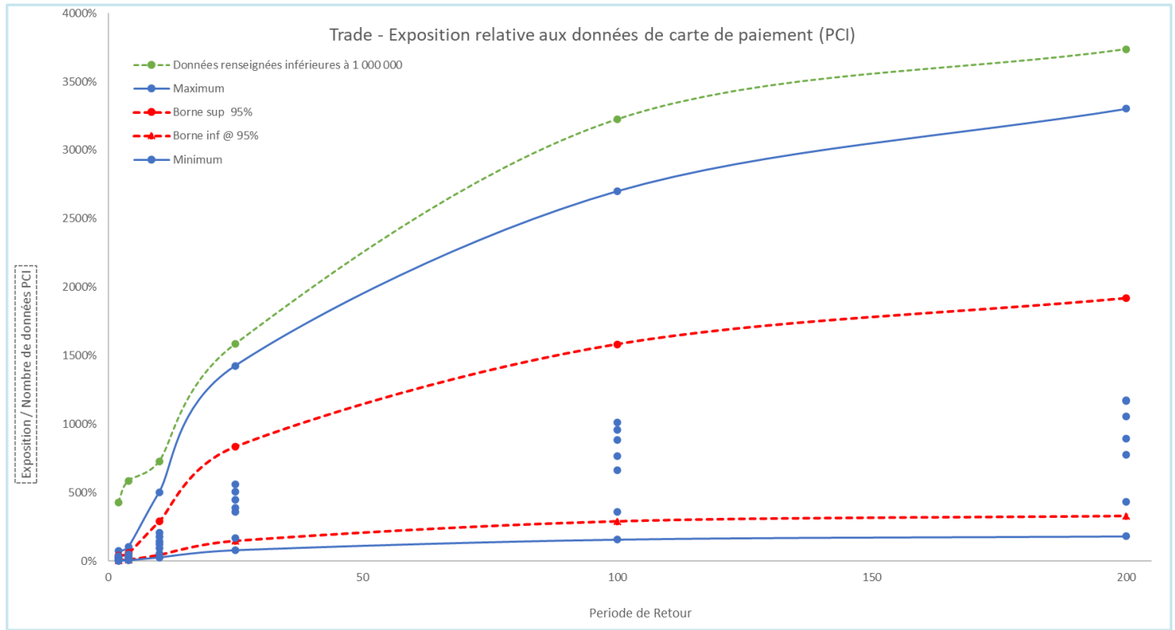
SECTEUR DES SERVICES – PCI



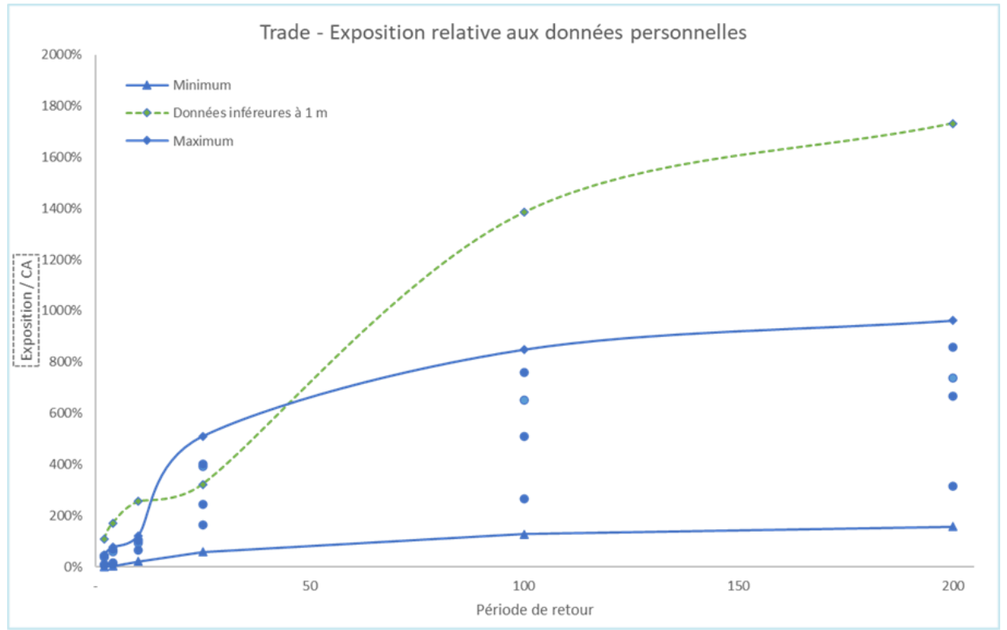
15 entreprises du secteur des Services possèdent des données de carte de paiement et leur nombre est compris entre 129 000 et 99,3 millions.
Comme pour le secteur du « Manufacturing » la courbe relative aux données autour de 100 000 est stable à partir d'une période de retour de 50 ans (courbe verte).

A noter que seules 4 entreprises ont renseignées des données sensibles, le graphique n'est donc pas exposé ici.

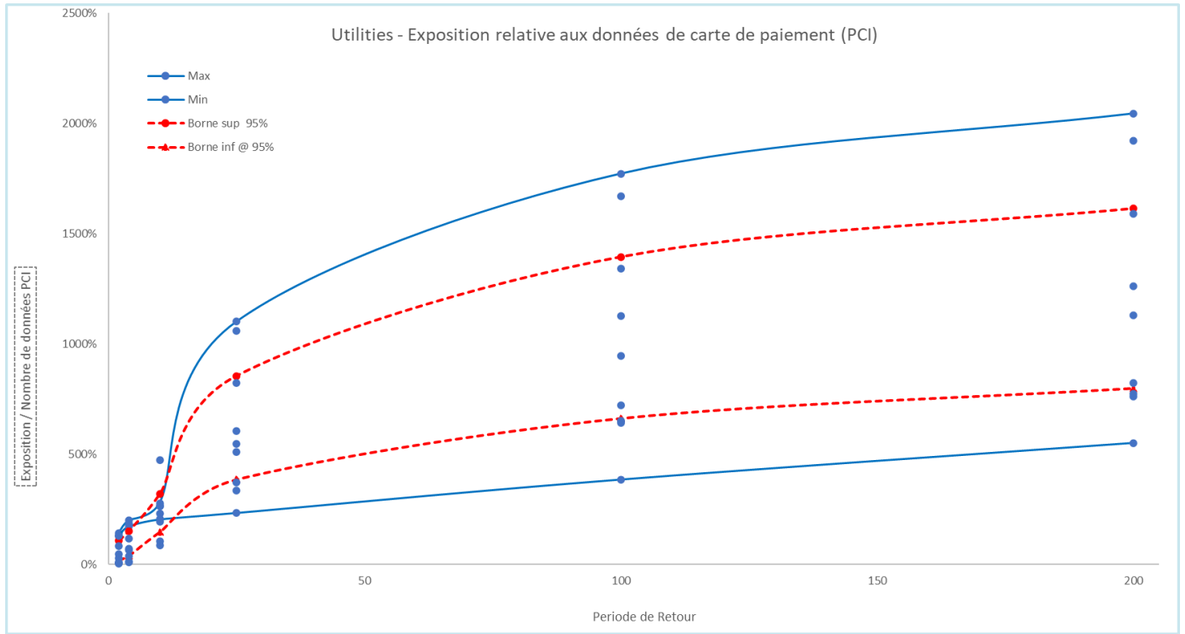
SECTEUR DU COMMERCE « TRADE » - DONNEES PCI (DONNEES DE CARTE DE PAIEMENT)



SECTEUR DU COMMERCE « TRADE » - DONNEES PII (DONNEES PERSONNELLES)



SECTEUR DES FOURNISSEURS DE SERVICES « UTILITIES » - DONNEES PCI (DONNEES DE CARTE DE PAIEMENT)



COMMENTAIRES

SECTEUR DU COMMERCE « TRADE »

- 9 entreprises du secteur du Commerce possèdent des données de carte de paiement et leur nombre est compris entre 300 566 et 200,3 millions.
- 7 entreprises possèdent des données personnelles et leur nombre est compris entre 456 000 et 35,3 millions.
- Seules 4 entreprises possèdent des données sensibles, la courbe n'est pas représentée ici.

