Mémoire présenté le :

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

Par : Kenza IGGIDR

Titre : Appréhension d'un risque émergent : création d'un produit cyber

Confidentialité : ☐ NON ☒ (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

.....

.....

.....

Membres présents du jury de l'ISFA

.....

.....

.....

Entreprise : Acheel
Nom :

Signature :

Directeur de mémoire en entreprise :
Nom : Franklin ABITBOL

Signature :

Invité :
Nom :

Signature :

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

Signature du responsable entreprise

Signature du candidat

Résumé

En 2023, le monde est plus connecté que jamais, 4,95 Milliards de personnes utilisent Internet soit plus de la moitié de la population mondiale. Le risque cyber est devenu en l'espace de quelques années une préoccupation majeure pour tous : les particuliers mais surtout les entreprises de toutes tailles et de tous secteurs. Les cyberattaques ont augmenté de plus de 38% dans le monde en 2022 et les impacts se chiffrent à plusieurs centaines de milliards d'euros. Les acteurs économiques cherchent des réponses techniques mais également financières à cette criminalité du XXIeme siècle. Dans ce contexte, ces derniers se sont rapidement tournés vers les assureurs, spécialistes historique de la gestion du risque. L'assurance cyber est donc un produit relativement jeune, challengé sur son efficacité et sa pertinence tant par les assureurs, que par les pouvoirs publics. Dans le prolongement de ce débat, ce mémoire a pour objectif d'analyser l'assurance cyber, sa conception, sa modélisation et sa tarification afin d'apporter une solution adéquate aux entreprises désireuses de transférer leur risque. Etant donné la nature technique, économique et systémique du risque cyber, une approche pluridisciplinaire combinant des éléments de l'analyse de risque, de la théorie de l'assurance et de la gestion des risques d'entreprise a été adoptée pour ce mémoire. Nous nous sommes également appuyé sur des études de cas pour illustrer les différentes problématiques et les pratiques actuelles en matière d'assurance cyber afin de confronter notre modèle à la réalité. L'approche utilisée contribue à une meilleure appréhension du risque cyber mais pourra également guider les assureurs dans leur appréhension de nouveaux risques inconnus dans un monde qui évolue bien plus rapidement.

Mots clés— Assurance cyber, Tarification, Cyberattaques, Modèles épidémiologiques

Abstract

In 2023, the world is more connected than ever, with 4.95 billion people using the Internet, which is more than half the world's population. The cyber risk has become in a short period of time a major concern for everyone: individuals but especially companies of all sizes and sectors. Global cyber attacks have increased by more than 38% in 2022 and the impact is estimated at several hundred billion euros. Economic actors are looking for technical but also financial answers to this modern kind of crime. In this context, they have quickly turned to insurers, historical specialists in risk management. Cyber insurance is therefore a relatively young product, challenged on its efficiency and relevance by both insurers and public authorities. As an extension of this debate, this thesis aims to analyze cyber insurance, its design, modeling and pricing in order to provide an adequate solution to companies willing to transfer their risk. Given the technical, economic and systemic nature of cyber risk, a multidisciplinary approach combining elements of risk analysis, insurance theory and enterprise risk management has been adopted for this dissertation. We also used case studies to illustrate the different issues and current practices in cyber insurance in order to confront our model with reality. The chosen approach contributes to a better understanding of cyber risk but can also guide insurers in their apprehension of new unknown risks in a world that is evolving much faster.

***Keywords*—** Cyber insurance, Pricing, Cyber attack ,Epidemic models

Remerciement

Je tiens à exprimer toute ma gratitude à Franklin ABITBOL, qui a su me guider, m'encourager et me faire confiance. Je le remercie particulièrement pour ses conseils avisés et pour le temps qu'il m'a accordé durant mon alternance et son encadrement pour la réalisation de mon mémoire.

Je souhaite également remercier Esterina MASIELLO, ma tutrice académique pour avoir assuré le suivi du mémoire.

Une pensée particulière pour Alicia GIULY et Pauline DARENE pour leurs précieux conseils ainsi que leur relecture de ce dit mémoire.

Enfin, toute ma gratitude va à ma famille et à mes amis pour leurs encouragements et leur soutien inconditionnel dans mes études et mes projets.

Table des matières

Introduction

Le développement de l'intelligence artificielle dans de nombreux domaines, l'utilisation de clouds dans les entreprises ainsi que la crise du covid-19 ont fait prendre conscience du risque que représentent les cyber attaques.

Si la crise sanitaire du Covid-19 a évidemment mis en exergue le risque de pandémie pour les maladies humaines, elle a également eu pour effet d'attirer l'attention sur un nouveau type de pandémie : la cyberpandémie.

Les restrictions sanitaires ont entraîné une utilisation massive des ordinateurs et surtout des réseaux pour les entreprises et leurs salariés. La plupart de ces structures ont dû recourir au télétravail de manière précipitée à la suite des annonces gouvernementales et n'ont pu l'encadrer de toutes les règles de sécurité protectrices nécessaires. Par exemple, l'utilisation d'un même appareil informatique pour ses besoins personnels et pour ses missions professionnelles augmente drastiquement les risques de virus. Ainsi, les virus informatiques sont, plus que jamais, devenus une menace pour les entreprises, les institutions publiques et les particuliers. Prévenir et lutter contre les cyber attaques devient alors un impératif stratégique pour les entreprises et les pays mais également pour les assureurs qui, selon leur rôle traditionnel, sont en charge de proposer des solutions pour couvrir les risques émergents.

Cependant, si la crise sanitaire a renforcé l'existence de menaces cyberattaques, ce risque était déjà connu. En effet, de nombreux exemples ont pu illustrer comment une cyberattaque pouvait affecter des centaines de milliers d'individus à travers le monde entier, et cela en quelques heures

seulement. Ainsi, en 2017, le ransomware Wannacry est venu frapper de nombreuses entreprises et institutions dans le monde en bloquant l'accès aux ordinateurs et à leurs données en échange du paiement d'une rançon. Les ransonwares ne sont pas les seules cyberattaques existantes. On peut également citer le phishing qui touche principalement des particuliers et qui consiste à envoyer un mail en se faisant passer la plupart du temps pour un organisme financier afin de sous tirer les coordonnées bancaires des victimes.

C'est donc de manière logique que le risque cyber figure dans la liste des 5 principaux risques émergents établie par les assureurs et se retrouve ainsi à côté d'autres enjeux contemporains, tels que le changement climatique, l'intelligence artificielle, la robotisation, l'instabilité financière.

L'assurance consiste à prévenir et à se préparer aux risques auxquels la société est ou sera confrontée dans les années à venir. Toutefois, les risques émergents, tel que le cyber risque, sont caractérisés avant tout par le manque de données. Cette complexité se traduit directement par la difficulté à prédire ou tarifer ce risque en perpétuelle évolution. Les méthodes de tarification traditionnelles se révèlent alors insuffisantes puisque l'assureur ne peut se baser sur des informations historiques.

À ce manque de données, s'ajoute la complexité de la nature même du risque cyber qui peut toucher aussi bien des particuliers, que des entreprises, des institutions publiques et ne connaît aucune limite territoriale.

Devant un tel risque, le rôle de l'assureur ne se limite pas à le couvrir mais également à être un réel acteur de prévention afin d'aider tout assuré à comprendre ce risque et à l'appréhender.

Le décalage entre la prise de conscience du danger que représente le cyber risque et la mise en oeuvre de mesures de protection efficaces reste un challenge pour le secteur de l'assurance.

Chapitre 1

Acheel : une nouvelle compagnie d'assurance

1.1 Présentation de l'entreprise

Acheel a été fondé par Ralph Ruimy et Francky Défossé en mars 2020. L'entreprise est née d'un constat simple : il n'existe pas sur le marché français de structures permettant aux consommateurs de souscrire à une assurance très rapidement via leur smartphone ou via un ordinateur, le tout sans se déplacer, sans téléphoner et surtout avec le moins de contraintes possibles. Acheel est donc la première compagnie d'assurance généraliste et 100% digitale qui permet de simplifier la souscription à une assurance, en passant par le choix de ses garanties et de ses options. Une des missions d'Acheel est de faire aimer l'assurance aux français en proposant les prix les moins chers du marché tout en offrant une information claire et précise sur le contenu du contrat d'assurance.

Acheel a été agréée le 21 avril 2021 par l'Autorité de contrôle prudentiel et de résolution. Cette décision a été publiée au Journal officiel de la République française du 13 mai 2021 permettant ainsi à Acheel d'opérer dans les branches d'activités suivantes :

— 1 - Accidents ;

— 2 - Maladie ;

— 8 - Incendie et éléments naturels ;
— 9 - Autres dommages aux biens ;
— 13 - Responsabilité civile générale.
— 16 - Pertes pécuniaires diverses
— 17 - Protection juridique

Le but d'Acheel est de proposer une assurance :

— simple et rapide,
— flexible et personnalisée,
— sans frais cachés : la transparence étant au cœur des valeurs d'Acheel : du début à la fin, le client sait combien il paye et ce pour quoi il est assuré.
— Toujours aux côtés de ses assurés grâce à un service client composé d'experts basé à Paris.

Ce projet a pu voir le jour grâce à une levée de fond de 29 millions d'euros et de deux grands soutiens : Xavier Niel et Jean de la Rochebrochard, qui ont tout de suite cru en cette volonté de monter une nouvelle compagnie d'assurance, simple et agile, afin de disrupter le marché.

1.2 Lignes de business

Le lancement du site Acheel au grand public a eu lieu fin mai 2021. Trois produits ont été proposés en BtoC au public : une assurance MRH (Multi-risques habitation), une assurance Santé et une assurance santé animal (chien et chat). Acheel est une compagnie d'assurance généraliste qui souhaite pouvoir assurer tout le monde et multi-équiper ses assurés afin de réduire les coûts d'acquisition. En effet, un prospect attiré par un produit spécifique d'Acheel pourra, face à l'offre généraliste d'Acheel, souscrire à un autre produit. C'est pourquoi, l'offre de produit Acheel ne cesse de se développer.

Les offres distribuées en direct sont :

— 2 produits MRH (Multi-risques habitation) ;
— 3 produits Santé animale ;
— 4 produits PNO (Propriétaire Non-Occupant) ;
— 19 produits Santé ;
— 4 produits automobile.

Grâce à un parcours de souscription simplifié et clair, ainsi qu'une offre très compétitive, Acheel a très vite su conquérir un large nombre d'assurés. Ainsi, au 31 décembre 2022, Acheel comptabilisait déjà 150 000 assurés.

Cependant, la distribution d'assurance via le canal internet ne représentant, actuellement, que 20% du marché français, Acheel a fait le choix de recourir également à la distribution via des courtiers afin de s'adresser à une plus large population, principalement en assurance santé.

La fluidité de conception des produits et les partenariats solides noués avec les réassureurs ont permis à Acheel de travailler avec des courtiers de premier plan. Si fin 2021, le nombre d'assurés couverts par un produit Acheel via ce canal de distribution s'élevait à 12 160 assurés, il s'élève à 117 975 fin 2022.

Afin de satisfaire toujours davantage ses assurés et partenaires, Acheel développe en permanence ses technologies. Ainsi, Acheel a mis en place un outil de remboursement des sinistres en santé animale, qui permet de traiter un sinistre en quelques minutes seulement, grâce à des techniques d'OCR (*Optical Character Recognition*) et d'intelligence artificielle.

1.3 Pourquoi intégrer un produit cyber

Acheel étant une jeune compagnie d'assurance innovante avec un modèle économique basé sur le digital, proposer un produit de couverture du risque cyber s'inscrivait dans l'optique de la compagnie.

De plus, comme expliqué précédemment, Acheel a construit son business autour de 2 canaux de distribution : le direct et le courtage. Ce dernier est un modèle économique à coûts variables et permet rapidement d'atteindre une masse d'assurés conséquente et bien répartie sur l'ensemble du territoire et ainsi de mieux répartir les risques.

La maîtrise des risques impose que les premiers produits en courtage soient des risques peu connus. La MRH et la complémentaire Santé sont des risques bien connus des assureurs et assez largement diffusés pour avoir accès à de nombreuses informations sur le risque. Néanmoins,

du fait de la couverture des incendies, des tempêtes et de la responsabilité civile, la MRH présente un risque de pointe assez conséquent. Le choix s'est donc porté en 2021, de focaliser la stratégie de distribution courtée sur le risque Santé.

Néanmoins, Acheel étant un acteur disruptif dans le marché de l'assurance, la décision de diversifier le risque porté en courtage a rapidement été prise : intégrer un nouveau produit, tel que le cyber, s'inscrit parfaitement dans l'ADN de la compagnie.

1.4 Intégration d'un nouveau courtier et d'un nouveau produit

Grâce à de solides partenariat avec des réassureurs de renom, l'opportunité d'un partenariat pour être porteur de risque d'un produit cyber s'est présentée.

Ainsi, l'intégration du risque cyber au sein d'Acheel présente un double enjeu :

- L'intégration et le suivi d'un nouveau partenaire ;
- l'intégration d'un nouveau risque : le risque cyber, encore peu connu de manière générale dans l'éco-système assurantiel et au sein d'Acheel.

1.4.1 Intégration d'un nouveau partenaire

Ce premier point est maitrisé au sein d'Acheel, puisqu'un process cadré est mis en place pour l'intégration de chaque nouveau courtier. L'implémentation opérationnelle du nouveau courtier ne fera pas l'objet d'une partie dans ce mémoire, néanmoins les points clés de l'intégration et du suivi du partenariat sont rapidement résumés dans cette sous-partie.

A la mise en place d'un partenariat, des spécificités fonctionnelles des produits sont transmises aux partenaires pour l'implémentation des tarifs et des documents contractuels dans leurs outils. Des recettes sont effectuées pour contrôler, au démarrage, les deux premiers points précédemment cités, ainsi que la conformité des templates de données qui seront transmis par le délégataire de gestion pour contrôler les flux financiers.

Un audit des procédures écrites et opérationnelles du partenaire est également réalisé dans lequel les éléments suivants sont contrôlés :

- Organigramme de la société ;
- Déclaration correspondant TRACFIN ;
- Désignation DPO ;
- Attestation ORIAS ;
- Plan de continuité informatique ;
- Procédure interne de traitement des réclamations client ;
- Processus du contrôle des ventes ;
- Durée de conservation des données personnelles ;
- Procédure de gestion des droits utilisateurs ;
- Politique RGPD ;
- Processus de vérification du gel des avoirs.

Par ailleurs, Acheel a créé des outils de contrôle des flux émis par les délégataires de gestion. Ces outils de contrôle permanent permettent d'établir pour chaque affaire souscrite via un intermédiaire :

- La justesse du tarif ;
- Le contrôle de l'encaissement ;
- Le calcul des commissions à devoirs et le comparatif avec ce qui est calculé par le délégataire de gestion ;
- Le contrôle des indus éventuels.

Ces outils permettent à Acheel d'exercer un contrôle opérationnel de l'activité déléguée et donne toute latitude pour mettre en œuvre l'ensemble des correctifs qui seraient nécessaires pour corriger des dysfonctionnements ou suspendre les souscriptions.

1.4.2 Intégration d'un nouveau risque : le risque cyber

Ce second point est plus complexe et constitue le point central de ce mémoire. En effet, avant toute intégration d'un nouveau risque, une étude poussée doit être réalisée. Cette étude a pour but d'être présentée au comité de direction, ce dernier allant ensuite arbitrer si le projet va être ou non retenu. Afin de présenter l'intégration d'un nouveau produit dans son entièreté, l'étude s'articule autour des piliers suivants :

— Étude globale du risque cyber ;
— Garanties couvertes ;
— Étude tarifaire proposée ;
— Obligation réglementaire et impact sur le bilan prudentiel de l'ajout d'un nouveau produit dans le business plan.

Chapitre 2

Le risque cyber en assurance

2.1 Histoire de l'assurance cyber

France Assureur publie chaque année un baromètre des risques sur les sociétés d'assurance et de réassurance à moyen terme. Pour la cinquième année consécutive le risque cyber se trouve en haut du classement réalisé comme montré dans le tableau ci dessous. Le score mentionné dans le tableau est un score (fréquence ; sévérité), ce dernier a un minimum de (0 ; 0) et un maximum de (5 ; 5).

	CLASSEMENT DES RISQUES À 5 ANS		ÉVOLUTION	
RANG	RISQUES	SCORE	RANG	SCORE
1	Cyberattaques	(4,1 ; 4,0)	(0)	(−0,4 ; −0,4)
2	Dérèglement climatique	(3,7 ; 3,7)	(0)	(−0,2 ; −0,2)
3	Environnement économique dégradé	(3,6 ; 3,5)	(+2)	(+0,2 ; −0,2)
4	Pénurie de matières premières et énergétiques	(3,4 ; 3,2)	Nouveau risque	
5	Risque politique mondial	(3,4 ; 3,1)	(+9)	(+0,1 ; +0,6)
6	Catastrophe naturelle exceptionnelle	(3,8 ; 2,5)	(−3)	(+0,4 ; −1,6)
7	Dégradation de l'environnement	(3,0 ; 3,1)	(+4)	(−0,4 ; +0,2)
8	Risque systémique	(3,6 ; 2,5)	(−1)	(+0,2 ; −0,9)
9	Changement règlementaire	(2,9 ; 3,2)	(0)	(−0,5 ; −0,1)
10	Risque de non-conformité et sanctions	(2,9 ; 2,9)	(−4)	(−0,5 ; −0,5)
11	Risque de transition	(3,1 ; 2,6)	Nouveau risque	
12	Risque politique européen	(3,1 ; 2,6)	(+5)	(+0,5 ; −0,2)
13	Vulnérabilité des infrastructures stratégiques	(3,2 ; 2,4)	Nouveau risque	
14	Inégalités et tensions sociales	(2,7 ; 2,9)	(−2)	(−0,9 ; +0,2)
15	Qualité des données	(2,7 ; 2,7)	(−7)	(−0,6 ; −0,7)
16	Risque pandémique	(3,0 ; 2,4)	(−6)	(+0,0 ; −1,1)
17	Risque de terrorisme	(2,7 ; 2,5)	(−4)	(−0,7 ; −0,1)
18	Risque politique français	(2,6 ; 2,4)	(−2)	(−0,2 ; −0,4)
19	Flux migratoires	(2,3 ; 2,6)	(+4)	(−0,8 ; +0,7)
20	Risques RH	(2,5 ; 2,3)	Nouveau risque	
21	Disruption du secteur de l'assurance	(2,6 ; 2,1)	(−2)	(+0,2 ; −0,8)
22	Équilibres démographiques	(2,4 ; 2,2)	(+3)	(+0,5 ; −0,2)
23	*Conduct risk*	(2,3 ; 2,2)	(−5)	(−0,2 ; −0,6)
24	Maîtrise des algorithmes	(2,3 ; 2,1)	(−9)	(−0,4 ; −0,8)
25	Dégradation de la santé mentale	(2,1 ; 2,1)	(−3)	(−0,6 ; −0,2)

FIGURE 2.1 – Classement des risques à 5 ans réalisé par France Assureur (26/01/2023)

En effet, une étude datant de 2020 montre que les pertes liées au risque cyber représente près de 1 % du PIB mondial, ce qui représentent environ 1 000 Md $.

