Mémoire présenté le :

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

Par : Antoine Delelis-Fanien

Titre : Tarification du risque cyber par approche micro-économique

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

Les signataires s'engagent à respecter la confidentialité indiquée ci-dessus

Membre présents du jury de l'Institut des Actuaires

signature

Membres présents du jury de l'ISFA

Entreprise :

Nom : SeaBird

Signature :

Directeur de mémoire en entreprise :

Nom : Romain NOBIS

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

Le risque cyber pose de nouveaux défis aux assureurs, notamment en matière de tarification, car les impacts financiers peuvent être significatifs. Actuellement, la question de l'assurabilité de ce risque reste un sujet de préoccupation majeur pour les assureurs, en raison du manque de connaissances et de maîtrise des spécificités du risque cyber.

Dans le cadre de cette étude, une attention particulière sera portée à l'élaboration d'une base de données française des attaques cyber en croisant les données disponibles en libre accès des bases PRC et VERIS avec les rapports LUCY de l'AMRAE. Cette démarche vise à pallier le manque de données spécifiques au contexte français et à renforcer la pertinence des analyses.

Ensuite, l'étude s'appuiera sur des modèles micro-économiques pour déterminer une prime optimale, en tenant compte de l'utilité perçue par les entreprises assurées. Cette approche permettra de mieux tarifer les polices d'assurance en fonction des attentes et des risques propres à chaque entreprise.

Enfin, une analyse de sensibilité sera conduite pour évaluer l'impact des différentes hypothèses formulées, notamment celles dues aux limitations de données. Cette étape critique permettra de tester la robustesse des conclusions et d'affiner les modèles en fonction des résultats obtenus, garantissant ainsi une approche de tarification plus fiable et adaptée aux réalités du marché cyber.

Mots-clés : *Risque cyber*, *Tarification*, *Utilité*, *Micro-économique*, *PRC*, *VERIS*, *LUCY*, *AMRAE*

Abstract

Cyber risk presents new challenges for insurers, particularly in terms of pricing, due to the potentially significant financial impacts. Currently, the issue of insurability for this risk remains a major concern for insurers, given the lack of knowledge and control over the specificities of cyber risk.

As part of this study, special attention will be given to developing a French database of cyberattacks by cross-referencing publicly available data from the PRC and VERIS databases with the LUCY reports from AMRAE. This approach aims to address the lack of data specific to the French context and to enhance the relevance of the analyses.

Next, the study will rely on microeconomic models to determine an optimal premium, taking into account the perceived utility for insured companies. This approach will enable better pricing of insurance policies based on the expectations and specific risks of each company.

Finally, a sensitivity analysis will be conducted to assess the impact of the various hypotheses formulated, particularly those due to data limitations. This critical step will test the robustness of the conclusions and refine the models based on the results obtained, thereby ensuring a more reliable pricing approach that is adapted to the realities of the cyber market.

Keywords: *Cyber risk*, *Pricing*, *Utility*, *Microeconomic*, *PRC*, *VERIS*, *LUCY*, *AMRAE*

Note de Synthèse

Cadre de l'étude

Comprendre et tarifer efficacement le risque cyber nécessite une connaissance approfondie de la nature et de l'évolution de ces risques. Caractérisés par leur dynamisme constant et la sophistication croissante des menaces, les risques cyber imposent une adaptation continue des produits d'assurance pour offrir une couverture pertinente. Une définition précise du "risque cyber" est difficile à établir, car il n'existe pas de consensus parmi les experts en sécurité, les gouvernements et les assureurs sur la façon de l'appréhender.

Pour mieux cerner ces risques, l'État français les classe en plusieurs catégories d'attaques aux impacts variés sur les individus, les entreprises et les administrations :

- **Cybercriminalité** : Vol de données personnelles ou financières pour un usage frauduleux.
- **Déstabilisation** : Attaques visant à nuire à la réputation ou à perturber les services.
- **Sabotage** : Destruction ou altération des systèmes d'information.
- **Espionnage** : Collecte secrète d'informations sensibles à des fins économiques, politiques ou militaires.