La courbe relative aux données faibles (inférieure à 1 millions) est la courbe verte (courbe très au-dessus des autres en termes de pourcentage de l'expositions par rapport au nombre de données).

SECTEUR DES FOURNISSEURS DE SERVICES « UTILITIES »

- Seules 3 entreprises de ce secteur d'activité possèdent des données sensibles, la courbe n'est pas représentée.
- De même seules 4 entreprises ont renseigné des sonnées personnelles, la courbe n'est pas représentée.
- 9 entreprises possèdent des données de carte de paiement et leur nombre est compris entre 923 780 et 63,5 millions.

F. TEST DE STUDENT

Soient X_1, …, X_n, n variables aléatoires mutuellement indépendantes et distribuées suivant une même loi normale d'espérance μ et de variance σ^2 qui correspondent à un échantillon de taille n.

Soit $\bar{X}$ la moyenne empirique ou estimateur ponctuel de l'espérance et S^2, l'estimateur sans biais de la variance.

Soit α un risque entre 0 et 1

$$P\left(-t_{\alpha/2}^{n-1} < \frac{\bar{X}-\mu}{S/\sqrt{n}} < t_{\alpha/2}^{n-1}\right) = 1 - \alpha$$

L'intervalle de confiance bilatéral de μ au niveau de confiance $1 - \alpha$ est donné par

$$\left[\bar{X} - t_{\alpha/2}^{n-1}\frac{S}{\sqrt{n}} ; \bar{X} + t_{\alpha/2}^{n-1}\frac{S}{\sqrt{n}}\right]$$

Avec t_γ^k le quantile d'ordre $1-\gamma$ de la loi de Student à k degrés de liberté et qui vérifie

$P\left(T \leq t_\gamma^k\right) = 1 - \gamma$ avec T suit une loi de Student à k degrés de liberté.

G. FREQUENCE DU GENERATEUR DE VIOLATION DES DONNEES

A partir des données renseignées dans le générateur de scénarios relatif aux violations de données, nous utilisons le logiciel R pour déterminer les variations de la fréquence par rapport aux données d'entrée. Pour ce faire, nous réalisons une régression linéaire multiple avec les données :

- CA : chiffre d'affaires,
- Nb_Pers : Nombre de données (PCI, PII, PHI) totales
- Cyence : Cyence Score
- Breach : Nombre d'incidents passés
- Activity : Secteur d'activité - Variable qualitative convertie en variable quantitative

```
Lm (formula = Frequence ~ CA + Nb_Pers + Cyence + Breach + Activity, data = FreqPriv)
```

Coefficients:

(Intercept)	CA	Nb_Pers	Cyence	Breach	Activity
-2.594e-02	2.224e-06	-4.942e-12	1.500e-04	1.033e-02	1.305e-03

Residuals:

Min	1Q	Median	3Q	Max
-0.194956	-0.020013	0.005313	0.027269	0.099390

Coefficients:

	Estimate	Std. Error	t value	Pr(>|t|)
(Intercept)	-2.594e-02	5.529e-02	-0.469	0.641
CA	2.224e-06	3.198e-07	6.955	7.78e-09 ***
Nb_Pers	-4.942e-12	2.260e-10	-0.022	0.983
Cyence	1.500e-04	1.636e-04	0.917	0.364
Breach	1.033e-02	2.377e-03	4.344	7.02e-05 ***
Activity	1.305e-03	5.827e-03	0.224	0.824

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
Residual standard error: 0.05604 on 49 degrees of freedom
Multiple R-squared: 0.7668, Adjusted R-squared: 0.743
F-statistic: 32.22 on 5 and 49 DF, p-value: 2.171e-14

Vif :

CA	Nb_Pers	Cyence	Breach	Activity
1.573172	1.331498	1.305506	1.479608	1.078120

P-value = 0 donc on rejette l'hypothèse de nullité des coefficients, le modèle est globalement significatif. Toutes les VIF sont inférieures à 10

On cherche le meilleur modèle qui décrit la fréquence

```
modelT = RegBest (y=FreqPriv[,1], x=FreqPriv[,-1], nbest=1)
modelT$summary
```

	R2	P-value
Model with 1 variable	0.6518799	9.602119e-14
Model with 2 variables	0.7624173	5.904536e-17
Model with 3 variables	0.7665585	3.938386e-16
Model with 4 variables	0.7667950	3.148826e-15
Model with 5 variables	0.7667973	2.171283e-14

```
modelT$best
lm(formula = as.formula(as.character(formul)), data = don)
```

Residuals:

Min	1Q	Median	3Q	Max
-0.194467	-0.024173	0.004951	0.029411	0.096987

Coefficients:

	Estimate	Std. Error	t value	Pr(>|t|)
(Intercept)	2.613e-02	9.443e-03	2.767	0.00782 **
CA	2.325e-06	2.834e-07	8.205	6.04e-11 ***
Breach	1.069e-02	2.173e-03	4.919	9.15e-06 ***

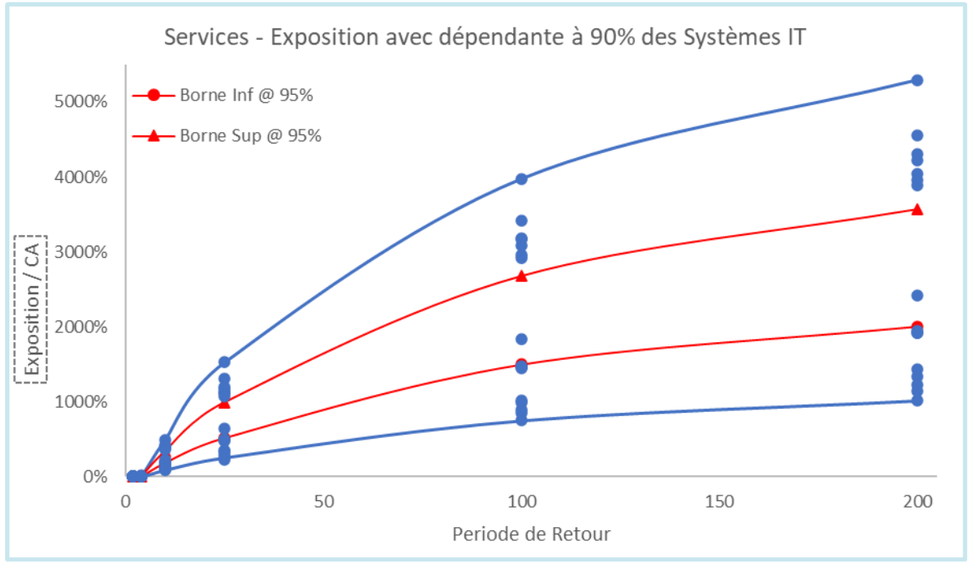
Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