Bien que le risque cyber soit au coeur de l'actualité, il n'est pas récent. Il est possible de se couvrir contre ce risque depuis la fin des années 1990, non pas par des assurances cyber à proprement parler mais par le biais d'autres polices d'assurances comme des assurances pertes d'exploitations ou encore responsabilité civile commerciale. Le flou que présentent ces polices a créé des tensions entre assurés et assureurs qui ont ainsi menés ces derniers à la conception d'un produit d'assurance cyber.

2.2 Définition du risque cyber

Dans cette partie, nous allons essayer de fournir une définition du risque cyber et dans quel contexte les produits assurantiels couvrant ce risque sont créés.

En assurance, on peut définir un risque de manière simple comme étant le produit de la probabilité d'occurrence d'un sinistre (l'aléa) et l'intensité ou l'amplitude de ce sinistre (la gravité) :

$$\text{Risque} = \text{Aléa} \times \text{Gravité}$$

2.2.1 Les différents types de menaces informatiques

Afin de mieux se prémunir du risque, il faut en connaître toutes les causes pour pouvoir comprendre les risques encourues par les entreprises et estimer leur sensibilité au risque cyber.

L'objectif d'un attaquant est d'entrer dans un système informatique afin d'en compromettre les données sensibles ou de déstabiliser l'entreprise. Ainsi, pour s'introduire dans un système informatique, un attaquant peut utiliser plusieurs types de vulnérabilité :

- Les vulnérabilités liées aux logiciels : les logiciels utilisés par l'entreprise peuvent contenir des failles de sécurité qui peuvent être exploitées par des attaquants pour accéder aux données ou aux systèmes de l'entreprise.
- Les vulnérabilités liées aux mots de passe : les mots de passe faibles, facilement devinables ou partagés peuvent permettre à des personnes non autorisées d'accéder aux systèmes et aux données sensibles de l'entreprise.
- Les vulnérabilités liées aux réseaux : les réseaux de l'entreprise peuvent être vulnérables à des attaques de type "*man-in-the-middle*" ou à des attaques par *déni de service (DoS)*.
- Les vulnérabilités liées aux périphériques : les périphériques utilisés par l'entreprise, tels que les ordinateurs portables, les téléphones mobiles ou les tablettes, peuvent être perdus ou volés, ce qui peut compromettre la sécurité des données.
- Les vulnérabilités liées aux utilisateurs : les utilisateurs peuvent être victimes de phishing ou d'autres attaques de social engineering qui peuvent compromettre la sécurité des données de l'entreprise.

— Les vulnérabilités liées aux applications web : les applications web utilisées par l'entreprise peuvent être vulnérables à des attaques telles que l'injection SQL ou les attaques par déni de service.
— Les vulnérabilités liées aux mises à jour : les mises à jour de sécurité peuvent ne pas être installées régulièrement, ce qui peut rendre l'entreprise vulnérable à des attaques qui ont été corrigées par ces mises à jour.

2.2.2 Les principales conséquences d'attaques cyber

Les conséquences d'une cyberattaque peuvent être très diverses et varier en fonction du type d'attaque, de la cible, de la gravité et de la durée de l'attaque. Voici quelques-unes des principales conséquences possibles d'une cyberattaque :

— **Fuite d'informations** : les cyberattaques peuvent entraîner la perte, la corruption ou la destruction de données sensibles, telles que des informations de clients, des données financières ou des secrets commerciaux.

  Selon une étude de l'Institut Ponemon et de IBM security [8], le coût moyen d'une violation de données pour les entreprises en France était de **2,52 millions d'euros** en 2020.
— **Dommages financiers** : les cyberattaques peuvent avoir des conséquences financières importantes, notamment en termes de coûts de récupération des données, de pertes de revenus, de coûts de remise en état des systèmes et de pertes de confiance des clients. D'après une enquête de Hiscox, le coût moyen d'une cyberattaque pour les entreprises en France était de **17 000 euros** en 2022 [7].
— **Atteinte à la réputation** : les cyberattaques peuvent avoir un impact négatif sur la réputation d'une entreprise ou d'une organisation. Les clients peuvent perdre confiance dans l'entreprise, ce qui entraîne une baisse de la demande et une perte de parts de marché, selon une étude de Deloitte, les coûts moyens de la gestion de crise de réputation pour les entreprises en France peuvent varier entre 50 000 et 100 000 euros.
— **Interruption ou dégradation de l'activité** : les cyberattaques peuvent causer l'arrêt complet ou partiel des services en ligne, ce qui peut entraîner une perte de productivité, des retards dans les projets et une baisse de la qualité des services. Le fournisseur de solutions

de cybersécurité Kaspersky [9] a évalué que le coût moyen d'une interruption de services pour les entreprises en France s'élevait à 171 000 euros en 2020. Cette estimation inclut le coût des mesures de récupération des données, les pertes financières liées à l'indisponibilité des services ainsi que les coûts de la restauration du système après l'attaque. Accenture a menée une étude en 2020 et fait lever ce chiffre à 1,58 million d'euros [1]. Il est important de noter que les coûts liés à une interruption de services peuvent varier considérablement en fonction de la taille de l'entreprise, du secteur d'activité, de la durée de l'interruption et de la complexité du système affecté. Cette évaluation du coût moyen sera un facteur clé dans la tarification effectuée dans la partie 4.

- **Sanctions légales** : les entreprises qui ne protègent pas suffisamment leurs données peuvent être soumises à des sanctions légales, notamment en cas de violation de la vie privée des clients ou de non-conformité aux réglementations de protection des données. Les amendes pour non-conformité aux réglementations de protection des données peuvent aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial, selon le Règlement Général sur la Protection des Données (RGPD) de l'Union européenne.
- **Risques pour la sécurité nationale** : les cyberattaques peuvent avoir des conséquences graves pour la sécurité nationale, notamment en cas de piratage de systèmes gouvernementaux ou militaires.

Il est important de noter que ces conséquences ne sont pas exhaustives et que les conséquences d'une cyberattaque varient en fonction des circonstances de chaque cas.

2.3 Les chiffres du marché de la cyber assurance

2.3.1 Dans le monde

En 2020, le coût médian d'une cyber-attaque dans le monde a été en moyenne de 13 200 $. Ce montant descend à 8000 $ pour les entreprises de moins de 10 employés. Les attaques les plus fréquentes sont les ransomwares : pas moins d'un sixième des entreprises a été touché par une de ces attaques durant l'année 2020. Parmi ces entreprises, 60% d'entre elles ont payé une rançon.

2.3.2 Aux Etats-Unis

Le plus gros marché concernant l'assurance cyber est le marché américain avec plus de 3Md$ de primes émises en 2020. Ce marché est dominé par 10 principaux acteurs : Chubb, AXA, AIG, Travelers, Beazley plc, AXIS, CNA, Fairfax Financial, The Hartford, BCS Insurancce Co. Ces 10 assureurs représentent à eux seuls 64,1 % des primes émises en 2019 et 63,3% des primes émises en 2020 2.1.

	2019	**2020**	**Evolution**
Primes émises	2 477 099 000 $	2 987 512 000 $	+ 21 %
Prestation moyenne payée	145 000 $	358 000 $	+ 147 %

TABLE 2.1 – Chiffres de la cyber assurance aux Etats-Unis, d'après l'Annual Report on the Insurance Industry ([5], pages 74-77)

On constate une hausse de 21 % des primes émises mais le constat le plus frappant est l'évolution du coût de sinistre moyen. Le département de la sécurité intérieure des États-Unis a annoncé qu'au titre de l'année 2020, près de 350M$ ont été payé au titre des rançons demandés par les ransomwares. Ce chiffre a fait un bond de plus de 300% depuis 2019, il peut être expliqué par la pandémie de Covid-19 et l'expansion du télétravail.

Néanmoins, d'après les données de plusieurs assureurs, le nombre de rançons payées durant l'année 2021 a baissé par rapport aux chiffres de 2020.

Il faut cependant relativiser ces chiffres car les primes émises en cyber ne représentent qu'1% du marché de l'assurance non-vie aux Etats Unis.

2.3.3 En France

L'Association pour le Management des Risques et des Assurances de l'Entreprise (AMRAE), une association professionnelle des métiers du risques et des assurances en entreprise, a effectué une étude quantitative des entrepries française couvertes par un contrat d'assurance cyber.

Cette étude montre que peu importe l'échelle de l'entreprise, sa couverture contre le risque cyber est encore trop faible.

— **Grandes entreprises** (Chiffre d'affaire supérieur à 1,5Md€) : malgré le fait que plus de 87 % d'entre elles soient couvertes contre le risque cyber, cette couverture est néanmoins insuffisante car elle représente en moyenne seulement 40M€ pour des entreprises dont le chiffres d'affaire dépasse les 1,5Md€.

— **Entreprise de taille intermédiaire** (Chiffre d'affaire compris entre 50M€ et 1,5Md€) : 8 % seulement sont assurées avec une couverture moyenne de 8M€.

— **Petites et Moyennes Entreprises** (Chiffre d'affaire compris entre 10M€ et 50M€) et les **Très Petites Entreprises** (Chiffre d'affaire inférieur à 10M€) : La couverture de ces structures est encore trop insignifiantes au regard de leur fragilité face à des attaques cyber, ce constat est d'autant plus alarmant lorsque 42 % des TPE/PME se disent novices en cybersécurité.

La répartition des primes acquises par type d'entreprise est reprise dans le graphique suivant. Sans surprise, les grandes entreprises représentent la majorité des primes émises étant donné que leur prime moyenne est plus élevée que celle des plus petites structures.

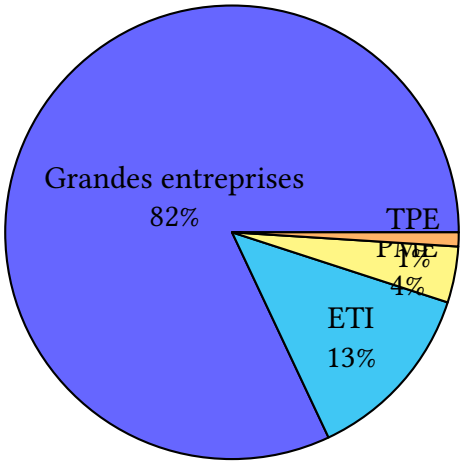

FIGURE 2.2 – Répartition des primes acquises en 2021 par typologie d'entreprises

Enfin, nous constatons une évolution des primes acquises au fil des années comme le témoigne le tableau 2.2, une hausse particulièrement importante de la sinistralité est observé pour l'année 2020 dû à la pandémie qui s'atténue par la suite en 2021.

	2019	2020	2021
Primes acquises (en Md€)	87	130	185
Sinistralité* (en Md€)	73	217	164
Loss ratio	84%	167%	88%

Table 2.2 – Étude des loss ratio par années de l'assurance cyber en France

Malgré le fait que la plupart des entreprises considèrent le risque cyber comme une véritable menace pour leur activité, le taux de couverture du risque cyber a chuté de 4,4 %

Ce premier constat sur le manque de couverture des PME et TPE, lance une première idée sur le marché cible qu'Acheel veut conquérir.

2.4 L'encadrement juridique du risque cyber

L'assurabilité du risque cyber est un domaine en constante évolution. Si les entreprises et les particuliers prennent conscience de l'importance de se protéger contre les risques liés à la cybercriminalité, les pouvoirs législatifs ont également de leur côté une volonté d'encadrer spécifiquement ce risque et les contrats d'assurance qui en découlent.

Les risques liés à une attaque cyber ont tout d'abord été encadrés au titre de la protection des données à caractère personnel. En effet, le Règlement(UE) 2016/679 du Parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après, le "RGPD") impose à tout organisme de déclarer à la Commission Nationale de l'Informatique et des Libertés toute violation de données à caractère personnel qu'il aurait subit. Cette violation de données personnelles est définie comme "une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données. À ce titre, une entreprise victime d'une introduction malveillante dans sa base de donnée devra notifier cette violation auprès de la CNIL en cas de risque élevé et à la personne concernée, en cas de risque très élevé pour cette dernière.

Sous l'angle de la protection des données personnelles, cette nouvelle obligation a ainsi contraint

les entreprises à se doter d'un dispositif permettant de prévenir toute violation de données et réagir de manière appropriée en cas de violation afin d'y mettre fin et minimiser ses effets.

Le cyber a fait sa première entrée dans le Code des assurances à la suite de la publication de l'Arrêté du 13 décembre 2022 relatif à la classification des engagements d'assurance consécutifs aux atteintes aux systèmes d'information et de communication. Cet Arrêté a eu pour effet de créer deux catégories ministérielles pour les risques cyber et cela afin d'améliorer le pilotage économique et réglementaire des passifs exposés à ce risque. Bien que cette nouvelle réglementation concerne uniquement les reportings et la comptabilité des assureurs, elle souligne l'intérêt porté par les pouvoirs publics d'encadrer juridiquement et de clarifier la place du cyber dans le secteur de l'assurance.

Cet intérêt a été de nouveau illustré par la promulgation de la loi n°2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur qui a créé un nouveau chapitre au sein du Code des assurances intitulé "L'assurance des risques de cyberattaques". Selon ce nouvel article L. 12-10-1 du Code des assurances, le versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnée aux articles 323-1 à 323-3-1 du code pénal est subordonné au dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard 72 heures après la connaissance de l'atteinte par la victime. Cette formalité obligatoire s'applique aux personnes morales et aux personnes physiques dans le cadre de leur activité professionnelle.

Indépendamment de ce cadre spécifique au risque cyber, tout contrat d'assurance cyber reste soumis aux règles communes à tout contrat d'assurance. À ce titre, il est obligatoire, pour l'assureur, de délivrer une information claire et complète sur le contenu de la couverture, les conditions et les exclusions du contrat. Les assureurs doivent également respecter les règles de la tarification, qui doivent être équitables et non-discriminatoires.

Concernant le contenu du contrat, le Code des assurances ne prévoit pas, à l'heure actuelle, de garanties obligatoires. Les assureurs proposent ainsi des garanties optionnelles pour couvrir les risques spécifiques liés à la cybercriminalité, que ce soit dans un contrat d'assurance spécifique au risque cyber que dans un contrat d'assurance couvrant un autre risque (exemple : une option

cyber incluse dans un contrat de Multirisques Habitation). Les polices d'assurance cyber peuvent notamment inclure des garanties de responsabilité civile pour les dommages causés aux tiers, y compris les pertes de données et les dommages à la réputation.

La volonté de se doter d'un encadrement spécifique et clarifié pour les acteurs du marché est également partagé par l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) qui a publié différentes recommandations sur le sujet : la recommandation ACPR 2017-R-01 : cette recommandation a été publiée par l'ACPR en 2017 et concerne les obligations des assureurs en matière de couverture des risques cyber. Elle décrit notamment les éléments d'information que les assureurs doivent fournir aux entreprises avant de souscrire une assurance cyber.

2.4.1 Les recommandation de l'ACPR

La recommandation 2019-R-01 a été publiée par l'ACPR en 2019 et concerne les obligations des assureurs en matière de gestion des risques cyber. Elle recommande notamment que les assureurs proposent des mesures de prévention et de gestion des risques cyber aux entreprises, en plus de la couverture d'assurance.

L'article ACPR N°2020-03, publié en juin 2020 par l'ACPR, traite des cyberattaques dans le contexte de la pandémie COVID-19 et fournit des recommandations pour les entreprises et les assureurs. Il souligne notamment l'importance de la prévention et de la gestion des risques cyber pour les entreprises et recommande aux assureurs de proposer des offres de couverture adaptées aux besoins spécifiques des entreprises.

2.5 Les différentes menaces cyber des entreprises

2.5.1 Les ransomwares : Exemple de Wannacry

Un ransomware (ou rançongiciel en français) est un type de logiciel malveillant qui chiffre les fichiers sur un ordinateur ou un réseau et qui demande une rançon pour les déchiffrer. Les rançongiciels sont l'une des formes les plus répandues de cyber-attaques, car faciles à concevoir et à diffuser.

Les ransomwares peuvent être diffusés de différentes manières, souvent par le biais d'e-mails

d'hameçonnage (phishing), de téléchargements malveillants ou de failles de sécurité dans les logiciels ou les systèmes d'exploitation. Une fois qu'un rançongiciel a infecté un système, il va chiffrer les fichiers importants pour l'utilisateur, rendant ainsi leur accès impossible.

En général, les rançongiciels affichent un message à la victime, indiquant que les fichiers ont été chiffrés et qu'une rançon doit être payée pour les récupérer. Les rançons sont souvent demandées en utilisant des crypto-monnaies, telles que Bitcoin ou Monero, ce qui rend les paiements difficiles à retracer. Ces logiciels malveillants sont souvent conçus pour cibler les entreprises, car elles ont souvent des données importantes et critiques, et sont donc plus susceptibles de payer une rançon pour récupérer leurs fichiers. Cependant, les particuliers sont également souvent victimes de ces attaques.

Il existe plusieurs types de ransomwares, tels que les ransomwares locker, qui empêchent l'accès à l'ordinateur de la victime, et les ransomwares crypto, qui chiffrent les fichiers de l'utilisateur. Certains ransomwares peuvent également utiliser des techniques de persistance pour continuer à infecter un système même après qu'il ait été nettoyé.

Pour se protéger contre les ransomwares, il est recommandé de maintenir les logiciels et les systèmes à jour avec les derniers correctifs de sécurité, d'effectuer des sauvegardes régulières des fichiers importants, et de ne jamais payer de rançon. Les victimes de ransomwares sont encouragées à signaler l'attaque aux autorités compétentes et à rechercher l'aide d'experts en sécurité informatique pour récupérer leurs données.