La complexité réside également dans le fait que les décisions et comportements des différents acteurs peuvent influencer mutuellement leur exposition au risque. Cette nature interdépendante et dynamique du risque cyber pose des défis significatifs pour les assureurs, qui doivent non seulement évaluer le risque de manière précise, mais aussi adapter les stratégies de tarification des polices d'assurance cyber en conséquence. Les méthodes de tarification traditionnelles, principalement basées sur le coût et la fréquence des sinistres, ne parviennent pas à saisir cette complexité et la variabilité des risques cyber.

Pour relever ces défis, cette étude propose de recourir à des modèles micro-économiques et à la théorie des jeux pour développer une approche de tarification innovante. En modélisant les interactions stratégiques entre les acteurs de l'assurance cyber, ces outils prennent en compte les influences mutuelles sur les décisions de protection et d'assurance.

Micro-économie de l'assurance cyber

Pour pouvoir proposer une prime à l'entreprise, ou agent i, tout en s'assurant de réaliser un profit, il faut commencer par établir les gains et pertes potentiels de l'entreprise avec et sans assurance.

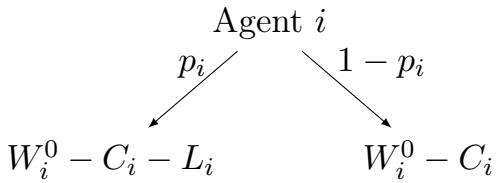

FIGURE 1 : Arbre représentant le risque de l'agent i sans assurance.

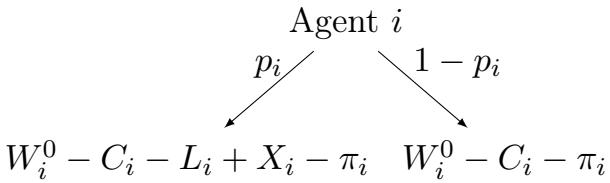

FIGURE 2 : Arbre représentant le risque de l'agent i avec assurance.

TABLE 1 : Description des Variables

Nom de la Variable	**Notation**
Probabilité d'incidence d'une attaque cyber associée à l'agent i	p_i
Richesse de l'agent i après la période d'assurance	W_i
Richesse initiale de l'agent i	W_i^0
Fonction d'utilité de l'agent i	U_i
Coût de l'autoprotection de l'agent i	C_i
Prime d'assurance de l'agent i	π_i
Profit de l'assureur sur l'agent i	Π_i
Niveau d'autoprotection de l'agent i	x_i

Ensuite, il est nécessaire d'examiner l'utilité associée à chaque acteur de l'assurance cyber, c'est-à-dire la mesure de la satisfaction ou du bien-être que chaque acteur retire de ses décisions. L'entreprise qui souhaite s'assurer cherche à réduire son exposition au risque, et sa fonction d'utilité doit refléter cette préoccupation. Deux fonctions d'utilité couramment utilisées en assurance peuvent être appliquées dans ce contexte :

- *Constant Relative Risk Aversion* (ou fonctions d'utilité **CRRA**)

$$U(x) = \frac{x^\alpha}{\alpha},\ \alpha \neq 0 \tag{1}$$

- *Constant Absolute Risk Aversion* (ou fonctions d'utilité **CARA**)

$$U(x) = -\frac{1}{\alpha}e^{-\alpha x},\ \alpha > 0 \tag{2}$$

Les bases de données disponibles

Une partie essentielle de l'étude porte sur l'évaluation des bases de données disponibles pour la modélisation des risques cyber. Les bases PRC et VERIS sont parmi les plus populaires et sont fréquemment utilisées dans la plupart des recherches en assurance cyber. En comparant ces deux bases, tant sur le plan qualitatif que quantitatif, la base VERIS se distingue comme étant plus pertinente pour notre étude. Toutefois, elle présente certaines limitations, notamment sa focalisation majoritaire sur le marché américain. En combinant les données de VERIS avec celles des rapports LUCY, nous pouvons adapter et renforcer la pertinence de cette base pour le marché français tout en offrant une estimation plus précise de la sévérité des attaques.