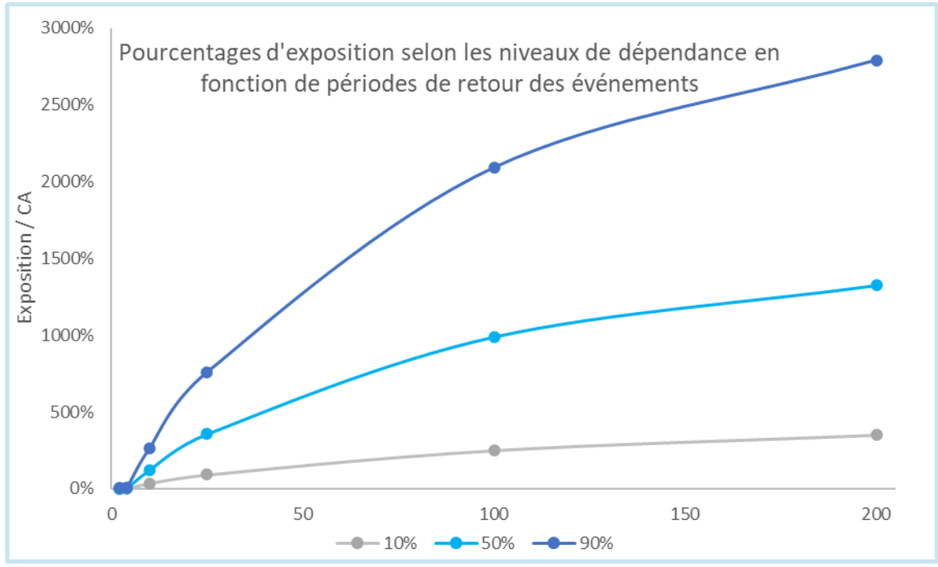
Residual standard error: 0.0549 on 52 degrees of freedom
Multiple R-squared: 0.7624, Adjusted R-squared: 0.7533
F-statistic: 83.44 on 2 and 52 DF, p-value: < 2.2e-16

La fréquence dépend principalement du chiffre d'affaires et du nombre d'incidents passés.

H. COURBE D'EXPOSITION A LA PERTE D'EXPLOITATION SELON LA DEPENDANCE AUX SYSTEMES D'INFORMATION

SECTEUR DES SERVICES « SERVICES » - PERTE D'EXPLOITATION



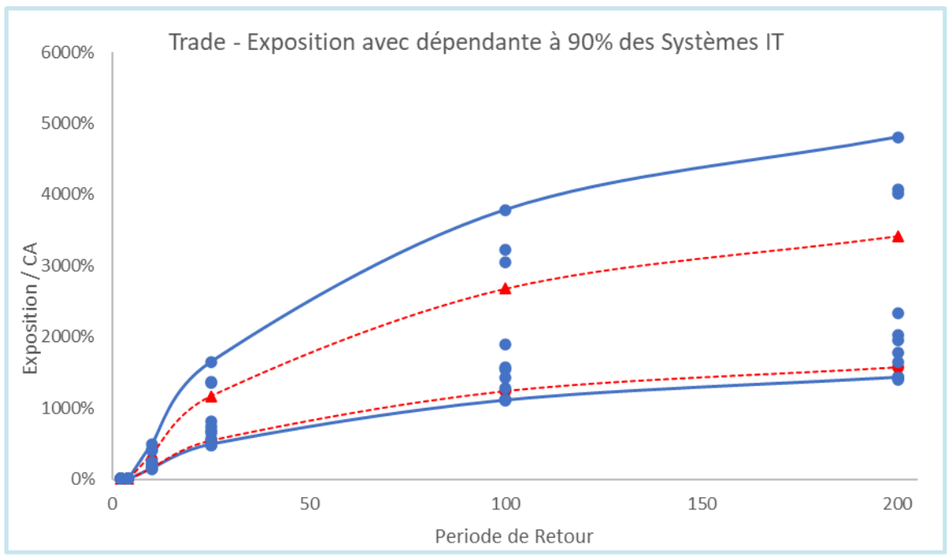


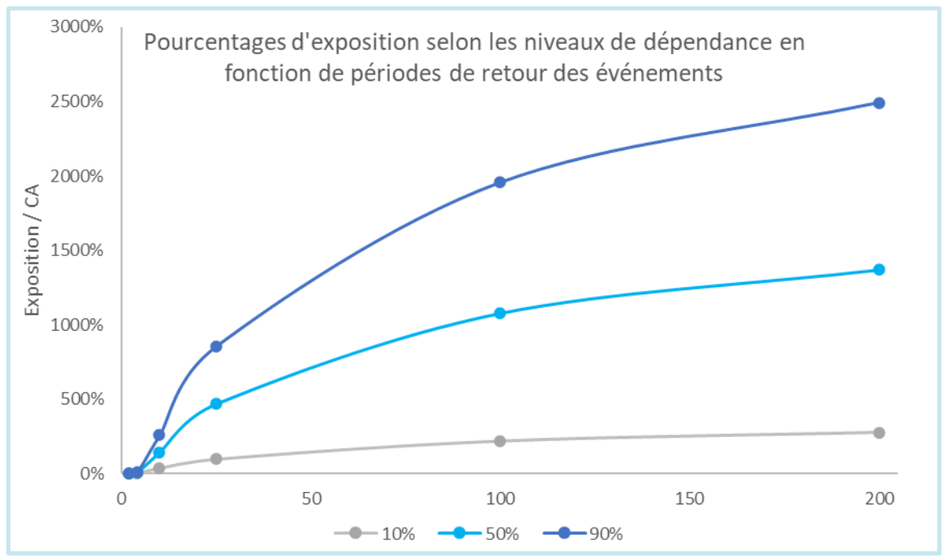
Le graphique de droite représente les courbes d'exposition moyennes pour des dépendances aux systèmes d'informations de 10%, 50% et 90%.

Le graphique de gauche détaille les courbes d'exposition aux pertes d'exploitation pour les entreprises du secteur des Services pour une dépendance à 90% des systèmes d'information.

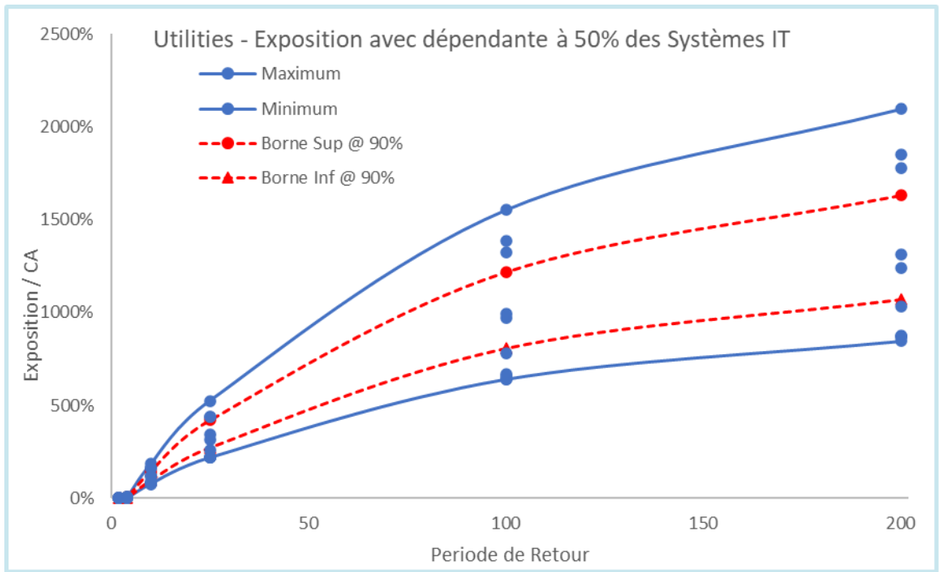
Ce niveau de dépendance constitue le niveau choisi dans la suite de l'étude pour ce secteur d'activité.