Un des exemples les plus connus de ransomware est **l'attaque Wannacry**. Cette dernière est à ce jour la plus grande attaque ransomware de l'Histoire touchant plus de 150 pays différents dont la France.

Wannacry est un rançongiciel (ou ransomware) qui a été découvert en mai 2017 et qui a rapidement infecté des centaines de milliers d'ordinateurs dans le monde entier. Il a utilisé une vulnérabilité dans les systèmes d'exploitation Microsoft Windows pour se propager. Si cette faille avait déjà été découverte par le *National Security Agency (NSA)*, elle a été rendue publique par un groupe de hackers appelé *Shadow Brokers*.

Le ransomware a été conçu pour chiffrer les fichiers sur les ordinateurs infectés et demander une rançon en échange de la clé de déchiffrement. Les victimes étaient invitées à payer en utilisant des crypto-monnaies, ce qui rendait ainsi les paiements difficiles à retracer.

Wannacry a infecté des ordinateurs dans plus de 150 pays et a touché de nombreuses organisations, notamment des hôpitaux, des entreprises et des services publics. Les conséquences de cette attaque ont été très importantes, car elle a entraîné des pertes financières considérables, la paralysie de certains services essentiels, ainsi qu'une perte de confiance des utilisateurs envers les systèmes informatiques.

Le coût de cette attaque est difficilement estimable car on ne peut savoir le coût réel subi par les entreprises, néanmoins, on note que le total des rançons payées s'élèvent à environ 80 000 £. Parmi les grandes entités touchées, on note FedEX, Renault, le ministère de l'Intérieur russe, le service National de Santé (NHS) au Royaume-Uni. Pour ce dernier, on évalue la perte à environ 109 M€.

Les experts en sécurité ont découvert que le rançongiciel avait été créé par un groupe de hackers nord-coréens connu sous le nom de Lazarus Group. Ils ont également découvert que la propagation rapide de WannaCry avait été facilitée par le fait que de nombreux ordinateurs n'avaient pas été mis à jour avec les derniers correctifs de sécurité de Microsoft.

Cette attaque a mis en évidence la vulnérabilité des infrastructures informatiques dans le monde entier et a incité les gouvernements et les entreprises à renforcer leur sécurité informatique. Elle a également souligné l'importance de maintenir les systèmes informatiques à jour avec les dernières mises à jour de sécurité pour prévenir de telles attaques à l'avenir.

2.5.2 Le phishing ou hameçonnage

L'objectif du phishing est d'usurper l'identité d'une personne ou d'une entreprise afin de récolter des informations personnelles ou professionnelles (comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux. Il s'agit d'une forme d'attaque utilisant des emails, des messages texte, des appels téléphoniques ou des sites web frauduleux pour tromper les utilisateurs en leur faisant croire qu'ils communiquent avec une entité de confiance. Les attaquants peuvent ensuite utiliser les informations récoltées pour effectuer des transactions frauduleuses, voler de l'argent

ou accéder à des comptes sensibles.

Les attaques de phishing sont souvent hautement ciblées et personnalisées, utilisant des informations obtenues à partir de sources telles que les réseaux sociaux et les bases de données de clients volées. Les messages de phishing sont conçus pour paraître légitimes, en utilisant des logos et des graphiques de marques populaires, des adresses email et des URL similaires aux sites web authentiques, et un langage persuasif pour inciter l'utilisateur à agir rapidement.

Les mesures de prévention du phishing incluent l'éducation des utilisateurs sur les techniques d'attaque, la sensibilisation aux signes avant-coureurs tels que les erreurs de grammaire et d'orthographe, les demandes de renseignements personnels non sollicitées et les adresses de courriel suspectes, ainsi que l'utilisation d'outils de filtrage de courrier indésirable et d'anti-virus pour bloquer les messages et les sites web malveillants.

En cas de suspicion d'une attaque de phishing, il est important de ne pas répondre ou de cliquer sur les liens suspects, de signaler les messages frauduleux aux fournisseurs de messagerie ou aux autorités compétentes, et de surveiller les activités de compte pour détecter toute activité suspecte.

Ce type d'attaque, bien que moins propice à des attaques de très grande échelle, sont souvent les plus dangereuses pour les petites et moyennes entreprises : en effet, le facteur humain entre en jeu et les PME ont tendance à penser que du fait de leur petite taille et de la nature ciblée du phishing, elles ne seront pas ciblées par ce type d'attaque.

2.5.3 Wiper : exemple de NotPetya

Les wipers (ou destructeurs de données) sont des programmes malveillants conçus pour supprimer ou détruire des données sur les disques durs et les systèmes informatiques. Contrairement aux ransomwares qui cryptent les données pour les rendre inaccessibles, les wipers effacent complètement les fichiers, ce qui les rend irrécupérables. Les wipers peuvent être utilisés pour effacer des fichiers critiques d'un système, ou même pour effacer complètement un disque dur.

Les wipers ont été utilisés dans plusieurs attaques notables, notamment contre des organisations gouvernementales, des entreprises et des réseaux informatiques critiques. En 2012, une attaque

utilisant un wiper appelé Shamoon a visé le géant pétrolier saoudien Aramco, détruisant plus de 30 000 ordinateurs et rendant les systèmes inutilisables pendant plusieurs semaines. En 2014, une autre attaque à l'aide d'un wiper, appelé DarkSeoul, a visé plusieurs banques et médias sud-coréens.

Les wipers sont souvent utilisés pour des attaques ciblées, car ils peuvent causer des dégâts importants et permanents. Les auteurs d'attaques utilisant des wipers peuvent être motivés par des raisons politiques, économiques ou idéologiques.

Pour se protéger contre les wipers, il est recommandé de mettre en place des mesures de sécurité robustes, notamment des sauvegardes régulières des données, des mises à jour de sécurité régulières, l'utilisation de logiciels de détection d'intrusion et la formation des employés à la cybersécurité. En cas d'attaque, il est important de réagir rapidement en isolant les systèmes infectés et en récupérant les données à partir des sauvegardes.

Il est également recommandé de surveiller de près les menaces potentielles, notamment en utilisant des outils de surveillance de la menace et en restant à l'affût des nouvelles vulnérabilités et des attaques en cours.

Enfin, il est important de signaler tout incident de sécurité aux autorités compétentes afin de prendre les mesures appropriées pour enquêter et poursuivre les auteurs d'attaques.

NotPetya est une attaque wiper ayant eu lieu en juin 2017 d'abord en Ukraine puis dans divers autres pays. Les dommages de cette attaques sont estimés à environ 10 Md $, elle a touché plus de 2 000 entreprises dans le monde comme par exemple : A.P. Moller - Maersk, laboratoire pharmaceutique Merck, TNT, Express (filiale de FedEx), Mondelez International.

En France, l'attaque a occasionné une perte de 220M€ de chiffre d'affaire pour l'entreprise de construction Saint-Gobain.

2.5.4 Les attaques "DDos" (*Distributed Denial of Service*)

Une attaque DDoS (*Distributed Denial of Service*) est une méthode d'attaque qui vise à rendre inaccessible un service, un site web ou une application en le submergeant d'un grand nombre de requêtes simultanées, émanant de milliers d'ordinateurs infectés à travers le monde. Le but est d'épuiser les ressources du serveur cible pour le rendre indisponible.

Les attaques DDoS peuvent être menées de différentes manières, notamment par des botnets, des réseaux d'ordinateurs infectés à distance par un attaquant, qui sont ensuite utilisés pour envoyer des requêtes simultanées vers la cible. Les attaquants peuvent également utiliser des techniques de spoofing pour masquer l'origine des requêtes et rendre plus difficile la détection et le blocage de l'attaque.

Les conséquences d'une attaque DDoS peuvent être graves pour les entreprises et les organisations ciblées, qui peuvent subir des pertes financières importantes en raison de l'indisponibilité de leurs services en ligne. De plus, les attaques DDoS peuvent avoir des conséquences négatives sur la réputation de l'entreprise et la confiance de ses clients.

Pour se protéger contre les attaques DDoS, les entreprises doivent utiliser des services de protection DDoS proposés par des fournisseurs spécialisés, qui permettent de filtrer le trafic malveillant et d'atténuer ainsi les attaques en temps réel. Les entreprises peuvent également mettre en place des mesures de prévention, telles que la limitation du nombre de connexions simultanées et la surveillance de leur trafic réseau pour détecter les signes d'une attaque imminente.

En résumé, une attaque DDoS est une méthode d'attaque qui vise à rendre inaccessible un service en submergeant la cible avec un grand nombre de requêtes simultanées. Les conséquences peuvent être graves pour les entreprises ciblées, mais il existe des mesures de protection et de prévention pour réduire le risque d'attaques réussies.

Un exemple de DDoS est l'attaque massive qui a touché le site de streaming vidéo Netflix en 2016. Cette attaque a été menée par le botnet Mirai, qui a utilisé des millions d'appareils connectés à Internet, tels que des caméras de sécurité et des routeurs, pour saturer le site de trafic et le rendre inaccessible aux utilisateurs légitimes. L'attaque a duré plusieurs heures et a nécessité une

intervention importante de la part de Netflix et de ses fournisseurs de services pour résoudre le problème.

2.6 Comprendre une cyber attaque

Avant de développer des méthodes de quantification du risque cyber, il faut d'abord s'intéresser au processus d'intrusion d'un virus dans un système informatique. Le ***kill chain***, également connu sous le nom de chaîne de l'attaque, est un modèle conceptuel utilisé pour décrire les différentes étapes d'une attaque informatique. Ce modèle est souvent utilisé dans le cadre de la cybersécurité pour aider les entreprises à comprendre comment les attaquants agissent et pour mettre en place des mesures de sécurité efficaces.

Le modèle du *kill chain* comprend généralement les étapes suivantes (**Figure 4.1**) :

- **Repérage (*Reconnaissance*)** : L'attaquant recueille des informations sur sa cible pour en savoir plus sur les vulnérabilités potentielles qu'il peut exploiter.
- **Évaluation (*Weaponization*)** : L'attaquant évalue les informations recueillies pour déterminer les meilleures méthodes d'attaque et les outils à utiliser.
- **Livraison (*Delivery*)** : L'attaquant envoie les charges utiles malveillantes à la cible, souvent via des emails de phishing ou des pages web malveillantes.
- **Exploitation (*Exploitation*)** : Les charges utiles malveillantes sont exécutées sur la machine de la victime, permettant à l'attaquant de prendre le contrôle de la machine ou d'accéder à des informations sensibles.
- **Installation (*Installation*)** : L'attaquant installe des logiciels malveillants supplémentaires pour assurer un accès à long terme au système compromis.
- **Commande et contrôle (*Command and Control*)** : L'attaquant établit un canal de communication avec le système compromis pour commander et contrôler les activités malveillantes.
- **Actions (*Actions*)** : L'attaquant effectue diverses actions malveillantes, telles que la collecte d'informations sensibles, le vol de données, le sabotage, etc.

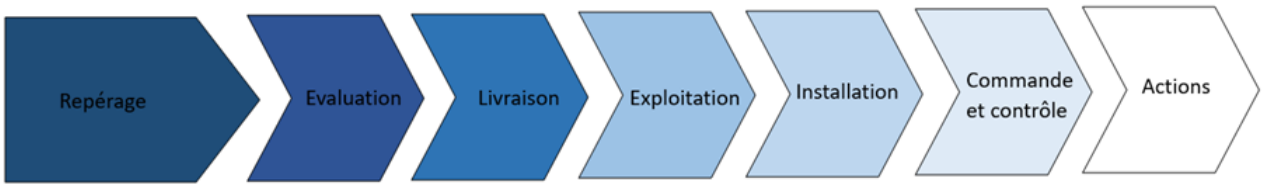

FIGURE 2.3 – Graphique explicatif du processus Kill chain

Le modèle de la *kill chain* permet aux entreprises de mieux comprendre les étapes clés de l'attaque, de détecter les activités suspectes et de prendre des mesures de sécurité pour prévenir ou limiter les dommages causés par une attaque. En utilisant des techniques telles que la surveillance de la sécurité des réseaux, les tests de pénétration et l'analyse des journaux, les entreprises peuvent réduire leur vulnérabilité à ces types d'attaques.

Un autre terme à bien comprendre est la notion de "pivot". Il correspond à une technique utilisée par les attaquants pour se déplacer latéralement à travers un réseau informatique après avoir compromis un ou plusieurs ordinateurs.

Par ailleurs, une fois qu'un pirate informatique a réussi à accéder à un ordinateur ou à un serveur sur un réseau, il utilise souvent cette première position comme point de départ pour explorer et attaquer d'autres machines sur le même réseau. Il peut le faire en utilisant des outils de piratage ou en exploitant des vulnérabilités dans les systèmes cibles.

Le pivot permet à l'attaquant de se déplacer discrètement à travers le réseau, en évitant les mesures de sécurité et en recueillant des informations sensibles. Il peut également utiliser cette technique pour installer des logiciels malveillants ou pour prendre le contrôle de systèmes distants.

Pour se prémunir contre les pivots, les entreprises doivent mettre en place des mesures de sécurité appropriées, telles que la segmentation de réseau, l'authentification multi-facteurs, le contrôle d'accès, la surveillance du trafic réseau, et la mise à jour régulière des systèmes et des logiciels.

Chapitre 3

Produit cyber envisagé

3.1 Condition de souscription

Le produit cyber assuré par Acheel est un produit spécifiquement pensé pour les PME. Au vu de l'exposition de ces derniers face à ce risque majeur, leur proposer une couverture était indispensable. Afin de souscrire à cette couverture, l'entreprise passe par un scan externe qui va dresser le profil de risque de l'entreprise. Ce scan externe permet de récupérer des données en libre accès sur internet à partir du nom de domaine de l'entreprise. Cet outil présente deux avantages : il permet à la PME de connaître ses faiblesses en terme de cyber sécurité mais aussi à l'assureur d'avoir une bonne vision du comportement de ses clients face au risque et de pouvoir ensuite ajuster sa prime en fonction et de proposer ainsi une assistance afin d'augmenter la protection de la PME envers les risques Cyber.

Après avoir passé ce scan, d'autres conditions de souscription sont à valider :

- Procéder à des sauvegardes des données au moins toutes les 2 semaines ;
- Être muni d'un antivirus à jour sur tous les postes de travail et serveurs Windows ;
- Réaliser un chiffre d'affaire inférieur à 50 millions d'euros dont moins de 30 % se fait aux USA ou au Canada ;

— Ne pas faire parti des secteurs d'activités dits à risque (liste dans le tableau 5.4 en annexe).

3.2 Les garanties couvertes

Après validation des prérequis cités plus haut, l'entreprise ayant souscrit un contrat est couverte pour les garanties présentées ci-dessous :

3.2.1 Services d'urgence liés à la gestion de crise

Après une attaque, la prise en charge de plusieurs intervenant est comprise dans les garanties avec pour chacun des missions :

- Un expert informatique afin de faire des recommandations pour :
  - identifier, analyser et contenir l'atteinte malveillante ;
  - mettre fin à l'atteinte malveillante ;
  - prévenir une atteinte malveillante similaire ;
  - prévenir une future atteinte malveillante en cas d'erreur humaine.
- Un expert juridique pour fournir des conseils relatifs :
  - à l'obligation de notification à l'autorité administrative et aux échanges avec celle-ci ;
  - aux obligations de notification aux personnes concernées.
- Un conseiller en communication de crise avec pour missions, si nécessaire, d'élaborer et de mettre en oeuvre une stratégie de communication de crise visant à prévenir ou limiter l'atteinte de la réputation de l'entreprise.

3.2.2 Garantie en cas d'atteintes aux données

Dans le cas où les données d'une entreprise ont été atteintes par un tiers, l'assureur prend en charge :

- Les frais de notification aux personnes concernées ;

— Les frais de surveillance qui permettent de détecter et contrôler toute utilisation non conforme des données personnelles ;
— Les frais de défense et les conséquences pécuniaires résultant de toute réclamation liée à des dommages immatériels.

3.2.3 Garantie en cas d'atteintes au système informatique

En cas d'attaque malveillante par un tiers impliquant une détérioration du système informatique : la reconstruction ou reconstitution des données à partir des sauvegarde, ainsi que la remise à niveau du système informatique dans l'état d'origine sont garantis par la couverture d'assurance.

3.2.4 Garanties pertes d'exploitation en cas d'altération du système informatique

Il s'agit ici du cas où le système informatique de l'entreprise venait à cesser ou à se dégrader suite à une attaque.

Les pertes de marge brute d'exploitation directement consécutives à l'arrêt du système sont prises en charge. L'assureur interviendra sur la base de la marge brute d'exploitation que l'entreprise aurait dû réaliser en temps normal. Les frais supplémentaires d'exploitation visant à limiter l'impact de l'atteinte malveillante sur les pertes de marge brute d'exploitation sont aussi couverts.

Chapitre 4

Tarification

Dans ce chapitre, nous allons proposer des solutions de tarification d'un produit de risque cyber tel que défini dans la partie 3.

4.1 Stratégie adoptée face à la jeunesse du risque

Le risque cyber étant encore peu développé, nous disposons de très peu de données. C'est pourquoi nous avons choisi de faire appel a un cabinet de conseil spécialisé dans l'accompagnement des entreprises face au risque cyber. Cette société est spécialisée dans la prévention des risques des systèmes d'information mais également dans la résolution d'évènements de cyber-sécurité. En tant qu'assisteur en cas de cyber attaque, cette société dispose d'une grande expérience dans l'évaluation du risque cyber, en particulier dans l'impact de la mise en place de système de sécurité (MFA, pentest, test de phishing ...) et sur la fréquence d'une attaque cyber.

Nous avons donc sélectionné certaines variables que nous qualifions de significatives, pour lesquelles nous décidons d'attribuer un coefficient qui viendra personnaliser notre évaluation du risque de chaque entreprise en fonction du niveau de cyber-sécurité. Ces coefficients sont déterminés soit à dire d'expert (basé sur l'impact historique observé par les assisteurs), soit comme une fonction des paramètres de sécurité de l'entreprise.

Nous avons également décidé de souscrire un traité de réassurance spécifique pour ce nouveau produit Cyber. Ainsi la grande majorité de notre sinistralité sera portée par un réassureur. De cette manière, nous pouvons récolter suffisamment de données de souscriptions et de sinistralités, sans mettre en danger la perenité d'Acheel, afin de pouvoir réajuster le modèle de tarification dans un second temps et progressivement réduire la cession au réassureur d'une année sur l'autre.