Nous obtenons alors une base résultante se présentant sous la forme suivante :

Nom	**Année**	**Type**	**Secteur**	**Taille**	**Montant**	**Types d'attaque**
Cameron Univ	2023	ETI	EDU	XS et S	38 461	['malware', 'hacking', 'social']
Tokopedia	2020	ETI	BSR	XS et S	71 194	['hacking']
SCUF Gaming	2020	ME	BSO	XS et S	181 538	['error']

TABLE 2 : Trois sinistres de la base de données résultante

Tarification

Enfin, cette étude propose un modèle de tarification optimisé pour l'assurance cyber en s'appuyant sur des principes microéconomiques et la bases de données précédemment construite. L'objectif est de définir une prime d'assurance qui maximise à la fois l'intérêt des assureurs et celui des entreprises assurées.

Le modèle repose sur une approche d'optimisation visant à équilibrer le profit de l'assureur et l'utilité perçue par les entreprises clientes. En reprenant la formulation classique, le problème s'écrit :

$$\max \Pi_i = (1 - p_i) \cdot \pi_i + p_i \cdot (\pi_i - X_i)$$

avec les conditions suivantes :

$$\mathbb{E}\left[U_i(W_i)\right] \geq \mathbb{E}\left[U_i(W_i)\right]_r$$

Nous trouvons l'équation de la prime pure optimale :

$$\pi_i^* = W_i^0 - C_i - U^{-1}((1 - p_i) \cdot U_i(W_i^0 - C_i) + p_i \cdot U_i((W_i^0 - L_i - C_i)) \tag{3}$$

L'ajout de franchises permet d'introduire une répartition des coûts entre l'assureur et l'assuré, modifiant ainsi l'espérance d'utilité et le calcul de la prime. La prime devient alors une fonction ajustée en fonction du seuil de franchise appliqué :

$$\pi_i^* = (1 + \lambda)(L_i - \delta_i^* \cdot L_i)p_i$$

où δ_i^* représente la franchise optimale appliquée à l'assuré. Cette modification impacte directement l'équilibre du modèle et permet de mieux refleter la réalité.

L'analyse de sensibilité montre que la prime optimale évolue en fonction des variations de la probabilité d'incident cyber (p_i) et la richesse initiale de l'assuré i.

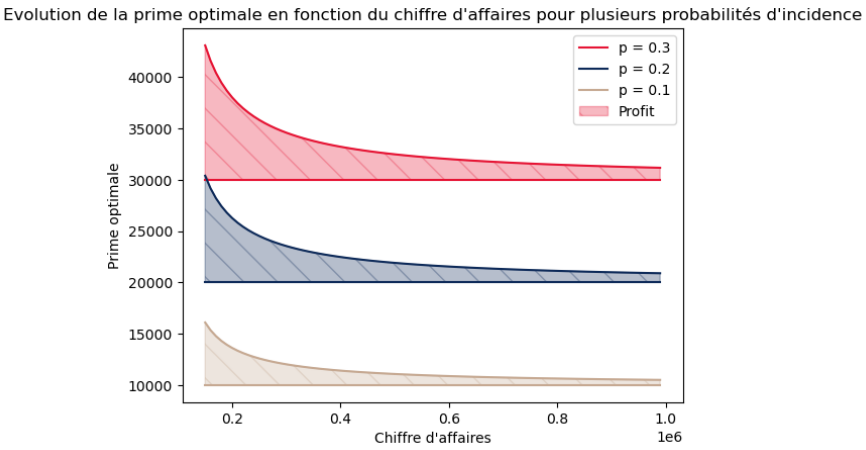

FIGURE 3 : Evolution de la prime optimale pour la fonction d'utilité $U(x) = ln(x)$

Cette variation met en évidence l'importance d'une estimation précise de p_i et montre que, pour assurer un équilibre entre rentabilité et attractivité, la marge de profit de l'assureur tend à diminuer à mesure que la richesse initiale de l'assuré augmente.