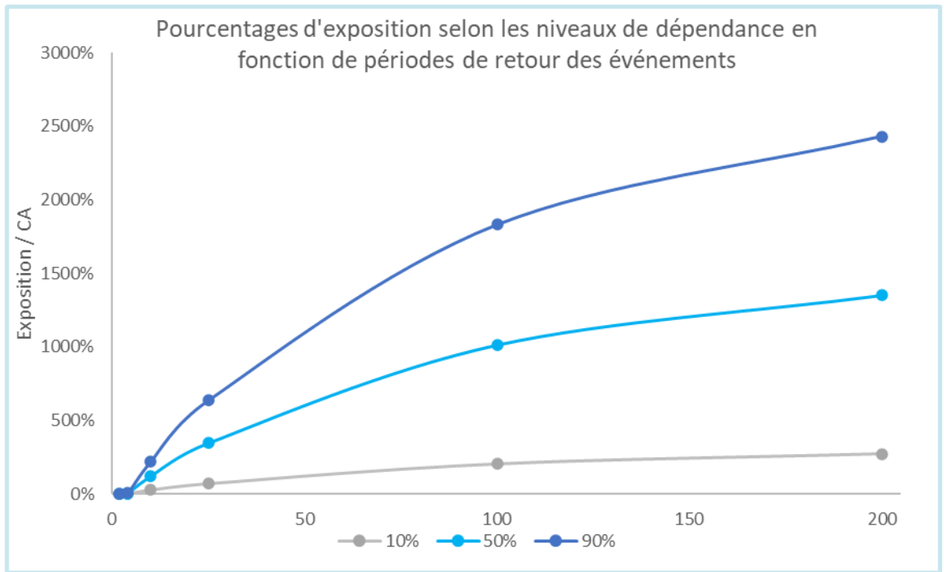
SECTEUR DU COMMERCE « TRADE » - PERTE D'EXPLOITATION



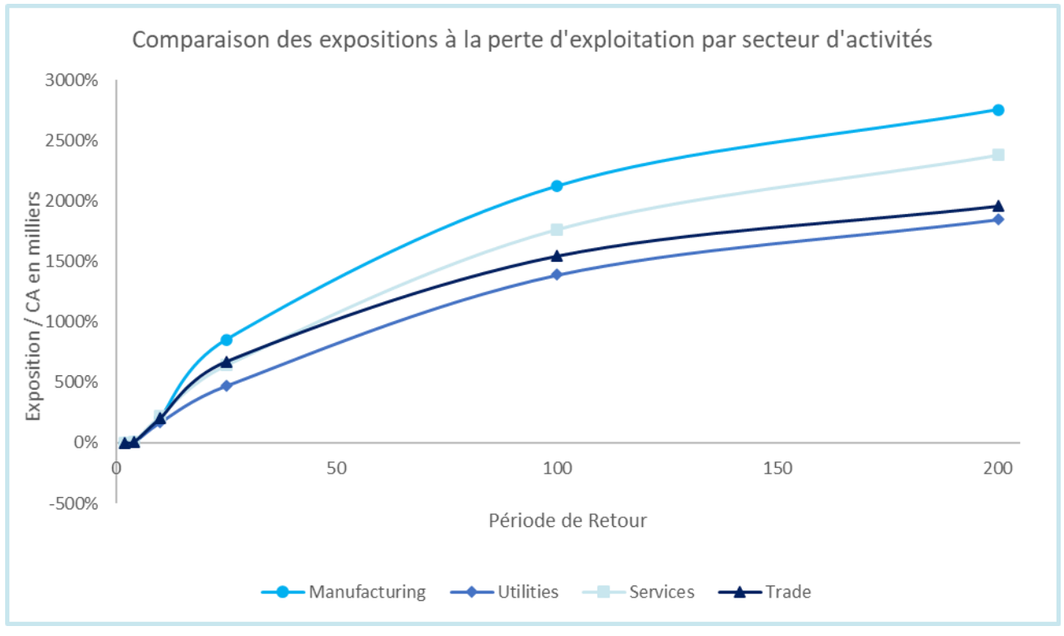


SECTEUR DES FOURNISSEURS DE SERVICES « UTILITIES » - PERTE D'EXPLOITATION





COMPARAISON DES MOYENNES DES SECTEURS D'ACTIVITES POUR UNE DEPENDANCE A 90% DES SYSTEMES INFORMATIQUES

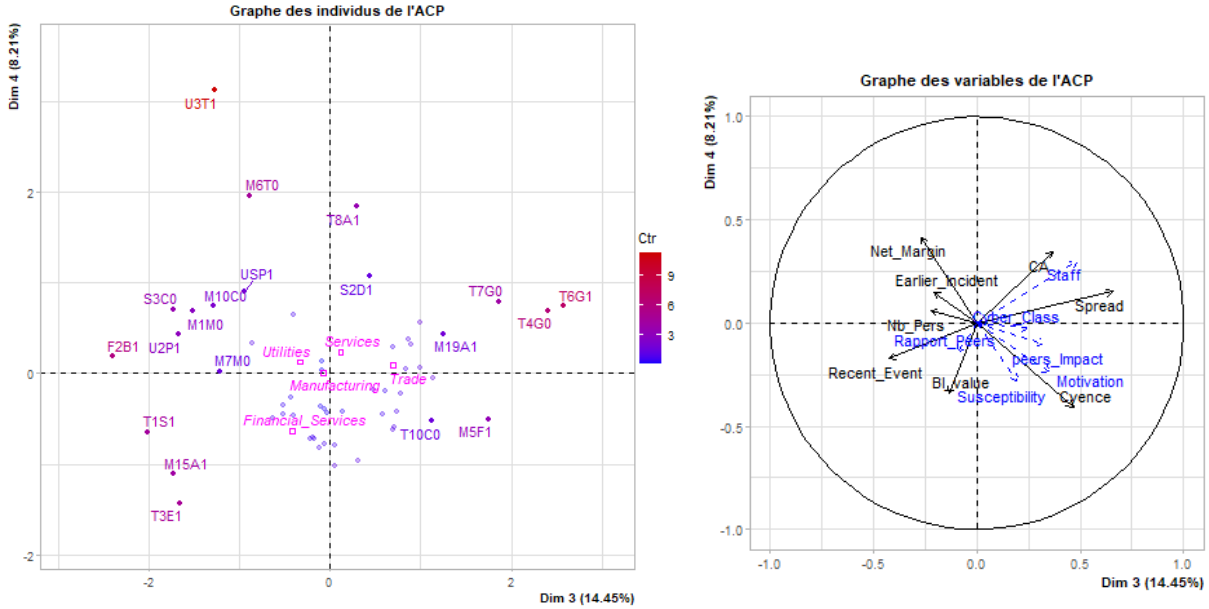


I. CLASSIFICATION *A PRIORI*

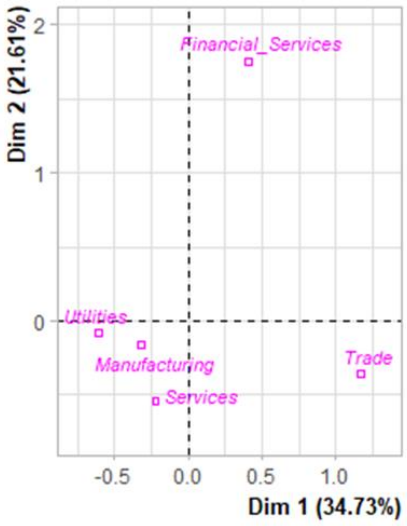
1. ANALYSE EN COMPOSANTES PRINCIPALES

a. GRAPHES SUPPLEMENTAIRES

Les informations ci-dessous complètent les analyses présentées dans le mémoire.



Graphe des individus et des variables décrivant la 3ème et 4ème dimension



Graphe des modalités de la variable qualitative supplémentaire Activity_Cyence

b. INTERPRETATION DES DIMENSIONS

La **dimension 1** oppose des individus tels que *F2B1*, *T8A1*, *S2D1* et *T1S1* (à droite du graphe, caractérisés par une coordonnée fortement positive sur l'axe) à des individus comme *U1P0*, *USP1*, *U10P1*, *U8W1* et *S3C0* (à gauche du graphe, caractérisés par une coordonnée fortement négative sur l'axe).

Le groupe auquel les individus *F2B1*, *T8A1*, *S2D1* et *T1S1* appartiennent (caractérisés par une coordonnée positive sur l'axe) partage :

- de fortes valeurs pour les variables *Recent_Event*, *Nb_Pers*, *Earlier_Incident*, *Staff*, *CA*, *Susceptibility*, *Motivation*, *Cyence* et *peers_Impact* (de la plus extrême à la moins extrême).