4.2 Première approche : Modèle coût/fréquence

Une première approche que l'on pourrait qualifier de naïve est de faire payer à l'assuré le coût moyen de son risque, c'est-à-dire son espérance. Cependant, compte tenu que tous les risques ne sont pas identiques, il est ainsi nécessaire de prendre en compte les variables propres à chaque assuré. En notant Ω_i l'ensemble des informations disponibles pour l'assuré i, sa prime pure sera égale à $\mathbb{E}(X|\Omega_i)$, avec X étant la variable aléatoire décrivant le comportement de l'assuré.

Parmi les différentes conséquences énumérées dans la Partie 2.2.2, les deux principales conséquences d'une attaque cyber que nous décidons de retenir afin de quantifier notre risque de manière déterministe sont la **fuite d'information** ainsi que **l'interruption ou dégradation de l'activité**.

Pour cela nous allons considérer 2 scénarios :

- La premier étant l'atteinte au système informatique menant à un perte d'exploitation.
- Le second scénario est un scénario perte de données.

Afin d'obtenir une tarification de ces 2 scénarios il faut déterminer l'ensemble des informations disponibles et influant sur la posture de risque de l'assuré.

4.2.1 Description des informations disponibles de l'assuré

Nous avons réuni plusieurs informations nécessaires à la tarification : tout d'abord des données liées à l'activité de l'entreprise. Nous avons ainsi besoin du **chiffre d'affaire annuel** de l'entreprise, du **nombre de jour d'activité**, de son **secteur d'activité** et de son **taux de marge brute**.

En effet, le taux de marge brute d'une entreprise est un indicateur financier important qui mesure la rentabilité d'une entreprise. Il représente la différence entre les revenus générés par l'entreprise et le coût direct de production de ses biens ou services.

Le taux de marge brute est calculé en soustrayant le coût des ventes (Coût des marchandises vendues ou coût des services fournis) du chiffre d'affaires total, puis en divisant le résultat par le chiffre d'affaires total, exprimé en pourcentage. La marge brute est considérée comme un indicateur clé de la performance de l'entreprise car elle indique la capacité de l'entreprise à générer des bénéfices avant de prendre en compte les autres coûts de l'entreprise, tels que les coûts de marketing, de vente, d'administration et autres frais généraux.

Un taux de marge brute élevé indique que l'entreprise a une forte rentabilité et une capacité à couvrir ses coûts de production et à générer des bénéfices. À l'inverse, un taux de marge brute faible peut indiquer que l'entreprise a des problèmes de rentabilité ou de compétitivité sur le marché.

Le taux de marge brute peut varier selon le secteur d'activité et la stratégie de l'entreprise. Par exemple, les entreprises ayant une stratégie de prix bas peuvent avoir un taux de marge brute plus faible que les entreprises offrant des produits ou services de qualité supérieure à un prix plus élevé. Il permet d'évaluer le risque en cas de cyber attaque.

Ensuite, un autre pilier à analyser est la maturité cybersécurité de l'entreprise, pour cela nous allons nous intéresser à 5 facteurs : le **nombre de postes de travail**, le **nombre de serveurs**, le **coefficient de maturité cyber**, le **niveau de dépendance à l'IT** et le **temps d'incidence**. Par temps d'incidence, nous entendons la durée moyenne durant laquelle le système informatique est hors service après une attaque.

Le niveau de dépendance à l'IT (Information Technology ou Technologie de l'Information) d'une entreprise correspond à la mesure dans laquelle l'entreprise dépend des technologies de l'information pour son fonctionnement quotidien. Plus précisément, cela se réfère à la dépendance des processus opérationnels, de la prise de décision et de la compétitivité de l'entreprise vis-à-vis de l'utilisation de la technologie de l'information.

Dans la plupart des entreprises modernes, les systèmes informatiques sont devenus une partie intégrante des opérations quotidiennes et de la stratégie d'entreprise. Par conséquent, une panne ou un dysfonctionnement de ces systèmes peut avoir des conséquences très négatives pour l'entreprise, notamment une interruption de la production, une perte de données, une baisse de la productivité, une diminution de la satisfaction clientèle, une perte de revenus, une perte de réputation, et même une mise en danger de la sécurité et de la confidentialité des données.

Pour mesurer le niveau de dépendance à l'IT d'une entreprise, on peut prendre en compte différents critères, tels que :

- la proportion des processus opérationnels de l'entreprise qui sont informatisés ;
- la part des données critiques stockées dans des systèmes informatiques ;
- le nombre d'employés dépendants de la technologie pour effectuer leur travail ;
- la part des ventes ou des revenus liés aux activités en ligne ;
- le niveau d'automatisation des processus métiers ;
- la dépendance aux systèmes tiers (par exemple, les services de cloud computing ou les fournisseurs de logiciels).

Plus la dépendance à l'IT est élevée, plus l'entreprise est vulnérable aux risques liés aux technologies de l'information. Pour atténuer ces risques, il est important pour les entreprises de mettre en place des stratégies de gestion des risques de cybersécurité, de planification de la continuité des activités, et de diversification des systèmes et des fournisseurs.

Le troisième pilier que nous avons dégagé est le nombre de données que détient l'entreprise. Nous retenons 3 types de données : les **PII (Personnal identifial information)**, **PCI (Payment card information)**, **PHI (Protected health information)**.

Les données PII, PCI et PHI sont toutes des types de données sensibles qui nécessitent une protection particulière pour garantir la confidentialité, l'intégrité et la sécurité.

- PII (Informations personnellement identifiables) : Les PII sont des informations qui peuvent être utilisées pour identifier directement une personne individuelle, telles que le nom, l'adresse,

le numéro de sécurité sociale, le numéro de téléphone, l'adresse e-mail, le numéro de permis de conduire, etc. Les PII sont réglementées par des lois telles que le Règlement général sur la protection des données (RGPD) et le Privacy Act.

— PCI (Données de cartes de crédit) : Les PCI sont des informations qui sont liées aux cartes de crédit et de débit, telles que le numéro de carte, la date d'expiration, le code de sécurité, etc. Les PCI sont réglementées par les normes de sécurité de l'industrie des cartes de paiement (PCI-DSS) pour protéger les informations de paiement des clients et éviter les fraudes.
— PHI (Informations de santé protégées) : Les PHI sont des informations liées à la santé d'une personne, telles que les dossiers médicaux, les diagnostics, les traitements, les ordonnances, etc. Les PHI sont réglementées par la loi sur la responsabilité et la portabilité de l'assurance maladie (HIPAA) aux États-Unis pour garantir la confidentialité et la sécurité des informations de santé des patients.

Pour protéger ces types de données sensibles, il est essentiel de mettre en place des politiques de sécurité rigoureuses, telles que la cryptographie, l'authentification et l'autorisation, la surveillance des accès et l'audit des logs. Les organisations doivent également former leur personnel sur les meilleures pratiques de sécurité et mettre en place des procédures de gestion des incidents pour détecter et gérer les violations de sécurité éventuelles.

Enfin, nous déterminons les fréquences d'occurrences des différents scénario à savoir : une perte d'exploitation totale, une perte de données, un procès à la suite d'une perte de données ; ainsi que le coût de restauration endpoint.

Un endpoint est un point de terminaison dans une architecture de système informatique ou d'API *(Application Programming Interface)*. Il s'agit d'un point d'entrée ou de sortie pour une application, une interface ou un service, qui peut être utilisé pour accéder à des ressources ou des fonctionnalités spécifiques.

Une API *(Application Programming Interface)* est un ensemble de protocoles, de routines et d'outils logiciels permettant à différentes applications informatiques de communiquer entre elles. En d'autres termes, une API fournit un moyen standardisé pour que les développeurs puissent accéder à certaines fonctionnalités ou données d'une application (ou d'un système) à partir d'une autre

application, sans avoir à connaître les détails de la mise en œuvre de l'application sous-jacente.

Les API sont largement utilisées pour créer des intégrations entre différents systèmes et services, pour automatiser des processus, pour partager des données, pour créer des applications tierces, et pour bien d'autres cas d'utilisation.

Dans le contexte des API, un endpoint est généralement une URL qui représente une ressource spécifique ou une fonctionnalité disponible via l'API. Les clients peuvent accéder à ces endpoints en envoyant des requêtes HTTP avec des méthodes spécifiques, telles que GET, POST, PUT ou DELETE, et des paramètres pour spécifier les actions à effectuer ou les données à récupérer.

Les endpoints peuvent être conçus pour prendre en charge différents types d'opérations et de formats de données, tels que JSON, XML, HTML, etc. Les développeurs peuvent également sécuriser les endpoints en utilisant des protocoles de sécurité tels que HTTPS, OAuth, JWT, etc.

L'utilisation efficace des endpoints est importante pour garantir des performances et une sécurité optimales de l'application ou de l'API. Les développeurs doivent concevoir des endpoints qui répondent aux besoins des utilisateurs tout en limitant les risques de sécurité, en évitant les erreurs et en fournissant des réponses rapides et précises.

Les différents coefficients tarifants sont résumés dans le tableau ci-dessous :

Activités de l'entreprise	**Cybersécurité**
CA	Nombre de postes de travail
Taux de marge brute	Nombre de serveurs
Activité	Coefficient de maturité cyber
Nombre de jour d'activité	Temps d'incidence
	Niveau de dépendance à l'IT
Données	**Fréquences et coût**
Coût et nombre de PII	Procès à la suite d'une perte de données
Coût et nombre de PCI	Perte d'exploitation totale
Coût et nombre de PHI	Occurence d'un sinistre perte de données
	Coût restauration endpoint

Table 4.1 – Récapitulatif des paramètres de la tarification

4.2.2 Scénario 1 : Perte d'exploitation

La première étape de calcul de ce scénario est la détermination de la perte d'exploitation maximale qu'une attaque cyber peut engendrer. En effet, la perte d'exploitation pour une entreprise est la diminution du chiffre d'affaires et du bénéfice résultant d'un événement imprévu qui interrompt temporairement ou définitivement les activités de l'entreprise.

La perte d'exploitation est un risque majeur pour toutes les entreprises, car elle entraîne des coûts élevés pour l'entreprise. Elle peut engendrer une diminution des revenus, des pertes de production, une baisse de la qualité des produits ou services, et une perte de clients, ce qui peut mettre en péril la viabilité financière de l'entreprise.

Pour mesurer l'ampleur de la perte d'exploitation, il est important d'estimer la durée de l'interruption, les coûts associés à la reprise de l'activité, les pertes de revenus, les dépenses engagées pour maintenir les activités pendant la période d'interruption et les coûts liés à la mise en place d'un plan de continuité des activités.

En résumé, la perte d'exploitation est un risque majeur pour toutes les entreprises, et il est important de bien évaluer les coûts et les impacts d'une interruption des activités pour mettre en place des mesures de prévention et de gestion des risques appropriées, et se prémunir avec une assurance perte d'exploitation.

Pour cela, la première étape est de calculer le chiffre d'affaire journalier, ainsi que la perte effective journalière :

$$\boxed{\text{CA journalier} = \frac{\text{Chiffre Affaire}}{\text{Nombre de jours d'activité}}}$$

et :

$$\boxed{\text{Perte effective journalière} = \text{CA journalier} \times \text{Niveau dépendance IT} \times \text{Taux marge brute}}$$

On en déduit ainsi la perte d'exploitation maximale :

$$\boxed{\text{Perte exploitation maximale} = \text{Perte effective journalière} \times \text{Temps incidence}}$$

Après avoir déterminé la perte d'exploitation, il faut déterminer les différents frais que la remise en service de l'activité coûte, ainsi on a :

$$\boxed{\text{Frais réponse} = \text{Coût frais réponse} \times \text{Temps incidence}}$$

et :

$$\boxed{\text{Frais restauration endpoints} = \text{Coût restauration endpoints} \times (\text{Nombre serveur + Nombre postes})}$$

Enfin on calcule la perte maximale totale à laquelle peut faire face une entreprise en cas de cyber attaque dans le cas du scénario 1 :

$$\boxed{\text{Perte max totale 1} = \text{Perte exploitation maximale} + \text{Frais réponse} + \text{Frais restauration endpoints}}$$

4.2.3 Scénario 2 : Perte données

Le second scénario que nous prenons en compte dans la tarification est la perte de donnée suite à une attaque cyber. Ainsi, nous considérons que chaque donnée perdue a un coût selon son type, nous obtenons ainsi la formule suivante :

$$\boxed{\text{Perte data} = \prod_{i \in I} (\text{Coût}_i * \text{Nombre données}_i)}$$

Avec I = (PII, PCI, PHI)

Les coûts pour chaque types de données peuvent se résumer dans le tableau suivant 4.2, ces coûts ont été déterminés par l'équipe de juristes d'Acheel ainsi que des experts en cybersécurité. Les coûts représentent le coût pour une donnée perdue, cette valeur prend en compte le coût de notification, les frais postaux ...

	Coût
PII	10 €
PCI	25 €
PHI	25 €

TABLE 4.2 – Perte engendrée selon le type de données leakée

On détermine ainsi la perte espérée pour le scénario 2 :

$$\boxed{\text{Perte max totale } 2 = \text{Perte data}}$$

4.2.4 Tarification finale

Dans la partie précédente, nous avons déterminé les pertes totales pour les deux scénarii décrits. Nous allons désormais introduire la perte maximale totale pour l'assureur. Pour ce faire, il faut introduire la franchise ainsi que la limite. La limite représente la valeur maximale que l'assureur sera amené a indemniser en cas de sinistre. La franchise, elle, est le montant qui reste à la charge de l'assuré en cas de sinistre. Ces deux valeurs sont définies contractuellement lors de la souscription du contrat d'assurance. Ainsi, nous obtenons :

$$\boxed{\textbf{Perte max totale} = \min(\text{Perte max totale } 1 + \text{Perte max totale } 2 - \text{Franchise}; \text{Limite})}$$

Nous pouvons désormais définir la prime pure

$$\boxed{\textbf{Prime pure} = \text{Coefficient activité} \times \text{Coefficient Cybersécurité} \times \text{Perte max totale}}$$

Enfin, nous allons déterminer la prime technique, c'est à dire la prime pure à laquelle nous ajoutons des chargements :

$$\boxed{\textbf{Prime technique} = \text{Prime pure} + \text{Chargement}}$$

Enfin, afin de calculer la prime que l'assuré va payer, il suffit d'ajouter les taxes. Dans le cas du cyber, la taxe est de 9% à laquelle s'ajoute 5,90€ correspondant à la contribution au Fonds de garantie des victimes des actes de terrorisme et d'autres infractions (pour les contrats d'assurance de biens).

$$\boxed{\textbf{Prime TTC} = \text{Prime technique} \times (1 + 9\%) + 5,90}$$

4.2.5 Positionnement de la tarification proposée avec d'autres acteurs du marché

Afin d'observer la pérennité de la tarification effectuée, un benchmark a été réalisé sur certaines entreprises afin de comparer le tarif Acheel avec le tarif de certains concurrents. Ainsi, les tarifs TTC de 7 profils ont été comparées.

	Acheel	Concurrence*	Particularité
Assuré 1	26k€	28k€	Acheel propose une limite à 2m€ tandis que le concurrent propose 3m€.
Assuré 2	40k€	49k€	Acheel propose une limite à 2m€ tandis que le concurrent propose 5m€.
Assuré 3	48k€	46k€	Les 2 offres sont à garanties égales.
Assuré 4	28,5k€	25,6k€	Les 2 offres sont à garanties égales.
Assuré 5	42k€	45k€	Acheel propose une franchise à 50k€ tandis que le concurrent propose 100k€.
Assuré 6	21k€	15,5k€	Les 2 offres sont à garanties égales.
Assuré 7	25k€	26k€	Acheel propose une limite à 1m€ tandis que le concurrent propose 1,5m€.

Table 4.3 – Benchmark positionnement tarification 1

**Tarif moyen des 5 plus gros acteurs de marché (Hiscox, Marsh, AON, Chubb, Axa)*

L'écart moyen constaté est de 1,96 %. La tarification fournie est ainsi une tarification exploitable et viable dans un marché encore peu concurrentiel.

4.2.6 Limite de cette méthode

Ce modèle bien que très simple de tarification permet d'avoir une vision d'ensemble des différents facteurs à prendre en compte afin de tarifer un risque cyber. Néanmoins, nous rencontrons plusieurs limites dans ce modèle. Tout d'abord, les coefficients liés à l'activité et à la cybersécurité sont déterminés par des experts en cybersécurité. Ainsi, afin de tarifer ce risque, la présence d'un expert est requise, ce qui n'est pas toujours possible et qui rend le tarificateur difficilement implémentable et automatisable. Un autre point bloquant dans cette méthode est le fait que la limite de souscription n'est pas prise en compte dans le calcul de la prime.

Néanmoins, cette méthode de tarification s'avère assez robuste pour fournir un tarif sur des risques marginaux dépassant les limites de souscription du produit. De plus, on constate que son positionnement tarifaire sur le marché est assez bon.

4.3 Deuxième approche

La première approche de la tarification du risque cyber a permis de faire un état des lieux des différents facteurs tarifant pour un produit d'assurance cyber.

En effet, l'exposition d'une PME au risque cyber dépend de nombreux facteurs, la posture de risque d'une petite entreprise régionale dans l'agriculture ne sera pas la même qu'une entreprise en télécommunication.

Ainsi, les caractéristiques de l'entreprise que nous retenons comme élément tarifant sont les suivants :

- Secteur d'activité
- Chiffre d'affaire
- Nombre d'employés

Ensuite, il faut déterminer la posture de risque de l'entreprise. Pour cela, deux variables vont être construites : la **maturité externe** et la **maturité interne**, ces 2 variables seront décrites plus bas dans la partie 4.3.1

Grâce à l'expertise et aux données transmises par notre réassureur, nous avons fait une étude de marché permettant de déterminer la prime pure moyenne de la cyber assurance sur le marché français.

Une fois le coût moyen du risque déterminé, les différents coefficients d'impact vont nous permettre de quantifier pour chaque assuré sa prime.

Ainsi, la prime pour une entreprise i se détermine de la manière suivante :

$$\boxed{\text{Prime pure assuré } i = \text{Prime pure moyenne} \times \prod_{j \in A_i} \text{Impact}_j}$$

avec A_i = (Maturité, Chiffre d'affaire, Secteur d'activité, Limite), le profil de risque de l'entreprise.