Le groupe auquel les individus *U1P0*, *USP1*, *U10P1*, *U8W1* et *S3C0* appartiennent (caractérisés par une coordonnée négative sur l'axe) partage :

- de faibles valeurs pour les variables *Spread*, *Cyber_Class*, *BI_value*, *Cyence*, *Motivation*, *Net_Margin* et *Nb_Pers* (de la plus extrême à la moins extrême).

La **dimension 2** oppose des individus tels que *M16C1*, *F7B0*, *F6B0*, *F4B0*, *F1B0*, *F5B1*, *F3B1*, *T10C0* et *U3T1* (en haut du graphe, caractérisés par une coordonnée fortement positive sur l'axe) à des individus comme *U1P0*, *USP1*, *U10P1*, *U8W1* et *S3C0* (en bas du graphe, caractérisés par une coordonnée fortement négative sur l'axe).

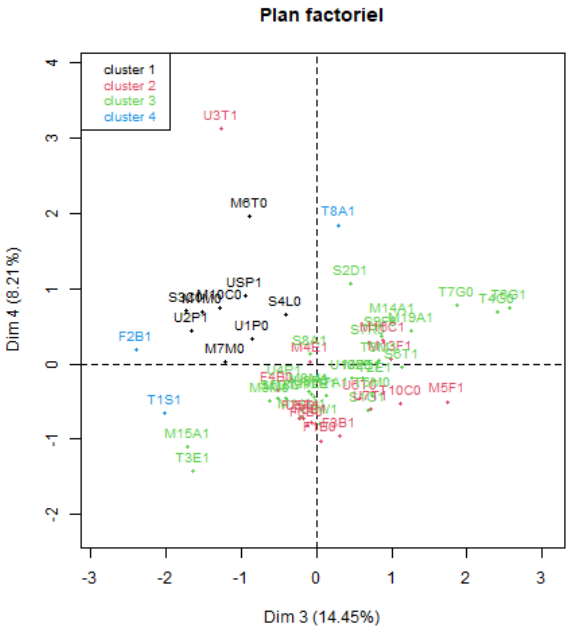
Le groupe auquel les individus *M16C1*, *F7B0*, *F6B0*, *F4B0*, *F1B0*, *F5B1*, *F3B1*, *T10C0* et *U3T1* appartiennent (caractérisés par une coordonnée positive sur l'axe) partage :

- de fortes valeurs pour les variables *Spread*, *BI_value*, *Cyber_Class* et *Net_Margin* (de la plus extrême à la moins extrême).
- de faibles valeurs pour la variable *CA*.

Le groupe auquel les individus *U1P0*, *USP1*, *U10P1*, *U8W1* et *S3C0* appartiennent (caractérisés par une coordonnée négative sur l'axe) partage :

- de faibles valeurs pour les variables *Spread*, *Cyber_Class*, *BI_value*, *Cyence*, *Motivation*, *Net_Margin* et *Nb_Pers* (de la plus extrême à la moins extrême).

2. CLASSIFICATION ASCENDANTE HIERARCHIQUE



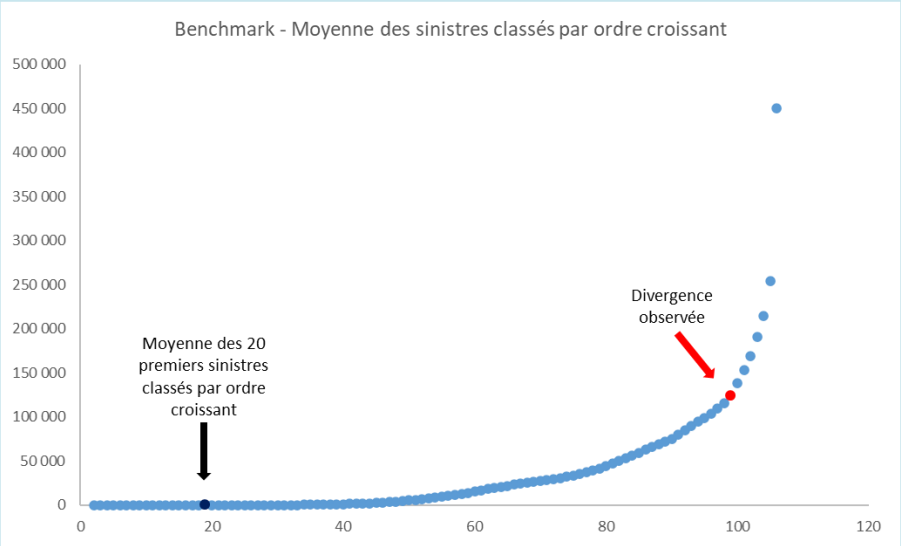
Visualisation des 4 classes selon les dimensions 3 et 4

Le plan factoriel selon les dimensions 3 et 4 séparent bien les classes « noires » et « vertes », ce qui est moins visible lors de l'interprétation selon les dimensions 1 et 2.

J. CHOIX DU SEUIL DES SINISTRES GRAVES

Pour définir le seuil des sinistres graves, le benchmark est utilisé et les sinistres sont classés par ordre décroissant. La moyenne des sinistres est calculée de façon incrémentale sur les sinistres croissants.

Le graphe ci-dessous représente les points obtenus avec ce calcul pour le benchmark européen.



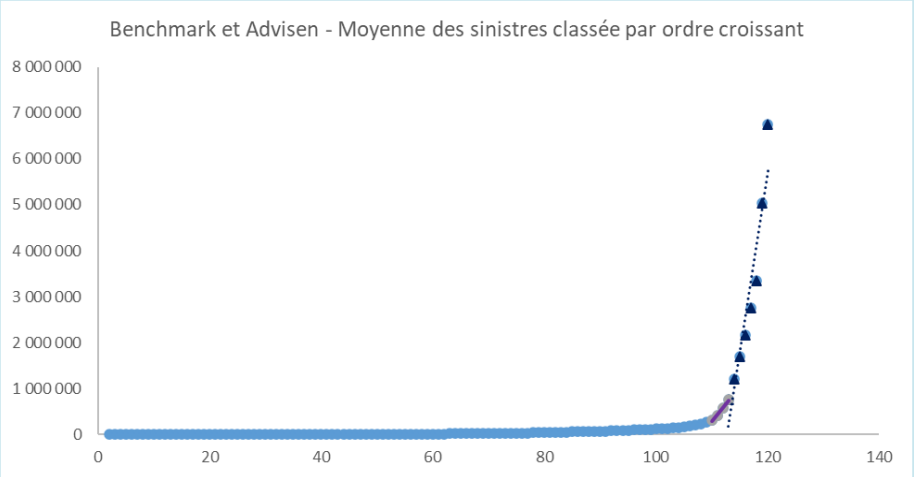
Fonctionnement

Le point d'abscisse 20 représente la moyenne des 20 premiers sinistres classés par ordre croissants.

A partir du point 99, la courbe diverge avec un changement de pente.

Ce point correspond au sinistre d'un montant de 1m€ qui est considéré comme le seuil des sinistres « graves ».

Le graphe suivant utilise en plus les sinistres Advisen du marché américain, transformé en Euros au taux de change de 20 décembre 2021.



En utilisant le benchmark de sinistres global, la courbe commence à diverger à partir du point 110 pour un sinistre de 4,8m€ puis un autre changement de pente est observé au point 113, ce qui correspond à un sinistre de 20,9m€.

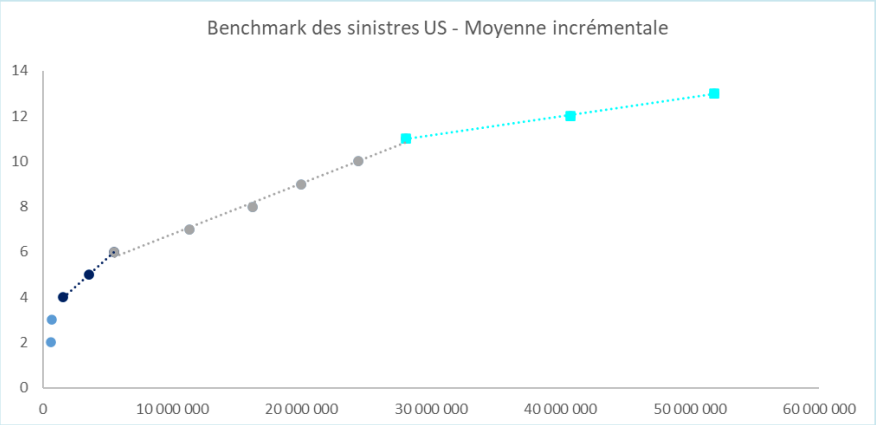
Ainsi nous pourrons considérer les triggers 1m€, 5m€ et 20m€ suivant la taille des captives.

Un sinistre de 20m€ pourra faire partie des sinistres catastrophiques pour des captives de petite taille avec une exposition au risque cyber inférieure à 20 m€.

K. CHOIX DES SEUILS DES SINISTRES CAT

Utilisation de deux méthodes :

METHODE DE LA MOYENNE INCREMENTALE



Avec la méthode précédente, les points de changement de pente sont les points dont les sinistres ont un montant de :

- 4,3 m€
- 46,3 m€
- 181 m€

METHODE DE LA PERIODE DE RETOUR

La base contient 13 sinistres US sur une période de 2002 à 2021 soit 20 ans. Le sinistre le plus important est affecté d'une période de retour de 20 ans et est défini comme le sinistre CAT.

La période de retour pourra être augmenté pour les captives dont l'exposition est inférieure à ce montant de 185 m$

Année de Sinistre	Nom de la compagnie	Montant
2002	Choicepoint Inc	15 500 000
2005	Fifth Third Bancorp	655 000
2005	The Tjx Companies Inc	64 788 000
2009	Heartland Payment Systems Inc	63 761 192
2011	Wells Fargo & Co	185 000 000
2013	Facebook Inc	11 357 600
2013	Target Corp	181 009 948
2013	Yahoo Inc	50 334 000
2014	The Home Depot Inc	46 343 818
2015	The Wendy'S Co	50 000 000
2017	Equifax Limited	657 561
2017	Sonic Corp	4 325 000
2018	Facebook Inc	645 000

L. MODELISATION DES PROGRAMMES DES CAPTIVES

Modélisation et simulation de sinistralité individuelle et annuelle

Application au programme d'assurance ou de réassurance souscrit par la captive

Simulation

Simulation des sinistres individuels

BI 90%-reliant SI	Ground up	Deductible 1	Layer 1	Market	Deductible 2	Layer 2	Market
		0	2 500 000		2 500 000	2 500 000	
Nb Loss	2	9,00%	Fréquence				
1	15 143 910	0	2 500 000	12 643 910	2 500 000	2 500 000	10 143 910
2	3 003 935	0	2 500 000	503 935	2 500 000	503 935	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0

PCI	Ground up	Deductible 1	Layer 1	Market	Deductible 2	Layer 2	Market
		0	2 500 000		2 500 000	2 500 000	
Nb Loss	0	2,00%					
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0

PHI	Ground up	Deductible 1	Layer 1	Market	Deductible 2	Layer 2	Market
		0	2 500 000		2 500 000	2 500 000	
Nb Loss	0	0,00%					
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0

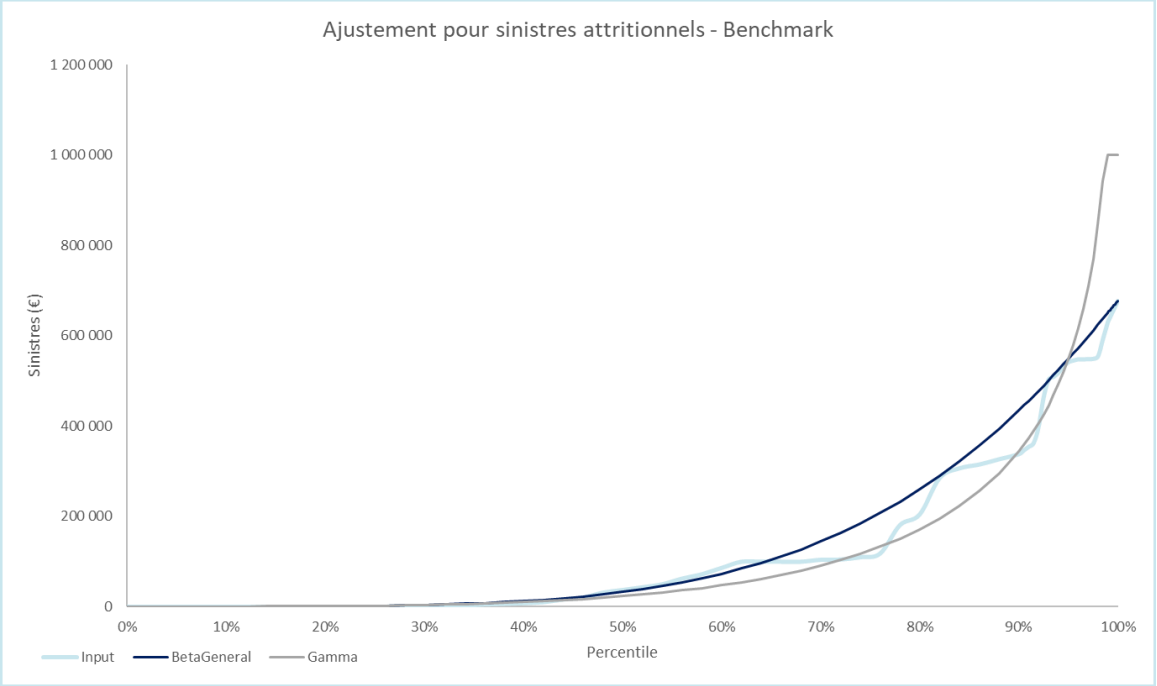
PII	Ground up	Deductible 1	Layer 1	Market	Deductible 2	Layer 2	Market
		0	2 500 000		2 500 000	2 500 000	
Nb Loss	0	1,00%					
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0

Simulation de la limite annuelle par tranche

All (AAL Limit)	Ground up	Deductible	Layer 1 occ	Market	Deductible	AAL 1	Market
		0	2 500 000			2 500 000	999 999 999
90% BI	18 147 845	0	5 000 000	13 147 845			
PCI	0	0	0	0			
PHI	0	0	0	0			
PII	0	0	0	0			
Total	18 147 845	0	5 000 000	13 147 845	0	2 500 000	18 147 845