Pour rappel, la prime pure en assurance correspond à la portion de la prime totale qui est calculée en fonction du risque sous-jacent, sans prendre en considération les frais administratifs, les coûts de gestion ou les frais de l'assureur ou même d'un chargement de sécurité. Ainsi, la prime pure représente le coût estimé du dit risque assuré. Cette valeur est calculée en évaluant les risques et les probabilités de sinistres, en se basant sur des données statistiques et des modèles mathématiques.

Dans les parties suivantes nous allons déterminer les différents coefficients d'impact qui vont venir choquer la prime pure moyenne.

4.3.1 Détermination des variables de posture de risque et de leur impact sur le tarif

Afin de quantifier la maturité d'une entreprise face au risque cyber, un questionnaire a été mis en place dans le but de récolter les informations nécessaires à la quantification du risque :

- Des pentests ou audit de sécurité sont-ils réalisés au moins 2 fois par an ?
- Des campagnes de phishing sont elles organisées à titre préventif au sein de l'entreprise au moins tous les 2 mois ?
- L'entreprise possède-t-elle un MFA (Multi-Factor Authentification) pour se connecter aux mails et aux infrastructures sensibles ?

Dès lors que les menaces externes sont moins prédictibles et qu'il est plus difficile de les empêcher, nous faisons l'hypothèse que l'impact de maturité externe de l'entreprise aura un poids plus élevé dans le tarif final.

Maturité interne

Le coefficient de maturité interne prend en compte les bonnes pratiques de défenses internes particulièrement l'EDR *(Endpoint Detection and Response)*, le patching et la réalisation de pentest.

L'EDR *(Endpoint Detection and Response)* est une solution de sécurité informatique qui permet aux

entreprises de détecter, d'analyser et de répondre aux menaces sur les appareils (endpoints) de leur réseau informatique, tels que les ordinateurs portables, les ordinateurs de bureau, les serveurs et les appareils mobiles.

Les solutions EDR utilisent des technologies avancées telles que l'analyse comportementale et l'intelligence artificielle pour détecter les activités malveillantes sur les endpoints. Ces activités peuvent inclure des attaques de logiciels malveillants, des tentatives d'exfiltration de données, des mouvements latéraux sur le réseau et d'autres types de menaces.

L'objectif principal de l'EDR est de fournir une visibilité et un contrôle granulaires sur les endpoints, ainsi que des fonctionnalités de réponse automatisées pour contenir et éliminer rapidement les menaces. Les solutions EDR sont souvent utilisées en conjonction avec d'autres technologies de sécurité telles que les pare-feux, les systèmes de prévention des intrusions (IPS), les solutions de gestion des informations et des événements de sécurité (SIEM) pour une sécurité complète du réseau informatique d'une entreprise.

Un autre concept à comprendre est le patching. En informatique, c'est le processus de mise à jour ou de correction des vulnérabilités des logiciels installés sur les systèmes informatiques d'une entreprise. Les vulnérabilités sont des failles de sécurité dans le code du logiciel qui peuvent être exploitées par des pirates informatiques pour accéder au système, voler des données sensibles ou causer d'autres types de dommages.

Le patching consiste à appliquer des correctifs logiciels fournis par les éditeurs de logiciels pour corriger ces vulnérabilités et garantir que les systèmes de l'entreprise sont à jour et protégés contre les attaques connues. Les correctifs peuvent inclure des mises à jour de sécurité, des correctifs de bugs et des améliorations de performance.

Le processus de patching peut être manuel ou automatisé, et peut nécessiter un redémarrage des systèmes. Il est généralement effectué en suivant un calendrier de patching régulier, ou en réponse à une vulnérabilité critique ou à une menace de sécurité active.

Un patching régulier est une pratique importante de la sécurité informatique pour les entreprises

car cela contribue à réduire le risque d'attaques informatiques réussies. Les entreprises doivent avoir une politique de patching claire pour garantir que les systèmes sont régulièrement mis à jour avec les dernières mises à jour de sécurité.

Ainsi, afin d'évaluer la posture de l'entreprise, nous devons vérifier la régularité à laquelle l'entreprise effectue un patching. Nous déterminons 4 fréquences : journalière, hebdomadaire, mensuelle et une dernière fréquence qui correspond à un patching avec une fréquence supérieure à mensuelle. A ces fréquences, nous attribuons les coefficients de risque ci dessous :

Quotidienne	-0,99
Hebdomadaire	-0,92
Mensuelle	0,46
Au delà	1

Table 4.4 – Coefficient de fréquence de patching

La fréquence de patching va impacter la quantité de perte de données en cas d'attaque. Si un patching est réalisé de manière quotidienne, en cas de cyber attaque la quantité de données perdue correspondra au pire à un jour. Cependant si le patching est réalisé mensuellement, la quantité de données perdues en cas d'attaque correspondra au pire à 31 jours de données. Partant de ce constat, nous avons construit nos coefficients de risque comme une fonction du nombre de jours de données perdues.

Nous caractérisons la fonction de la manière suivante :

- $f(0) < 0$, on considère que 0 correspond à une fréquence de patching continue, cette valeur est fictive car aucune entreprise ne réalise de sauvegarde continue. De plus, comme nous impactons une prime moyenne basée sur un large panel d'entreprise ayant une couverture cyber et étant donnée que très peu d'entreprises procèdent à des sauvegardes en continue,
- f est croissante et convexe, la convexité de la fonction s'expliquant par le fait que moins il y a de sauvegarde et plus grande sera la difficulté de restaurer l'ensemble du système et/ou des données. La croissance, elle, s'explique de manière assez naturelle : plus la fréquence de patching est irrégulière et plus l'entreprise court un risque.

— Au delà d'un mois, la régularité de patching a un impact négligeable, ainsi la fonction sera constante à partir de 60 jours. Enfin, nous décidons que les entreprises réalisant un patching moins d'une fois dans l'année sont refusés à la souscription.

Nous obtenons ainsi la fonction représentée dans le graphique ci-dessous :

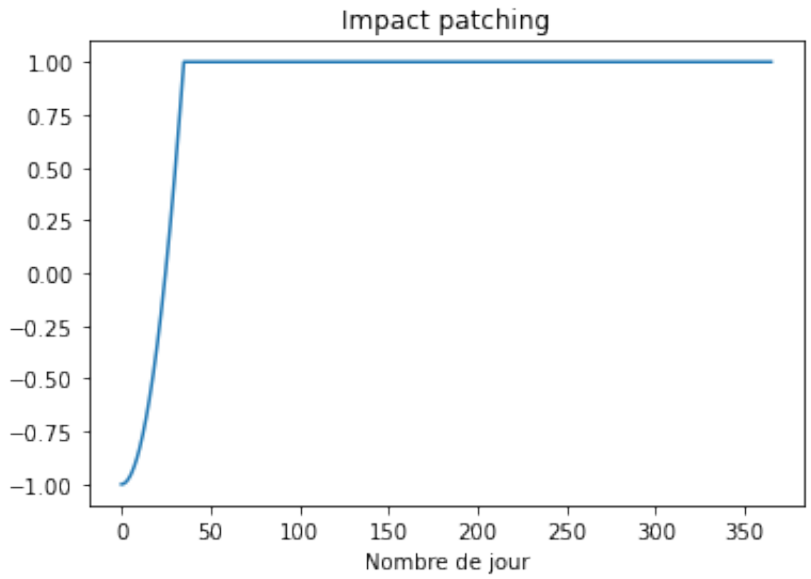

FIGURE 4.1 – Représentation du coefficient d'impact de la fréquence de la réalisation de patching

Un pentest (ou test de pénétration) est une évaluation de la sécurité d'un système informatique, d'un réseau ou d'une application web en simulant une attaque de la part d'un pirate informatique.

Le but d'un pentest est d'identifier les vulnérabilités du système et les failles de sécurité afin de les corriger avant qu'un attaquant réel ne les exploite pour compromettre le système.

Les pentesters utilisent une variété d'outils et de techniques pour tester la résistance du système à différentes attaques, telles que l'ingénierie sociale, l'exploitation de vulnérabilités connues, l'analyse de la sécurité des applications web, le test de la sécurité du réseau, etc.

À la fin du pentest, les résultats sont compilés dans un rapport de test qui contient des recomman-

dations pour améliorer la sécurité du système. Ce rapport est ensuite utilisé par les responsables de la sécurité informatique pour corriger les failles de sécurité identifiées et pour renforcer la sécurité globale du système.

En fonction de la régularité de pentest effectués nous appliquons les coefficient suivants :

Au moins 2 fois par an	-0,2
Moins de 2 fois par an	0,2

TABLE 4.5 – Coefficient de fréquence de pentest

D'après le réassureur, nous devions avoir un coefficient d'environ 0,2. De plus, nous voulions avoir une symétrie entre les 2 paramètres étant donné que leur impact est opposé, un montre une certaine prévention du risque tandis que le second cas de figure (des pentests réalisés moins de 2 fois par an) montre une certaine fragilité du système informatique.

On obtient ainsi :

$$\boxed{\textbf{Maturité interne} = 1 + 0,02 \times (\text{Coefficient pentest} + \text{Coefficient patching})}$$

Maturité externe

Le coefficient de maturité externe prend, lui, en compte les bonnes pratiques de défenses externes (pentest, test de phishing, MFA) et la taille de l'entreprise.

Nous reprenons le même coefficient de pentest que mentionné 4.5.

Des tests de phishing, doivent être réalisés au sein de l'entreprise afin d'évaluer l'aptitude des employés à détecter des mails frauduleux. Nous déterminons ainsi les coefficients selon si l'entreprise réalise des test de phishing au moins tous les 2 mois :

Oui	1
Non	0,3

Table 4.6 – Impact de la réalisation de tests de phishing tous les 2 mois

Un autre point d'analyse est : le MFA qui signifie "authentification multi-facteurs" en français, c'est un mécanisme de sécurité qui exige des utilisateurs qu'ils fournissent deux ou plusieurs formes d'authentification pour vérifier leur identité et accéder à un système ou une application. Les facteurs d'authentification incluent généralement un élément connu par l'utilisateur à l'instar d'un mot de passe, quelque chose qu'il possède (comme un jeton de sécurité ou un appareil mobile), et quelque chose qu'il est (comme un identifiant biométrique comme une empreinte digitale ou la reconnaissance faciale). En exigeant plusieurs facteurs d'authentification, MFA contribue à augmenter la sécurité d'un système et à réduire le risque d'accès non autorisé ou de violations de données.

Plus en détail, MFA est une méthode d'authentification qui ajoute une couche de sécurité supplémentaire à la simple utilisation d'un mot de passe. Les mots de passe peuvent être facilement piratés ou devinés, et c'est là que MFA entre en jeu. En utilisant plusieurs facteurs d'authentification, MFA rend plus difficile pour les pirates informatiques de compromettre la sécurité d'un système ou d'une application.

Par exemple, pour se connecter à un service MFA, un utilisateur pourrait être invité à saisir son mot de passe, puis à saisir un code unique envoyé sur son téléphone portable. Dans ce cas, le mot de passe est quelque chose que l'utilisateur connaît, tandis que le code unique envoyé sur le téléphone portable est quelque chose qu'il possède. La combinaison de ces deux facteurs d'authentification permet de s'assurer que l'utilisateur est bien celui qu'il prétend être, ce qui renforce la sécurité de la connexion.

En fin de compte, MFA est un moyen efficace de réduire les risques de piratage et de violation de données, en s'assurant que seuls les utilisateurs autorisés ont accès aux systèmes et aux applications.

L'impact constaté par un panel d'expert :

Oui	1
Non	0,1

TABLE 4.7 – Impact de la présence d'un service MFA

Lorsqu'il s'agit de souscrire une assurance cyber, la taille de l'entreprise est considérée comme l'un des attributs les plus importants par les assureurs. En effet, elle permet de différencier les entreprises en termes d'exposition au risque, ainsi que d'évaluer le risque de perte de données ou de violation de la vie privée. Dans la plupart des polices d'assurance cyber, la taille de l'entreprise est déjà prise en compte, et parfois même utilisée comme critère exclusif pour accorder une souscription.

En général, la taille de l'entreprise est divisée en trois classes : les PME, les entreprises de taille moyenne et les grandes entreprises. Pour évaluer ce critère, on peut se baser sur deux sous-facteurs : le chiffre d'affaires (ce critère sera traité dans la partie 4.3.2) et le nombre d'employés de l'entreprise. Les entreprises de petite taille ont souvent une infrastructure réseau moins développée, parfois limitée à un seul poste et un site web. En revanche, les plus grandes entreprises ont souvent des réseaux beaucoup plus vastes, avec des milliers de postes, et elles sont plus susceptibles de consacrer des moyens importants à la sécurité et de disposer d'équipes dédiées à cette fin.

Ainsi, selon la taille de l'entreprise, nous allons appliquer les coefficient suivant selon le nombre d'employés :

≤ 20	0,11
≤ 200	0,54
≥ 201	0,87

TABLE 4.8 – Coefficient d'impact du nombre d'employés

Enfin, l'impact de la maturité externe est donné par :

$$\textbf{Maturité Externe} = 1 + 0,08 \times (\text{Coefficient pentest} + \text{Coefficient MFA} + \text{Coefficient phishing} + \text{Coefficient taille entreprise})$$

4.3.2 Impact du chiffre d'affaire

A défaut de constat empirique, l'étude sur l'impact du chiffre d'affaire va se baser sur des constats théorique. Une première idée de fonction pouvant simuler le chiffre d'affaire est une fonction concave comprise entre 0 et 1. Le choix de ne pas dépasser la valeur 1 vient du fait que le chiffre d'affaire maximal retenu est de 50m d'euros, ce chiffre d'affaire est dans la moyenne basse en comparaison avec les chiffres d'affaires des entreprises ayant permis le calcul de la prime moyenne sur laquelle se base le calcul final.

Dans un premier temps, nous allons réduire notre étude sur un intervalle de chiffre d'affaire compris entre 0 et 50 millions d'euros. Ensuite, nous allons créer une segmentation des chiffres d'affaire afin de les regrouper par types de structures :

- 0 à 2 000 000 € : une microentreprise est une entreprise dont l'effectif est inférieur à 10 personnes et dont le chiffre d'affaires ou le total du bilan annuel n'excède pas 2 millions d'euros comme le précise la définition du décret 2008-1354 du 18 décembre 2008 [10]. On considère ainsi que ces entreprises sont des petites structures avec peu de personnel et peu d'infrastructures informatiques et qu'elle présente un risque équivalent.
- 2 000 001 à 10 000 000 € : on considère désormais des entreprise intermédiaire et non des micro entreprises comme la branche précédente. Cette catégorie d'entreprise possèdent plus de salariés, donc plus d'interconnexions systèmes au sein de l'entreprise.
- 10 000 001 à 25 000 000 € : Là encore, nous avons des entreprises avec plus d'interconnexion système, nous avons augmenter le coefficient directeur de la pente car le risque PE est plus important à couvrir. Car ses entreprises comportent souvent de nombreux fournisseurs et clients et donc bcp d'interaction informatiques avec l'extérieure
- 25 000 001 à 50 000 000 € : Entreprises plus grosses et souvent un budget plus conséquent pour les systemes informatiques, on réduit le coefficient directeur de la courbe

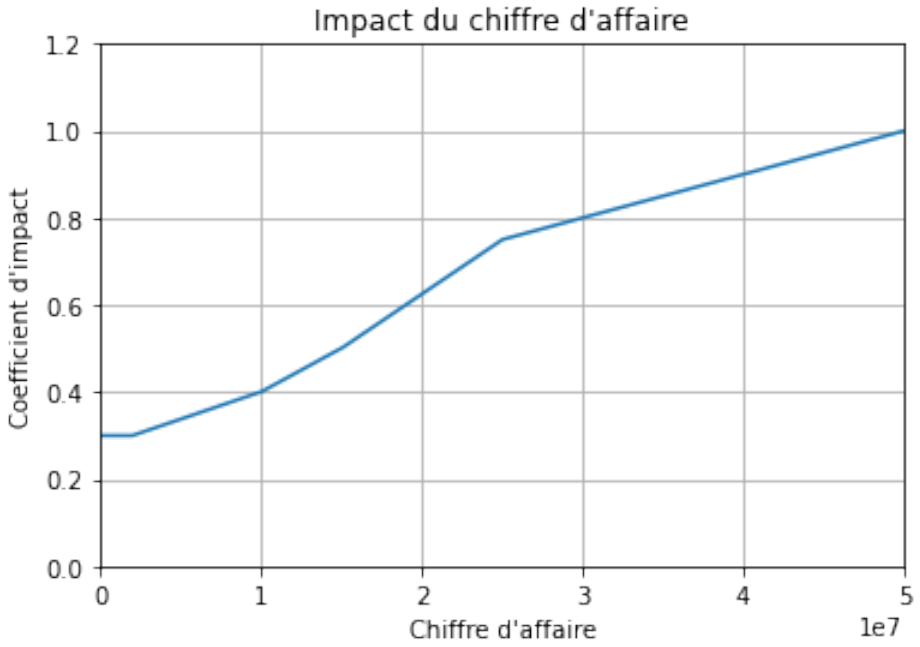

FIGURE 4.2 – Représentation du coefficient d'impact du chiffre d'affaire en fonction du chiffre d'affaire

4.3.3 Impact du secteur d'activité

L'exposition d'une entreprise aux attaques informatiques dépend également en grande partie de son secteur d'activité. En effet, les entreprises opérant dans des domaines proches du numérique sont plus vulnérables aux cyberattaques.

Les institutions bancaires sont des cibles privilégiées pour les cybercriminels car une attaque peut rapporter une somme considérable en peu de temps. En effet, les attaques à distance sont souvent moins risquées pour les criminels que les attaques physiques. En plus du secteurs bancaires nous pouvons penser à d'autres secteurs d'activités à risques tels que la défense ou des institutions stratégiques pour des raisons géopolitiques, avec la possibilité pour un État de faire pression sur un autre ou pour des groupes terroristes. On peut aussi penser au domaine de la santé. Les entreprises les plus vulnérables étant les laboratoires qui détiennent des données sensibles sur des sujets d'études confidentielles. Les hôpitaux sont aussi des cibles pour les attaquants, car ces derniers disposent d'énormément de données personnelles (PHI). Un des exemples ayant fait l'actualité

récemment étant l'attaque contre le système informatique de l'hôpital de Corbeil-Essonnes (Essonne) en août, les hackers ont mis en ligne des données de santé volées. Les cyberattaques contre les hôpitaux sont malheureusement de plus en plus courantes et peuvent avoir des conséquences très graves sur les soins aux patients. Les hôpitaux doivent prendre des mesures de sécurité informatique appropriées pour protéger leurs systèmes et leurs données, ainsi que pour prévenir les attaques.

La nature des clients d'une entreprise (professionnels ou particuliers) peut également influencer son exposition aux risques cyber. Les clients professionnels peuvent contribuer à accroître les risques en apportant leur propre exposition. En revanche, dans une relation clientèle B to C, le coût de la notification en cas de sinistre peut être beaucoup plus élevé. En effet, une campagne de communication appropriée doit être mise en place pour informer un grand nombre de clients, pouvant atteindre des millions de personnes. Ainsi, certains secteurs d'activité réputé pour avoir une clientèle BtoC va voir son scoring augmenté.

Une fois le secteur de l'entreprise assuré connu, les secteurs sont répartis en 4 types de secteurs selon leur criticité :

- Classe 1
- Classe 2
- Classe 3
- Classe 4

Après une étude menée sur les différentes attaques cyber ayant eu lieu sur les différents secteurs d'activités, nous avons dressé une répartition qui se trouve en annexe de ce mémoire.

A chaque seuil de criticité va être assimilé un coefficient qui va indexer la prime pure.

Manquant de données sur ce point, nous décidons d'allouer des coefficient arbitraire qui seront ajustés, une fois le portefeuille plus étoffé. Ainsi, les coefficient retenu sont les suivants :

Classe 1	0,85
Classe 2	1
Classe 3	1,15
Classe 4	1,25

TABLE 4.9 – Coefficient de secteur d'activité par criticité

Un cinquième niveau peut être ajouté : ce niveau correspond aux secteurs d'activités nécessairement exclus car exposés au risque cyber ou car l'activité en question peut être sujette à controverse. La liste des secteurs d'activités exclus est disponible en annexe 5.4.4.

4.3.4 Impact de la limite contractuelle

Le risque cyber présente une particularité en comparaison aux autres produits couverts par Acheel. L'assurance santé est un **risque de fréquence** (Forte Fréquence $\times$ Coût Bas). En effet, un assuré ayant un contrat santé va, dans la grande majorité des cas, avoir des consommations. Dans un portefeuille santé, il y a quelques risques de pointe : une hospitalisation, par exemple. Mais en majorité les risques sont assez maîtrisés. Cette caractéristique ne se retrouve pas dans le risque cyber, en effet, on peut qualifier ce risque de **risque de d'intensité ou de pointe** (Faible Fréquence $\times$ Coût Elevé), c'est à dire qu'il y a peu de sinistres mais lorsqu'un sinistre se produit, ce dernier a des conséquences financières bien plus importantes. Nous retrouvons cette même typologie de risque en Multi-risque Habitation, avec les incendies et les catastrophes naturelles. Ainsi, il est intéressant d'étudier ce qu'on appelle les extrêmes.

Définition Les extrêmes sont des événements rares qui conduisent à des pertes financières importantes.

Les événements extrêmes les plus étudiés sont les catastrophes naturelles et les cracks boursiers, puisque ces événements s'inscrivent parfaitement dans la définition proposée précédemment.

Les difficultés de modélisation de ces événements vient de leur caractère rare. Ainsi, on essaye de prévoir des faits qui pourront ne jamais se réaliser. La théorie des valeurs extrêmes (TVE) nous fournit une base mathématique et probabiliste sur laquelle il est possible de fonder des modèles statistiques pour prévoir la taille et la fréquence de ces phénomènes rares.

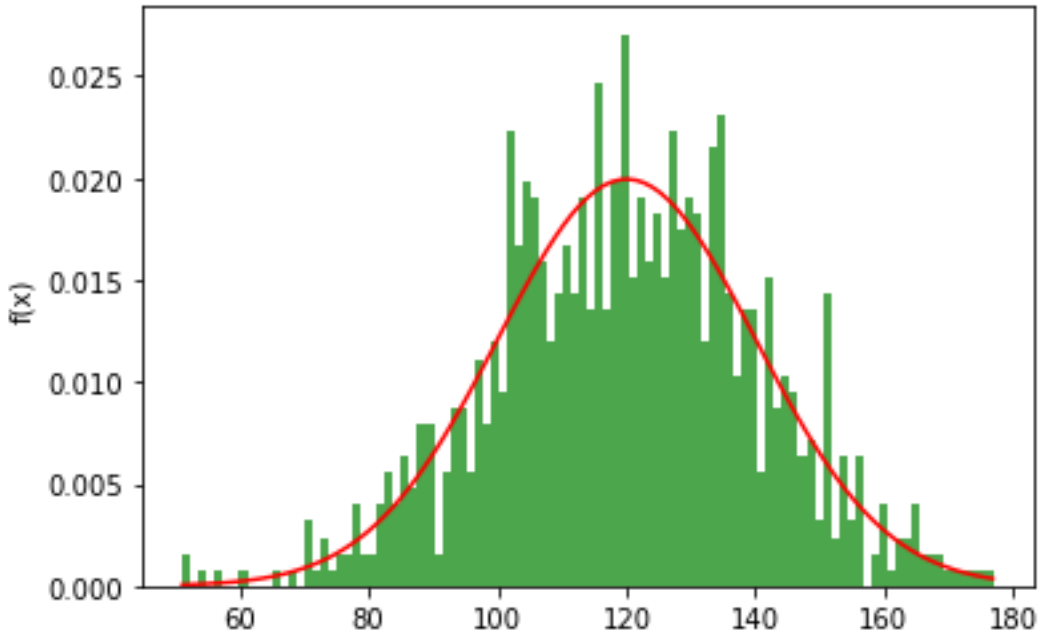

FIGURE 4.3 – Ensemble d'observations de variables aléatoires indépendantes et identiquement $X_1, X_2, ..., X_N$ distribuées de distribution inconnue F

La figure précédente permet d'illustrer la difficulté l'estimation des queues de distribution sur un jeu de donnée fictif simulé sur Python. En effet, la majorité des données est regroupée au centre de la distribution tandis que les données en queue de distribution se font rares.

Soit $X_1, X_2, ..., X_N$ une suite de variables aléatoires identiquement distribuées de fonction de distribution inconnue F, on note $M_n = max(X_1, X_2, ..., X_N)$, cette valeur M_n est assez importante à déterminer. Or, on a :

$$\mathbb{P}(M_n \leq x) = \mathbb{P}(X_1 \leq x_1, ..., X_n \leq x_n) = \mathbb{P}(X_1 \leq x_1)...\mathbb{P}(X_n \leq x_n) = [F(x)]^n$$

Or, nous n'avons pas d'information sur F, ainsi cette formule est difficilement utilisable, afin de pouvoir l'utiliser, nous allons chercher les lois limites pour le maximum. Dans notre cas, nous allons déterminer la fonction d'impact de la limite, grâce à l'étude des dépassements de seuils.

Plutôt que de considérer M_n d'un échantillon $X_1, X_2, ..., X_N$, nous allons étudier les variables $S_n = \sum_{i=1}^{n} \mathbb{I}_{X_i > u_n}$, autrement dit, nous nous intéressons aux observations strictement positives $(X_i - u_n)_+$. Ces observations sont caractérisées par la distribution de Pareto généralisées (GPD : Generalized Pareto Distribution).

Définition Distribution de Pareto généralisée GPD(β,ξ)

$$G_{\xi,\beta}(x) = \begin{cases} 1 - \left[1 + \xi \dfrac{x}{\beta}\right]^{-1/\xi} & \text{si } \xi \neq 0 \\ 1 - e^{-\dfrac{x}{\beta}} & \text{si } \xi = 0 \end{cases}$$

Cette loi est une loi de probabilité continue, elle est caractérisée par deux paramètres : le paramètre de forme (ξ) et le paramètre d'échelle (β). Nous pouvons toutefois ajouter un troisième paramètre dit de position que l'on note x_{min} si la distribution ne commence pas à 0. On obtient ainsi l'équation suivante :

$$G_{\xi,\beta,x_{min}}(x) = \begin{cases} 1 - \left[1 + \xi \dfrac{(x - x_{min})}{\beta}\right]^{-1/\xi} & \text{si } \xi \neq 0 \\ 1 - e^{-(x - x_{min})/\beta} & \text{si } \xi = 0 \end{cases}$$

Cette fonction a pour support :

- $x \geq x_{min}$ si $\xi \geq 0$
- $x_{min} \leq x \leq x_{min} - \beta/\xi$ si $\xi < 0$

Ainsi, l'impact de la limite sera déterminée en fonction de la limite de couverture désirée par l'assuré par la fonction : $G_{\xi,\beta,x_{min}}(limite)$ avec $\xi = 20$, $\beta = 36,23$ et $x_{min} = 100000$. Nous traçons ainsi la fonction sur l'intervalle $[0; 2000000]$, puisque la limite contractuelle est comprise entre ses bornes, la valeur de x_{min}, nous fourni la première valeur possible de la limite contractuelle à

savoir 100 000 € :

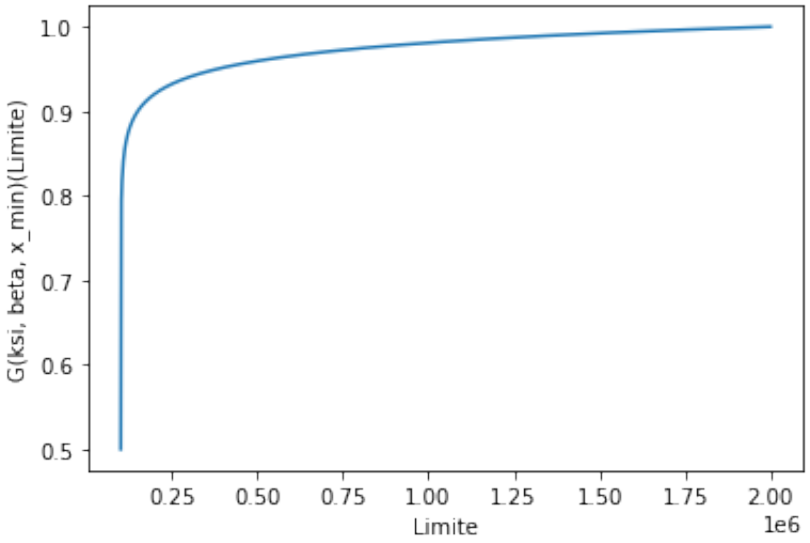

FIGURE 4.4 – Impact de la limite contractuelle modélisée par une loi de distribution de Pareto généralisée de paramètre $(20, 1000, 50000)$

Nous choisissons $\xi > 0$ afin d'avoir une fonction concave, car à partir d'une certaine limite nous considérons qu'à partir d'un million d'euros l'impact de la limite contractuelle présente moins de variation. Enfin le coefficient β est déterminé afin de vérifier la condition suivante : $G_{\xi,\beta,x_{min}}(2000000) = 1$

4.3.5 Construction de la prime commerciale

Après avoir déterminé la prime pure pour chaque profil d'assuré, nous cherchons à évaluer la prime commerciale qui se compose de la prime technique et des différentes taxes. Pour rappel, comme expliqué dans la partie 4.2.4, la prime technique se décompose de la manière suivante :

$$\boxed{\textbf{Prime technique} = \text{Prime pure} + \text{Chargement}}$$

Elle est ainsi composée de la prime pure calculée précédemment ainsi que de chargements. Ces chargements sont de plusieurs types :

- Un **chargement de sécurité** : c'est le montant qui va venir s'ajouter à la prime pure afin de permettre l'assureur de pouvoir résister à la volatilité naturelle des sinistres.
- Des **frais d'acquisition et/ou de distributions** qui couvrent l'ensemble des coûts liés à l'acquisition de nouveaux clients.
- Des **frais de gestion** qui englobent les coûts administratifs associés à la gestion des polices d'assurance, tels que les coûts de traitement des demandes de règlement, les coûts informatiques ...
- Des **frais assureur** qui représentent le bénéfice de l'assureur pour assurer la rentabilité de l'entreprise.

Les trois derniers types de frais sont déterminés par la direction financière afin de garantir la pérennité financière de l'entreprise. Il reste ainsi le chargement de sécurité sur lequel nous allons nous attarder.

La détermination du chargement de sécurité est un élément crucial dans la tarification des risques, elle s'est déroulée selon un processus visant à assurer la fiabilité des coefficients experts fournis par des acteurs externes tels que le réassureur ou des consultants en cybersécurité. Au sein d'Acheel, ces coefficients sont considérés comme des valeurs "à dire d'experts" car non déterminés en interne. Pour garantir la robustesse de ces paramètres et la validité des tarifs finaux, un coefficient de sécurité de 10% a été établi pour prendre en compte le risque de non fiabilité de ces variables. Ce coefficient est appliqué sur l'intégralité de la prime pure Acheel qui est calculée avec les coefficients tarifant présentés dans ce mémoire.

Afin de challenger les coefficients "à dire d'expert" nous avons commencé par la création d'un portefeuille fictif comprenant plus de 96 000 combinaisons de tous les paramètres tarifants.

Après avoir défini la liste des paramètres que nous souhaitons étudier, nous simulons l'ensemble des combinaisons possibles entre ces différents paramètres à l'aide de la fonction "itertools.product" sous Python. Ensuite, nous stockons ces profils dans un DataFrame dont un échantillon aléatoire

de 30 profils est représenté dans le tableau suivant :

	Profil	Chiffre_affaire	Pentest	Patching	Coef_MFA	Secteur_activite	Taille_entreprise	Phishing
83250	83251	43400000	Non_pentest	Mensuelle	Oui_mfa	Classe 4	< 20	Oui_phishing
71978	71979	37600000	Oui_pentest	Plus	Non_mfa	Classe 1	> 200	Oui_phishing
47489	47490	24800000	Non_pentest	Hebdomadaire	Oui_mfa	Classe 3	<= 200	Non_phishing
94910	94911	49600000	Oui_pentest	Hebdomadaire	Oui_mfa	Classe 3	> 200	Oui_phishing
18844	18845	10000000	Oui_pentest	Quotidienne	Non_mfa	Classe 1	<= 200	Oui_phishing
64622	64623	33800000	Oui_pentest	Mensuelle	Oui_mfa	Classe 3	> 200	Oui_phishing
6662	6663	3600000	Oui_pentest	Mensuelle	Non_mfa	Classe 3	> 200	Oui_phishing
63817	63818	33400000	Oui_pentest	Hebdomadaire	Non_mfa	Classe 1	< 20	Non_phishing
65648	65649	34200000	Non_pentest	Plus	Non_mfa	Classe 2	> 200	Oui_phishing
3022	3023	1600000	Non_pentest	Mensuelle	Non_mfa	Classe 4	<= 200	Oui_phishing
28193	28194	14800000	Oui_pentest	Plus	Oui_mfa	Classe 3	<= 200	Non_phishing
57816	57817	30200000	Non_pentest	Quotidienne	Non_mfa	Classe 1	< 20	Oui_phishing
47932	47933	25000000	Non_pentest	Mensuelle	Non_mfa	Classe 1	<= 200	Oui_phishing
35023	35024	18400000	Oui_pentest	Hebdomadaire	Non_mfa	Classe 2	< 20	Non_phishing
88374	88375	46200000	Oui_pentest	Hebdomadaire	Oui_mfa	Classe 2	< 20	Oui_phishing
60075	60076	31400000	Oui_pentest	Plus	Non_mfa	Classe 1	> 200	Non_phishing
66283	66284	34600000	Non_pentest	Quotidienne	Non_mfa	Classe 4	< 20	Non_phishing
21254	21255	11200000	Oui_pentest	Mensuelle	Non_mfa	Classe 3	> 200	Oui_phishing
40752	40753	21400000	Oui_pentest	Hebdomadaire	Oui_mfa	Classe 1	< 20	Oui_phishing
25421	25422	13400000	Oui_pentest	Hebdomadaire	Non_mfa	Classe 1	<= 200	Non_phishing
2954	2955	1600000	Non_pentest	Hebdomadaire	Non_mfa	Classe 1	> 200	Oui_phishing
61612	61613	32200000	Oui_pentest	Plus	Non_mfa	Classe 1	<= 200	Oui_phishing
18928	18929	10000000	Oui_pentest	Mensuelle	Oui_mfa	Classe 3	<= 200	Oui_phishing
30059	30060	15800000	Oui_pentest	Mensuelle	Oui_mfa	Classe 2	<= 200	Non_phishing
11589	11590	6200000	Oui_pentest	Hebdomadaire	Oui_mfa	Classe 4	> 200	Non_phishing
5757	5758	3000000	Non_pentest	Plus	Non_mfa	Classe 4	> 200	Non_phishing
8805	8806	4600000	Non_pentest	Plus	Oui_mfa	Classe 4	> 200	Non_phishing
26186	26187	13800000	Oui_pentest	Hebdomadaire	Non_mfa	Classe 1	> 200	Oui_phishing
74959	74960	39200000	Oui_pentest	Hebdomadaire	Non_mfa	Classe 2	< 20	Non_phishing
40991	40992	21400000	Non_pentest	Hebdomadaire	Non_mfa	Classe 4	<= 200	Non_phishing

FIGURE 4.5 – Paramètres d'un échantillon de 30 profils tirés aléatoirement dans le portefeuille fictif créés

Ensuite, une fonction de mapping est créée pour lier les critères des paramètres à leurs valeurs.

Les primes purs Acheel ont ensuite été calculés en utilisant les variables spécifiées dans ce mémoire, fournissant ainsi une référence de base. Par la suite, les primes intégrant le chargement de sécurité, ont été déterminés pour chaque combinaison du portefeuille fictif.

Dans le but d'évaluer la robustesse du chargement de sécurité dans différentes situations, cinq scénarios alternatifs ont été générés en modifiant les valeurs des paramètres tarifants. Ces valeurs sont référencées dans le tableau 4.10.