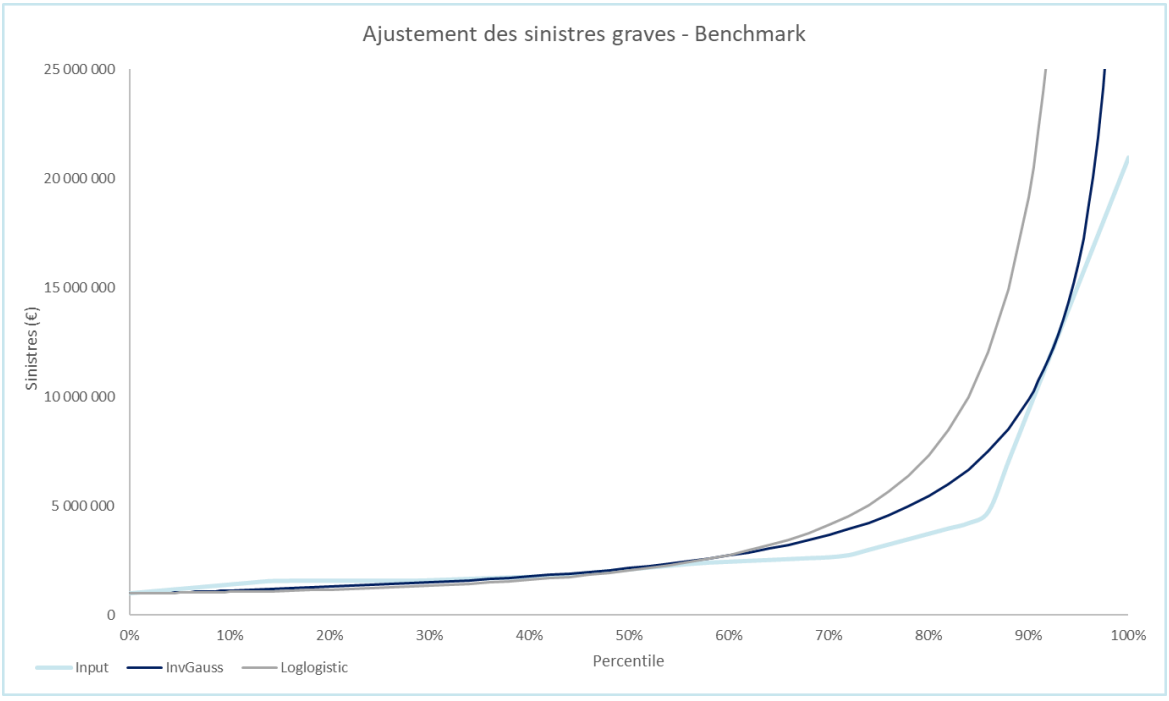
All (AAL Limit)	Ground up	Deductible 2	Layer 2 occ	Market	Deductible	AAL 2	Market
		2 500 000	2 500 000			5 000 000	999 999 999
90% BI	18 147 845	5 000 000	3 003 935	10 143 910			
PCI	0	0	0	0			
PHI	0	0	0	0			
PII	0	0	0	0			
Total	18 147 845	5 000 000	3 003 935	10 143 910	5 000 000	3 003 935	13 147 845

M. AJUSTEMENTS DES SINISTRES ATTRITIONNELS ET GRAVES

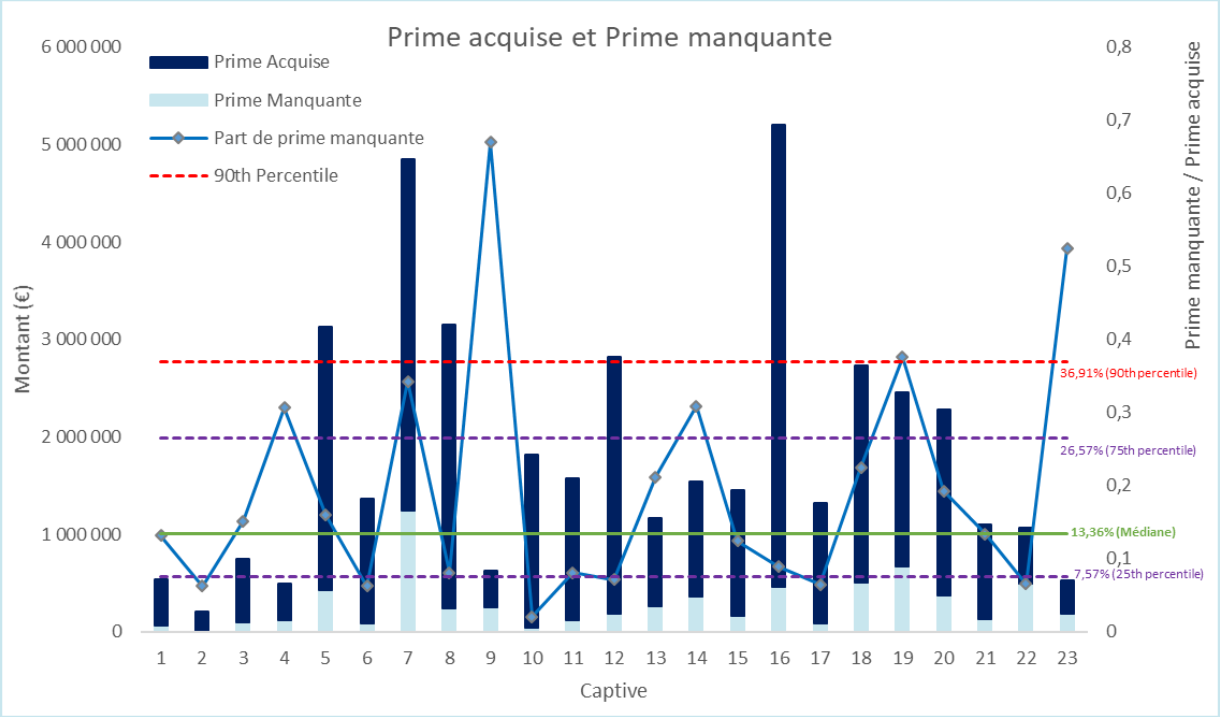


Les deux courbes ci-dessus décrivent les ajustements possibles, réalisées avec @Risk sur les sinistres attritionnels (< 1 m€) du Benchmark sinistres. C'est la courbe Beta Général qui est choisie dans l'étude de *back testing* avec le benchmark sinistre.

Pour les sinistres graves, c'est la courbe Inverse Gauss qui est utilisée dans l'étude de *back testing*.



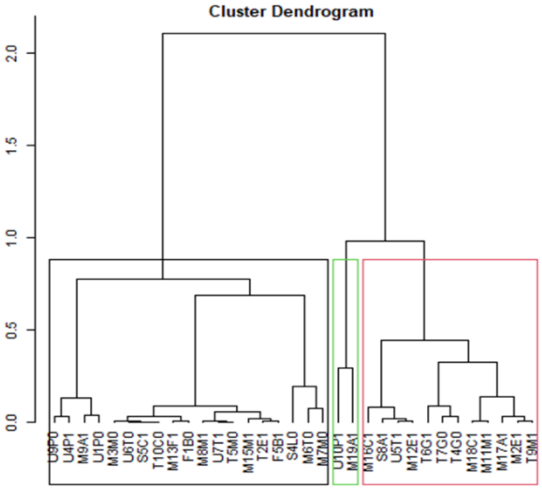
N. PRIME MANQUANTE FIRST PARTY & PRIME ACQUISE < 5 m€

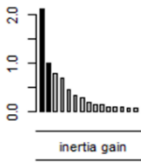


Pour les 23 captives qui souscrivent une prime inférieure à 5 m€ sur des programmes couvrant des garantie First Party, ce graphe permet de mieux visualiser la prime manquante, comparé au graphe graphe qui prime manquante pour la totalité des captives.
Pour 50% des captives, la prime manquante est supérieure à 13,36%, ce qui n'est pas négligeable au regard de la prime totale sur le programme tarifé.

O. CLASSIFICATION – BASE PRIME MANQUANTE FIRST PARTY

Arbre hiérarchique





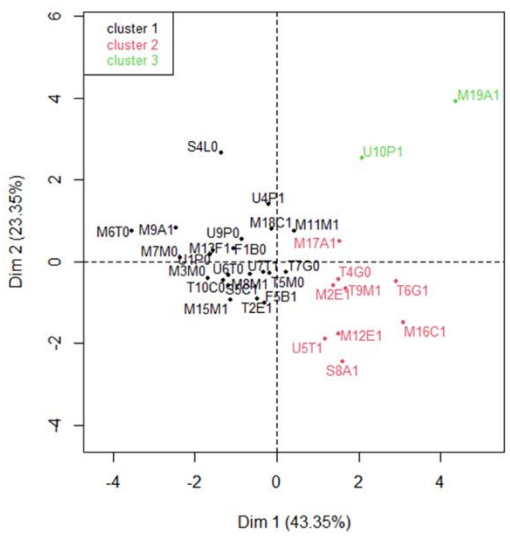
La classification utilise les variables obtenues lors du calcul de la « prime manquante ».