	Scénario retenu	Scénario 1	Scénario 2	Scénario 3	Scénario 4	Scénario 5
Oui_pentest	-0.2	-0.5	-0.3	-0.1	-0.2	-0.5
Non_pentest	0.2	0.5	0.3	0.1	0.2	0.5
Oui_mfa	1	1	0.8	0.9	0.9	1
Non_mfa	0.1	0.2	0.1	0.4	0.2	0.1
Oui_phishing	1	1	0.9	0.8	0.9	1
Non_phishing	0.3	0.1	0.1	0.1	0.4	0.1
Quotidienne	-0.99	-1.2	-1	-0.99	-1.2	-1
Hebdomadaire	-0.92	-1.1	-0.96	-0.92	-1.1	-0.96
Mensuelle	0.46	0.6	0.67	0.46	0.6	0.99
Plus	1	1.2	0.99	1	1.2	1.14
≤ 20	0.11	0.09	0.1	0.08	0.09	0.11
≤ 200	0.54	0.5	0.4	0.44	0.54	0.54
≥ 200	0.87	0.7	0.7	0.66	0.99	0.87
Classe1	0.85	0.8	0.9	0.8	0.7	0.7
Classe2	1	1	1.1	1	1	0.9
Classe3	1.15	1.1	1.3	1.1	1.07	1.1
Classe4	1.25	1.3	1.4	1.3	1.5	1.25

TABLE 4.10 – Coefficients choisis en fonction des différents scénarios

Le tableau présente les coefficients utilisés pour moduler les primes d'assurance dans différents scénarios. Dans le scénario retenu, les coefficients initiaux sont maintenus inchangés, ce qui constitue la base de référence pour les primes d'assurance chez Acheel. En revanche, les scénarios 1 à 5 introduisent des ajustements significatifs.

Les tarifs de ces scénarios ont été calculés et comparés avec le tarif chargé (c'est à dire le tarif pur auquel est ajouté le chargement de sécurité). Cette comparaison a permis d'analyser la couverture du tarif avec le chargement de sécurité par rapport à l'ensemble des tarifs des scénarios alternatifs.

Profil	Prime_pure_Acheel	Prime_chargée_Acheel	Scenario1	Scenario2	Scenario3	Scenario4	Scenario5
83251	3503.782382	3854.160620	3745.073623	3892.264925	3531.150039	4153.527888	3633.324913
71979	2109.159917	2320.075908	1947.074688	2174.041382	2003.267635	1743.793632	1694.221563
47490	2511.283667	2762.412034	2396.611360	2752.461504	2298.883690	2346.838297	2431.010036
94911	3323.397343	3655.737077	3075.568320	3609.809174	3121.010302	3039.297028	3092.973460
18845	947.265432	1041.991975	859.353600	974.779200	892.744448	783.276480	758.850400
64623	2875.134960	3162.648456	2678.566440	3138.740062	2699.894680	2646.423844	2706.864225
6663	1031.319117	1134.451028	966.408960	1139.893248	995.532595	962.248090	969.666509
63818	1775.518880	1953.070768	1600.415309	1829.212200	1696.717356	1477.277878	1395.345984
65649	2472.812544	2720.093798	2559.646320	2698.272526	2450.772352	2482.471968	2291.616300
3023	1114.773300	1226.250630	1187.768400	1241.629200	1140.512256	1352.397600	1156.207950
28194	1677.149402	1844.864342	1526.937984	1804.207142	1561.843290	1579.613779	1543.918802
57817	1866.524867	2053.177354	1808.021101	1978.511544	1749.378348	1528.377816	1579.543812
47933	1895.114610	2084.626071	1827.336000	1995.475500	1754.634240	1577.797200	1618.691130
35024	1465.197552	1611.717307	1403.241840	1568.209500	1487.679336	1480.314420	1258.392704
88375	2710.380358	2981.418394	2624.166688	2888.293408	2672.576067	2659.171944	2371.943602
60076	1861.465619	2047.612181	1690.411008	1901.337293	1768.674829	1562.254848	1470.434085
66284	2749.771143	3024.748257	2904.030698	3059.684208	2847.469304	3330.414360	2786.914350
21255	1366.497830	1503.147613	1280.491872	1510.358554	1319.080689	1274.978719	1284.808124
40753	1580.585635	1738.644199	1440.291072	1621.287360	1466.860877	1277.065944	1265.694091
25422	1055.445506	1160.990057	942.289920	1075.734691	994.659195	886.410907	831.341085
2955	720.808704	792.889574	697.132800	756.678240	672.310272	591.438960	609.223104
61613	2025.995237	2228.594760	1853.721792	2085.025687	1909.233754	1689.121224	1628.245745
18929	1402.897328	1543.187061	1296.187200	1529.636160	1308.231936	1302.037632	1321.383888
30060	1512.705376	1663.975914	1438.070400	1590.402528	1472.768128	1529.498880	1320.406402
11590	1218.175140	1339.992654	1206.553920	1298.872260	1242.559906	1456.427070	1166.925870
5758	1091.200000	1200.320000	1159.372500	1202.750500	1124.327750	1333.830000	1108.646250
8806	1237.644800	1361.409280	1305.083780	1346.577918	1240.460676	1490.975220	1256.865960
26187	1102.757044	1213.032749	1010.003456	1135.883750	1047.472957	904.808598	882.427688
74960	2234.113190	2457.524509	2139.643968	2391.184400	2268.393107	2257.163184	1918.779987
40992	2271.857280	2499.043008	2373.571200	2498.340768	2322.492058	2778.490440	2300.191740

FIGURE 4.6 – Prime pure des scénario générés d'un échantillon de 30 profils tirés aléatoirement dans le portefeuille fictif créés

Le tableau 4.11 présente un résumé des résultats d'un portefeuille simulé sur différents scénarios, mettant en évidence la prime pure Acheel, la prime chargée Acheel, ainsi que les primes totales et moyennes pour chaque scénario.

	Prime pure Acheel	Prime chargée Acheel	Scénario 1	Scénario 2
Prime totale	195 746 100.39	215 320 710.43	191 727 841.93	211 211 701.75
Prime moyenne	2039.02	2242.92	1997.17	2200.12
	Scénario 3	Scénario 4	Scénario 5	
Prime totale	190 530 356.01	197 079 285.54	181 263 357.18	
Prime moyenne	1984.69	2052.91	1888.16	

TABLE 4.11 – Résumé des résultats du portefeuille simulé sur les différents scénarios

Les deux premières colonnes affichent la prime pure Acheel et la prime chargée Acheel. Ces valeurs sont essentielles pour évaluer les performances du portefeuille et le coût total du risque. Les cinq colonnes suivantes présentent les résultats pour chaque scénario. Chaque scénario a une influence sur les paramètres tarifaires, affectant ainsi les primes du portefeuille. On constate que dans tous les cas la prime totale chargée est strictement supérieure aux primes totales pour cha-

cun des scénarios ce qui indique que le chargement de sécurité dans ce scénario est suffisant pour couvrir les risques.

En résumé, ce tableau offre une vue complète des performances du portefeuille simulé dans divers scénarios, permettant une évaluation approfondie de l'efficacité du modèle tarifaire, en mettant en lumière l'impact des changements de paramètres sur les primes.

Enfin, après avoir fait une analyse macro en observant les primes totales et primes moyennes. Il est important de s'intéresser aux profils un à un. Nous allons donc observer la proportion de risque pour lesquels la prime chargée est supérieure aux primes pures des différents scénarii.

La conclusion tirée de cette démarche démontre que le tarif avec le chargement de sécurité couvre 90.26% des tarifs des différents scénarios, établissant ainsi la viabilité des paramètres présentés dans le mémoire. Cette approche méthodique, alliant la création d'un portefeuille fictif, le calcul des tarifs purs et l'évaluation des scénarios alternatifs, renforce la validité des coefficients de sécurité et la confiance dans le processus de tarification mis en place.

L'approche méthodologique que nous avons employée dans notre étude avec nos 5 scénarios a démontré son efficacité pour évaluer la validation des coefficients choisis. Cependant, il est important de noter que notre méthode initiale testait seulement un ensemble spécifique de valeurs de coefficients, ne couvrant pas toutes les combinaisons potentielles. Afin de pallier cette limitation, nous avons élaboré un second code s'inspirant du premier avec les 5 scénarios mais qui génère une multitude de scénarios en modifiant tous les coefficients de manière exhaustive.

Pour chacun des 17 paramètres possibles (Oui_pentest, Non_pentest, Oui_mfa, Non_mfa, Oui_phishing, Non_phishing, Quotidienne, Hebdomadaire, Mensuelle, Plus, ≤ 20, ≤ 200, ≥ 200, Classe 1, Classe 2, Classe 3, Classe 4) un intervalle de valeur a été défini 4.12, afin de générer un ensemble de scénarios exhaustif.

	Valeur minimale	Valeur maximale	Pas
Oui_pentest	-0.5	0	0.15
Non_pentest	0	0.5	0.15
Oui_mfa	0.5	1.2	0.2
Non_mfa	0	0.5	0.2
Oui_phishing	0.8	1.3	0.1
Non_phishing	0	0.5	0.1
Quotidienne	-1.2	-0.95	0.1
Hebdomadaire	-0.95	0.3	0.2
Mensuelle	0.3	0.8	0.2
Plus	0.8	1.2	0.1
≤ 20	0.05	0.2	0.1
≤ 200	0.2	0.5	0.1
≥ 200	0.5	0.9	0.1
Classe1	0.5	0.8	0.1
Classe2	0.8	1.1	0.1
Classe3	1.1	1.2	0.1
Classe4	1.2	1.5	0.1

TABLE 4.12 – Valeurs possibles des coefficients tarifants

Le nombre de combinaisons possibles avec ces valeurs de coefficients possibles est de : 19 110 297 600. Pour des raisons de complexités, 10 000 combinaisons vont être sélectionnées aléatoirement afin de tester la validité du chargement choisi. La même méthodologie que celle utilisée pour 5 scénarios est appliquée. Avec ces 10 000 scénarios, on constate que le tarif avec le chargement de sécurité couvre 88,47% des tarifs des différents scénarios (pour rappel sur nos 5 scénarios présentés précédemment, ce taux était de 90.26%).

Cette nouvelle méthode permet ainsi d'explorer un espace beaucoup plus vaste de paramètres, offrant ainsi une perspective plus complète des implications tarifaires. En considérant un éventail plus large de scénarios, nous avons cherché à garantir une évaluation robuste et exhaustive de la variabilité des primes. Cette approche, basée sur une exploration systématique des coefficients, vise à renforcer la crédibilité de nos conclusions en démontrant la robustesse des résultats face à une diversité étendue de conditions.

On constate que même avec l'extension significative du nombre de scénarios générés, les conclu-

sions obtenues restent alignées avec nos premières observations. Cela renforce la solidité de notre méthode et suggère que les résultats demeurent cohérents, même lorsque l'on considère un spectre plus étendu de configurations possibles.

Chapitre 5

Impact de l'ajout du produit de risque cyber sur les exigences réglementaires

L'implémentation du risque cyber constitue un impact non négligeable sur la solvabilité de l'entreprise. Ainsi, une étude sur l'impact du SCR à la suite de l'ajout d'un produit de couverture cyber est nécessaire.

5.1 Les grands principes de la réforme de solvabilité II

En tant que compagnie d'assurance, Acheel est soumise à Solvabilité II qui est un régime réglementaire régissant tout organisme d'assurance opérant dans l'Union européenne. Il est fondé sur trois piliers qui visent à améliorer la surveillance et la gestion des risques. Les trois piliers de Solvabilité II sont les suivants :

Pilier 1 - Exigences de capital : Ce pilier établit des exigences de capital pour les compagnies d'assurance afin de garantir qu'elles disposent d'un capital adéquat pour couvrir les risques qu'elles encourent. Les exigences de capital sont basées sur l'évaluation des risques et sur la quantité de capital nécessaire pour les couvrir.

Pilier 2 - Surveillance et évaluation interne : Ce pilier vise à garantir que les compagnies d'assurance ont des systèmes et des processus efficaces de gestion des risques pour évaluer et surveiller leur profil de risque. Les compagnies d'assurance doivent établir des processus de surveillance internes pour évaluer leur propre solvabilité et leur propre capacité à gérer les risques. Les autorités de surveillance doivent également évaluer la solvabilité des compagnies d'assurance et leur capacité à gérer les risques.

Pilier 3 - Transparence et communication : Ce pilier exige que les compagnies d'assurance fournissent des informations régulières et détaillées sur leur profil de risque, leur capital et leur solvabilité. Les compagnies d'assurance doivent communiquer ces informations aux autorités de surveillance et aux parties prenantes, telles que les clients, les investisseurs et les analystes financiers.

En résumé, les trois piliers de Solvabilité II visent à renforcer la stabilité et la solidité du marché de l'assurance en garantissant que les compagnies d'assurance disposent d'un capital adéquat pour couvrir les risques qu'elles encourent, qu'elles disposent de systèmes et de processus de gestion des risques efficaces pour évaluer et surveiller leur profil de risque, et qu'enfin, elles communiquent des informations régulières et détaillées sur leur solvabilité et leur situation financière.

5.2 L'ORSA (évaluation des risques et de la solvabilité propre)

L'ORSA (évaluation des risques et de la solvabilité propre) est un cadre de gestion des risques et de la solvabilité utilisé par les compagnies d'assurance pour identifier, mesurer, surveiller et gérer leurs risques. Le processus ORSA exige des assureurs qu'ils effectuent une évaluation approfondie de leur profil de risque, en tenant compte de tous les risques pertinents pour leur entreprise, notamment les risques de souscription, les risques de marché, les risques de crédit, les risques opérationnels et les risques de liquidité, entre autres.

Le processus ORSA vise à aider les assureurs à comprendre les risques auxquels ils sont confrontés, à évaluer l'adéquation de leur capital et de leur position en matière de solvabilité et à élaborer des stratégies pour gérer ces risques sur un horizon de plusieurs années.

Pour compléter le propos voici quelques exemples de processus d'évaluation des risques et de solvabilité (ORSA) que les compagnies d'assurance peuvent entreprendre :

- **Identification et évaluation des risques** : Une compagnie d'assurance évaluera tous les risques auxquels elle est confrontée, y compris les risques de marché, de crédit, opérationnels, d'assurance et de réputation. L'assureur évalue la probabilité et l'impact de chaque risque et son effet potentiel sur la solvabilité de la société.
- **Appétit et tolérance au risque** : L'assureur déterminera son appétit et sa tolérance au risque en fonction de sa stratégie et de ses objectifs commerciaux. L'appétit pour le risque est le niveau de risque que la société est prête à accepter dans la poursuite de ses objectifs. La tolérance au risque est le montant de risque que la société peut absorber sans enfreindre ses exigences en capital.
- **Tests de résistance (Stress test)** : L'assureur effectuera des tests de résistance pour évaluer sa résilience à divers scénarios, tels qu'une catastrophe naturelle majeure, une baisse des marchés financiers ou un événement de perte important.
- **Évaluation de l'adéquation des fonds propres** : L'assureur évaluera son niveau d'adéquation des fonds propres actuel et déterminera s'il est suffisant pour soutenir son profil de risque. L'évaluation tiendra également compte de l'impact des risques futurs sur la position en capital de l'assureur.
- **Gestion et surveillance des risques** : L'assureur élaborera un plan de gestion des risques pour atténuer les risques identifiés et établira des procédures pour surveiller et rendre compte de l'exposition aux risques.

Dans l'ensemble, le processus ORSA est un cadre de gestion des risques complet qui permet aux assureurs d'évaluer leur profil de risque, d'évaluer l'adéquation des fonds propres et de développer des stratégies de gestion des risques pour assurer la solvabilité et la viabilité de l'entreprise.

5.3 Bilan prudentiel et calcul du SCR : calcul des capitaux réglementaires

Le bilan prudentiel d'une compagnie d'assurance est basé sur les principes de Solvabilité II, il est un outil de mesure de sa solvabilité et de son niveau de risque. Il s'agit d'un bilan qui prend en

compte les risques que la compagnie d'assurance court et les actifs qu'elle détient pour les couvrir.

Le bilan prudentiel intervient dans le cadre des trois piliers pour évaluer la solvabilité de la compagnie d'assurance. Il permet de mesurer les risques que la compagnie d'assurance court en évaluant les actifs qu'elle détient, tels que les placements et les réserves techniques, ainsi que les passifs, tels que les sinistres non payés et les obligations contractuelles.

Le bilan prudentiel permet également de mesurer la capacité de la compagnie d'assurance à couvrir les risques qu'elle court. Pour cela, il prend en compte les exigences de capital établies par les autorités de surveillance, ainsi que le niveau de capital effectivement détenu par la compagnie d'assurance.

En résumé, le bilan prudentiel est un outil important pour mesurer la solvabilité et le niveau de risque d'une compagnie d'assurance. Le bilan prudentiel permet ainsi aux autorités de surveillance de surveiller la situation financière et la solvabilité des compagnies d'assurance et de garantir la stabilité du marché de l'assurance.

Le MCR (minimum solvency requirement) correspond au montant minimum de fonds propres constituant le seuil déclencheur de l'intervention prudentielle la plus drastique, dès qu'il est franchi à la baisse. Dans le cas d'Acheel ce montant est évalué à 4m€.

Le SCR (Solvency Capital Requirement) est un indicateur clé de la solvabilité des compagnies d'assurance. Il s'agit d'une mesure quantitative des risques encourus par une compagnie d'assurance, qui doit être respectée pour se conformer aux exigences de Solvabilité II. Il correspond à la Value-at-Risk à 99,5% sur un horizon d'un an : si le montant de fonds propres d'une entreprise est égal au SCR, l'entreprise pourra faire face à ses engagements dans 99,5% des cas, sur un horizon d'un an.

Le calcul du SCR est basé sur une analyse approfondie des risques encourus par la compagnie d'assurance, en prenant en compte une grande variété de facteurs tels que les risques de souscription, les risques de marché, les risques de crédit, les risques opérationnels, les risques de liquidité et les risques de concentration.

Une fois le SCR calculé, nous pouvons le comparer au montant des fonds propres de la compagnie d'assurance avec le montant de capital requis pour couvrir les risques encourus. Si le capital disponible est supérieur au capital requis, la compagnie d'assurance est considérée comme solvable.

Le SCR est donc un outil clé pour mesurer la solvabilité d'une compagnie d'assurance et s'assurer qu'elle dispose d'un niveau de capital suffisant pour couvrir les risques encourus. Le calcul du SCR est une étape importante dans le cadre de la mise en œuvre des exigences de Solvabilité II et contribue à renforcer la stabilité du marché de l'assurance.

N'ayant pas de modèle interne, le SCR d'Acheel est calculé grâce à la formule standard. Le calcul du SCR (Solvency Capital Requirement) peut être effectué à l'aide de la formule standard, qui utilise une approche simplifiée pour mesurer les risques encourus par une compagnie d'assurance. La formule standard est utilisée par les compagnies d'assurance qui ne disposent pas de modèles internes pour le calcul du SCR.

La formule standard pour le calcul du SCR est la suivante :

$$\boxed{SCR = BSCR + SCR_{\text{opérationnel}} + Adj}$$

où :

- BSCR : Basic Solvency Capital Requirement : représente le montant du SCR de base ;
- Adj : Ajustement lié au risque d'écoulement des provisions techniques et de la fiscalité différée ;
- $SCR_{\text{opérationnel}}$: Le SCR opérationnel correspond au maximum des quantités indexées sur des primes et des provisions. Ce montant est toutefois plafonné à 30% du BSCR.

Le montant du SCR doit être supérieur ou égal au niveau de capital minimum requis par l'autorité de surveillance, afin de garantir que la compagnie d'assurance dispose d'un niveau de capital suffisant pour couvrir les risques encourus.

Le capital réglementaire dont doit disposer une compagnie d'assurance correspond au montant maximal entre le SCR et le SCR. L'ACPR (l'autorité de controle prudentiel de resolution) recommande de disposer d'au moins 130% de ce capital.

$$\text{BGS} = 130\% \times max(MCR; SCR)$$

Dans le cadre de ce mémoire, nous n'allons pas nous attarder sur les différents calculs menant au calcul du SCR mais à l'étude des résultats et l'impact qu'a l'intégration du produit Cyber sur le bilan prudentiel de la compagnie.

5.4 Impact de l'intégration d'un produit Cyber sur le bilan prudentiel

Afin de conserver la confidentialité des chiffres de la compagnie, les chiffres présentés plus bas ont été mis en base 100.

5.4.1 SCR avant intégration du risque cyber

Année	**2022**	**2023**	**2024**	**2025**	**2026**
SCR	100	199	307	400	494
MCR	97	97	97	100	124
Montant Réglementaire à couvrir	100	199	307	400	494
BGS	130	258	400	520	642
FP	416	603	1 048	1 570	2 179
Couverture du SCR	415,8%	303,4%	341,0%	392,6%	441,0%

TABLE 5.1 – Evolution de la couverture de capital réglementaire avant intégration du produit cyber

5.4.2 SCR après intégration du produit cyber

Année	2022	2023	2024	2025	2026
SCR	103	206	322	421	523
MCR	97	97	97	105	131
Montant Réglementaire à couvrir	103	206	322	421	523
BGS	134	268	418	547	680
FP	443	671	1 186	1 794	2 512
Couverture du SCR	429,3%	325,5%	368,7%	426,3%	480,1%

TABLE 5.2 – Evolution de la couverture de capital réglementaire après intégration du produit cyber

Nous constatons une augmentation de la couverture du SCR. En effet, au regard du cadrage du produit et du niveau de réassurance, nous avons une sinistralité très basse sur programme.

Le risque cyber nous expose principalement à des sinistre d'intensité et que nous avons peu d'historique, il est donc primordial d'observer l'impact d'un sinistre conséquent sur la solvabilité de la compagnie.

5.4.3 Stress test scénario sinistre cyber

Acheel a un ratio de couverture élevé entre autre grâce à des fortes couvertures en réassurance. Néanmoins, Acheel étant une jeune compagnie, le montant de fond propre dont elle dispose est encore modeste. c'est pourquoi il est impératif de nous assurer que l'ajout d'un nouveau produit cyber ne remet pas en question la solvabilité de l'entreprise. Nous avons donc réalisé une étude pour évaluer l'impact de cette nouvelle garantie sur le montant du capital réglementaire, dans le cas d'un scénario central classique (où nous prévoyons que tout se passe en accord avec le business plan que nous avons tracé) ainsi que de le cas d'un scénario stressé, correspondant ici a la survenance d'un sinistre exceptionnel d'une valeur extrême estimée à 8m.

Dans ce scénario, il est fait l'hypothèse qu'un sinistre de 8 M€ intervient sur notre produit Cyber durant l'année 2024. Notre traité Cyber prévoyant une limite de couverture à 2m€ le reste à la charge d'Acheel s'élève à 6m€ auquel s'ajoute les 15% de quote part.

Le coût réel du sinistre pour Acheel est ainsi de 6,3mm€.

Année	2022	2023	2024	2025	2026
SCR	103	206	324	420	522
MCR	97	97	97	105	131
Montant Réglementaire à couvrir	103	206	324	420	522
BGS	134	268	422	546	679
FP	443	671	1 173	1 780	2 497
Couverture du SCR	429,3%	325,5%	361,7%	423,6%	478,0%

TABLE 5.3 – Evolution de la couverture de capital réglementaire dans le cas d'un sinistre exceptionnel en 2024

Afin d'avoir une vision graphique de l'impact de l'ajout du produit cyber, nous traçons les 3 courbes de couverture du SCR selon les 3 scénarios suivants : sans intégration du produit cyber, après intégration du produit cyber et à la suite d'un sinistre important sur le programme.

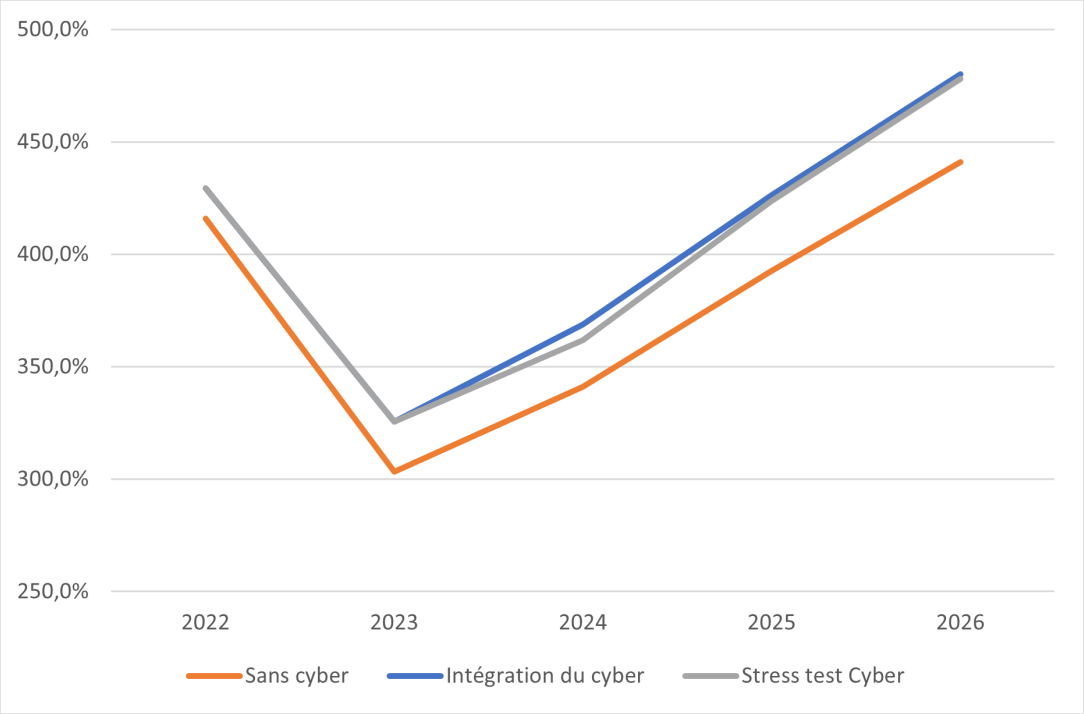

FIGURE 5.1 – Comparaison de la couverture de capital réglementaire

5.4.4 Conclusion

A la suite de cette étude sur la solvabilité d'Acheel, l'intégration d'un produit cyber ne présente pas un impact négatif sur la solvabilité de la compagnie. Acheel cédant une grande partie de son risque aux réassureurs, un sinistre majeur sera absorbé par la couverture des traités. Néanmoins, cette étude a permis de définir un périmètre plus clair concernant la création de ce produit cyber et de cadrer les garanties ainsi que la typologie de risque souhaitée dans le portefeuille d'Acheel dans son portefeuille. Les risques dont la limite contractuelle excède les 2m d'euros seront ainsi refusés à la souscription afin de ne pas compromettre l'avenir de la compagnie.

Conclusion

Le risque cyber est un enjeu crucial pour la sécurité des entreprises et de leurs données. Il est donc nécessaire que les compagnies d'assurance continuent à développer des produits et des solutions adaptées pour aider les entreprises à faire face à ce risque et à se protéger efficacement. Ainsi, proposer une modélisation du risque cyber est un enjeu important pour les actuaires désirant proposer ce type d'assurance. Le risque cyber étant un risque très récent, très peu de données sont disponibles, ce qui limite grandement la mise en place de modèle de tarification traditionnelle.

L'intégration d'un produit cyber dans le portefeuille de la compagnie d'assurance Acheel semble être une décision judicieuse. Le risque cyber est de plus en plus présent dans le monde des affaires et la demande pour une assurance couvrant ces risques est en hausse. De plus, Acheel se positionne en tant que compagnie innovante en répondant aux besoins de ses clients en proposant de nouvelles solutions adaptées à leurs besoins. Les différents types de garanties proposées par Acheel dans son produit cyber, telles que la gestion de crise, la couverture des atteintes aux données et la couverture des atteintes au système informatique, répondent aux préoccupations actuelles des entreprises. Avec cette nouvelle offre, Acheel se positionne comme un acteur de choix pour les entreprises qui cherchent une assurance fiable et complète pour se prémunir contre les risques liés à la cybersécurité.

Enfin, au regard des changements climatiques, des changements de modes de consommations, et des différents nouveaux enjeux économiques, les assureurs vont devoir adapter de plus en plus d'approches pour prévenir des risques en l'absence de données.

Annexes

Répartition des secteurs d'activités selon leur criticité

Criticité	Secteur d'activité	Criticité	Secteur d'activité
Classe 1	— Droit (Conseil juridique à titre accessoire ; notaire ; avocat) — Agent immobilier — Métiers du chiffre (comptable, expert-comptable) — Démarcheur et conseiller financier — Métiers du chiffre (comptable, expert-comptable) — Agent immobilier — Expert d'assurance — Métiers du droit (avocats, notaires) — Activité administrative de bureau — Marketing traditionnel et communication — Traducteur — Grossiste — Vétérinaire — Restaurant, bar et discothèque — Construction — Artisan — Agriculture, sylviculture et pêche	Classe 2	— Conseiller en gestion de patrimoine indépendant — Intermédiaire d'assurance — Conseil en entreprise et audit — Formation et éducation — Événementiel — Éditeur de logiciels, fournisseur de matériels informatiques — Création de site web — Création de contenus numériques — Biotechnologie — Logistique, entrepôt et transport de marchandises — Professionnel de la santé (hors établissement) — EHPAD et maison de retraite — Hébergement et camping — Transport de passagers — Divertissement (sport, parc d'attractions) — Bien-être — Industrie manufacturière — Autres industries
Classe 3	— Commerce de détails — Établissement médico-social — Cabinet médical (hors établissement) — Agence de voyages et tour opérateur — Culture (musée, cinéma)	Classe 4	— E-commerce — Pharmacie et parapharmacie — Laboratoire d'analyses médicales — Centre de radiologie — Clinique et hôpital

Table 5.4 – Répartition des secteurs d'activités selon leur criticité

Liste des activités exclues

- Vente d'armes, de drogue, de vente de substances et produits illicites ;
- Communication et diffusion d'informations ou images à caractère érotique ou pornographique ;
- Site internet à caractère religieux, politique et idéologique ;
- Activité de jeux et paris ;
- Réseaux sociaux ;
- Activités liées aux crypto-monnaies ;
- Compagnies aériennes, aéroports ; Marché boursier ;
- Les banques et autres institutions financières et/ou établissements bancaires, les agents de changes, courtiers en bourse, les courtiers en assurance/réassurance ayant un chiffre d'affaires supérieur à 50 000 000 €, les fournisseurs de service de paiement ainsi que les compagnies d'assurance ou de réassurance ainsi que les Big 5 (KPMG, PWC, Accenture, Ernst & Young, Deloitte & Touche) ;
- Fortune 500 ;
- Opérateurs de réseaux : Eaux, Électricité, Télécom, Internet, GAFA ;
- Chaînes de télévision, journaux ;
- Établissements Publics à caractère administratif (EPA) sous la tutelle des Ministères de Santé, de la Défense, des Affaires étrangères et de l'Intérieur ;
- Hôpitaux publics, hôpitaux privés (cliniques), hôpitaux universitaires (CHU), hôpitaux spécialisés (à l'exclusion des maisons de retraite et EHPAD et centres de rééducations qui peuvent être couverts). Sont totalement exclus : Assistance Publique — Hôpitaux de Paris, Hospices Civils de Lyon, Assistance Publique – Hôpitaux de Marseille.

Article 103 (Directive S2)

Le capital de solvabilité requis calculé selon la formule standard est la somme des éléments suivants :

a) le capital de solvabilité requis de base, prévu à l'article 104 ;

b) l'exigence de capital pour risque opérationnel, prévue à l'article 107 ;

c) l'ajustement visant à tenir compte de la capacité d'absorption de pertes des provisions techniques et des impôts différés, prévu à l'article 108.

Directive Solvabilité 2 (article 75)

« les actifs sont valorisés au montant pour lequel ils pourraient être échangés dans le cadre d'une transaction conclue, dans des conditions de concurrence normales, entre des parties informées et consentantes »

« les passifs sont valorisés au montant pour lequel ils pourraient être transférés ou réglés dans le cadre d'une transaction conclue, dans des conditions de concurrence normales, entre des parties informées et consentantes »

Décomposition du SCR en formule standard

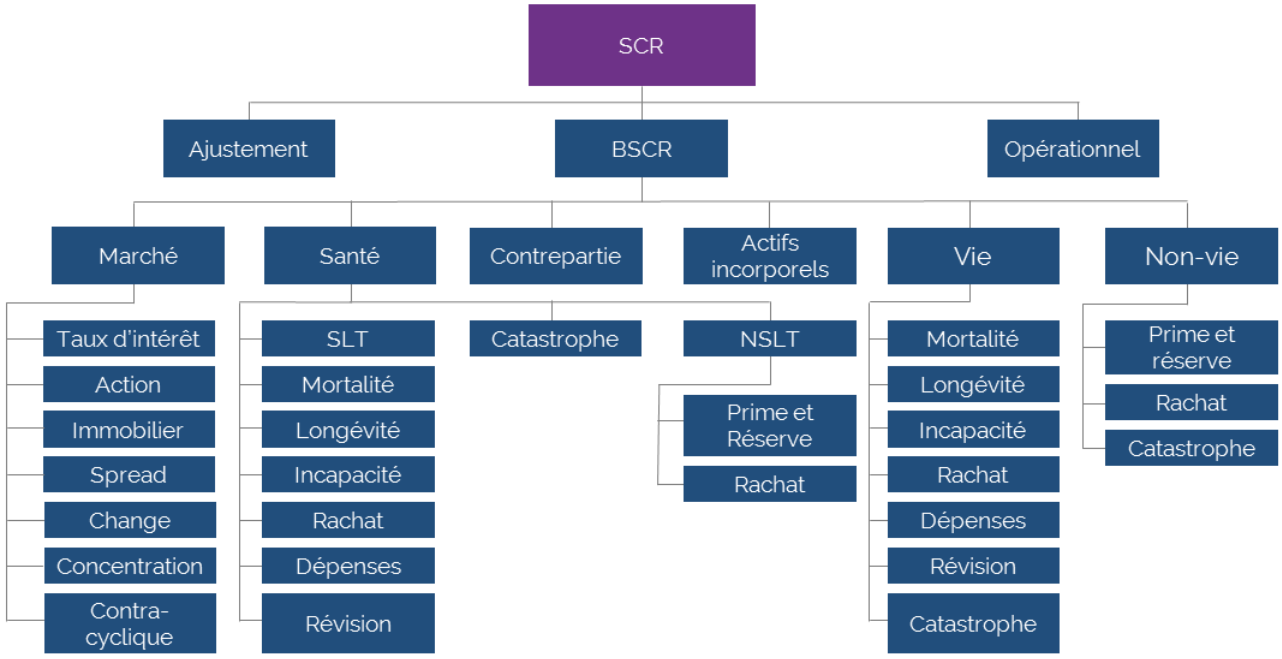

Figure 5.2 – Décomposition du SCR en formule standard

Liste des tableaux

Table des figures

Bibliographie

[1] Accenture. Cost of cyber crime study france. 2020.

[2] France Assureur. Cartographie prospective de l'assurance. 2022.

[3] James J. Cebula and Lisa R. Young. A taxonomy of operational cyber security risks. 2010.

[4] Thierry Cohignac and Nabil Kazi-Tani. Laplacian Spectra of Graphs and Cyber-Insurance Protection. working paper or preprint, August 2020.

[5] U.S. DEPARTMENT OF THE TREASURY FEDERAL INSURANCE OFFICE. Annual report on the insurance industry. Septembre 2021.

[6] Caroline Hillairet and Olivier Lopez. Propagation of cyber incidents in an insurance portfolio : counting processes combined with compartmental epidemiological models. *Scandinavian Actuarial Journal*, 2021(8) :671–694, jan 2021.

[7] Hiscox. Hiscox uk cyber readiness report 2022, 2022.

[8] IBM. Cost of a data breach. 2022.

[9] Kaspersky. Kaspersky global report. Septembre 2020.

[10] Legifrance. Décret 2008-1354. 2008.

[11] Bertrand Lemaire. L'amrae éclaire la cyber-assurance avec son étude lucy. *CIO*, Mai 2022.

[12] Michael Y. Li. *An Introduction to Mathematical Modeling of Infectious Diseases*. Springer International Publishing, Cham, 2018.

[13] Brieuc Spoorenberg Louise d'Oultremont, Olivier Lopez. Modeling accumulation scenarios in cyber risk. 2021.

[14] Sénat. La cybersécurité des entreprises - prévenir et guérir : quels remèdes contre les cyber virus ? Juin 2021.

[15] Alice Vitard. Les pertes dues à la cybercriminalité s'élèvent à plus d'1 % du pib mondial. Décembre 2020.