Du fait d'une forte corrélation entre les variables moyenne, SD, VAR200 et CA, seule la variable moyenne est conservée comme variable quantitative, les autres sont utilisées comme variables quantitatives supplémentaires.

La variable qualitative « Activity » est considérée comme une variable qualitative supplémentaire.

Une Analyse en Composantes Principales est réalisée en amont de la classification pour réduire les variables.

Plan factoriel



La **classe 1** est composée d'individus tels que *M6T0*, *M7M0*, *M9A1*, *U4P1* et *S4L0*. Ce groupe est caractérisé par de faibles valeurs pour les variables *moyenne*, *SD*, *Freq*, *VAR200*, *CA*, *Nb_Incident*, *Prime_Manq* et *Cyence.*

La **classe 2** est composée d'individus tels que *M12E1*, *U5T1*, *M16C1*, *T6G1* et *S8A1*. Ce groupe est caractérisé par de fortes valeurs pour les variables *Nb_Incident*, *Freq*, *moyenne*, *SD*, *VAR200*, *CA* et *Cyence.*

La **classe 3** est composée d'individus tels que *U10P1* et *M19A1*. Ce groupe est caractérisé par de fortes valeurs pour les variables *Prime_Manq*, *Limite_1st*, *CA*, *VAR200*, *moyenne* et *SD* (de la plus extrême à la moins extrême).

En conclusion, les classes sont définies de la façon suivante :

- Classe 1 : Entreprise peu sinistrée dans le passé et peu « courtisée » par les hackers.
- Classe 2 : Entreprise sinistrée dans le passé et de taille importante.
- Classe 3 : Entreprise avec seulement deux « individus » qui pourraient rejoindre la classe 2. Entreprise caractérisée par de « gros » programmes souscrits dans la captive (capacité importante)

P. REGRESSION LINEAIRE POUR LE *THIRD PARTY*

Comme pour les garanties *First Party*, les variables VAR200 et SD sont fortement corrélés à la moyenne et sont retirées de l'analyse. Le meilleur modèle est celui composé de 4 variables (La p value recommence à augmenter à partir de 5 variables).

	R2	P value
Model with 1 variable	0.6036149	9.119147e-05
Model with 2 variables	0.7829897	4.918616e-06
Model with 3 variables	0.8965445	1.260784e-07
Model with 4 variables	**0.9260296**	**9.066405e-08**
Model with 5 variables	0.9281146	5.445345e-07
Model with 6 variables	0.9413276	1.030309e-06
Model with 7 variables	0.9559237	1.338487e-06
Model with 8 variables	0.9573961	7.053250e-06
Model with 9 variables	0.9583342	3.609003e-05
Model with 10 variables	0.9583793	1.835006e-04

modelT$best

Call:
lm(formula = as.formula(as.character(formul)), data = don)

Residuals:

Min	1Q	Median	3Q	Max
-102150	-28216	9680	29749	94677

Coefficients:

	Estimate	Std. Error	t value	Pr(>|t|)
(Intercept)	-3.348e+04	1.820e+04	-1.840	0.087126.
Limite_Third	9.172e-03	1.736e-03	5.283	0.000116 ***
Nb_PCI	-8.562e-03	2.748e-03	-3.116	0.007591 **
Incident	5.584e+04	9.803e+03	5.697	5.52e-05 ***
SD	6.199e-02	1.246e-02	4.974	0.000204 ***

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 54380 on 14 degrees of freedom
Multiple R-squared: 0.926, Adjusted R-squared: 0.9049
F-statistic: 43.82 on 4 and 14 DF, p-value: 9.066e-08

BIBLIOGRAPHIES

Advisen, *Cyber Loss Data (2019)* ; Cyber Loss Data - Advisen Ltd.

Allianz Global Corporate & Specialty, *Baromètre des risques 2020 d'Allianz : les incidents cyber pour la première fois en tête des risques d'entreprise (14 janvier 2020) ; D*isponible sur Allianz-Risk-Barometer-2020.pdf

ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) (2016), *Adoption de la directive Network and Information Security (NIS) : l'ANSSI, pilote de la transposition en France* ; disponible sur : https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/

Apref (Association des Professionnels de la Réassurance en France) (2016), *Etude sur les cyberrisques et leur (ré)assurabilité* ; disponible sur : https://www.apref.org/sites/default/files/espacedocumentaire/note_apref_cyber_risque.pdf

Cybermalveillance, site web du gouvernement ; Assistance aux victimes de cybermalveillance

Deloitte, *Cyber attaques comment chiffrer les impacts ;* Cyberattaques : comment chiffrer les impacts ? (deloitte.com)

Haude-Marie Thomas ; L'ascension fulgurante du risque cyber (Janvier 2016) ; L'ascension fulgurante du risque cyber (Dossier risk management) (argusdelassurance.com)

Goron, *Les 5 cyberattaques qui ont marqué ces dernières années (Octobre 2020)* ; Le top des plus grosses cyberattaques de ces dernières années - RNMPS (goron.fr)

Hiscox, *Rapport 2019*; 2019-Hiscox-Cyber-Readiness-Report.pdf

Hiscox, *Rapport 2020 ;* Rapport_Hiscox_2020_sur_la_gestion_des_cyber_risques.pdf

Hiscox, *Rapport 2021;* 21486 - Hiscox Cyber Readiness Report 2021 - France.pdf

Jon Bateman, *War, terrorism and Catastrophe in Cyber Insurance (5 Octobre 2020)* ; War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions - Carnegie Endowment for International Peace

Le club des juristes*, Assurer le risque Cyber, (Janvier 2018)*

L'express, Cyberattaque NotPetya: son réseau, ses victimes et comment s'en protéger - L'Express L'Expansion (lexpress.fr)

Mahmoud Morsy, *Not Petya tactical report (25 juin 2019)* ; Rapport tactique NotPetya (menshaway.blogspot.com)

www.oodrive.com ; Le top 10 des différents types de cyberattaques (17 Mars 2021) ; Top 10 des différents types de cyberattaques - Oodrive

Pierre-Louis Lussan, *Les 10 types de cyberattaques les plus courants (Septembre 2019)* ; Les 10 types de cyberattaques les plus courants (netwrix.fr)

Sofian Larachi, *Les stratégies d'optimisation fiscale des entreprises internationales (2015 – 2016)* ; view (uclouvain.be)

Swiss Re, *A risk we need to insure (8 Janvier 2019)* ; Cyber – a risk we need to insure | Swiss Re

Swiss Re, *Too big to insure* (2016); 160946_IH_IVW_Studie_CyberRisk_Bd59.indd (unisg.ch)

Théophile Robert, *Les entreprises françaises investissent plus dans le cyber* (Août 2020) ; Cyber sécurité : les entreprises françaises investissent plus (assurlandpro.com),

Tristan Gaudiaut, Les cyberattaques les plus courantes contre les entreprises françaises en 2021 (6 Juillet 2021) ; Graphique: Les cyberattaques les plus courantes contre les entreprises françaises | Statista

Vadim Rubinstein, *Les 8 plus importants cyberattaques de l'histoire, de Stuxnet à Solarwinds (Mars 2021)*; Business Insider Les 8 plus importantes cyberattaques de l'Histoire, de Stuxnet à Solarwinds (businessinsider.fr)

Vuk Mujovic, *Les 10 plus grands hacking de données de tous les temps (Févier 2019)* ; Les 10 plus grands coups de piratage informatique. | Le VPN (le-vpn.com)

Wikipédia, *Le paradoxe des anniversaires (2014)* ; Paradoxe des anniversaires — Wikipédia (wikipedia.org)