Plusieurs scénarios ont été étudiés afin d'évaluer la probabilité p_i en fonction des différents type d'entreprise pour notre modèle :

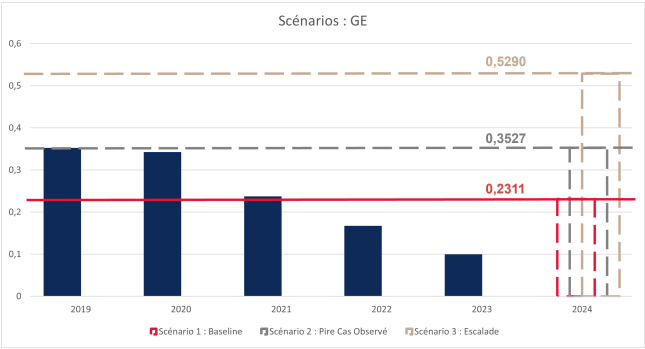

FIGURE 4 : Les différents scénarios appliqués aux grandes entreprises

En appliquant à la base de données précédemment construite, nous trouvons une prime pure pour chaque type d'entreprise et pour chaque scénario :

Scénario	**Baseline**	**Maximum Historique**	**Escalade**
Grande Entreprise	127 786	154 285	72 387
Entreprise de Taille Intermédiaire	25 532	39 645	46 168
Moyenne Entreprise	5 272	11 389	16 500
Petite Entreprise	1 800	4 312	6 355

TABLE 3 : Prime Pure Moyenne optimale par entreprise assurée et par scénario

Ces résultats montrent des variations notables selon la taille des entreprises, avec des primes plus élevées pour les grandes structures en raison de leur exposition accrue au risque cyber. L'intégration des franchises permet également d'ajuster la couverture de manière plus fine et de proposer une tarification plus attractive.

Ainsi, cette approche permet de proposer un cadre méthodologique rigoureux et adaptable, contribuant à une meilleure structuration du marché de l'assurance cyber, tout en offrant une base pertinente pour la tarification du risque, y compris lorsque les données disponibles sont moins fiables.

Synthesis note

Study Framework

Understanding and effectively pricing cyber risk requires in-depth knowledge of the nature and evolution of these risks. Characterized by their constant dynamism and the increasing sophistication of threats, cyber risks demand continuous adaptation of insurance products to provide relevant coverage. Defining "cyber risk" precisely is challenging, as there is no consensus among security experts, governments, and insurers on how to approach it.

To better categorize these risks, the French government classifies them into several attack categories with varying impacts on individuals, businesses, and administrations:

- **Cybercrime**: Theft of personal or financial data for fraudulent use.
- **Destabilization**: Attacks aimed at damaging reputation or disrupting services.
- **Sabotage**: Destruction or alteration of information systems.
- **Espionage**: Covert collection of sensitive information for economic, political, or military purposes.

The complexity also lies in the fact that the decisions and behaviors of various actors can mutually influence their exposure to risk. This interdependent and dynamic nature of cyber risk poses significant challenges for insurers, who must not only assess the risk accurately but also adapt cyber insurance pricing strategies accordingly. Traditional pricing methods, primarily based on cost and frequency of claims, fail to capture this complexity and the variability of cyber risks.

To address these challenges, this study proposes using microeconomic models and game theory to develop an innovative pricing approach. By modeling strategic interactions among cyber insurance actors, these tools account for mutual influences on protection and insurance decisions.

Microeconomics of Cyber Insurance

To offer a premium to a company, or agent i, while ensuring profitability, it is necessary to first establish the potential gains and losses of the company with and without insurance.

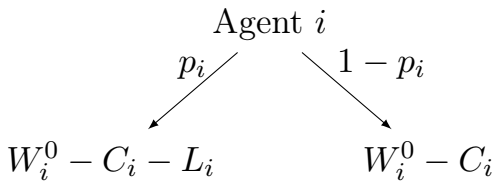

Figure 5: Tree representing agent i's risk without insurance.

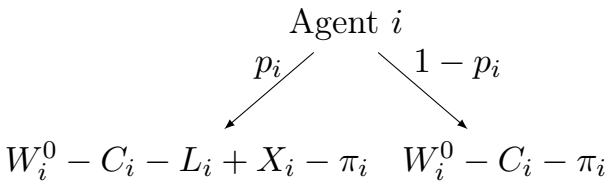

Figure 6: Tree representing agent i's risk with insurance.

Table 4: Variable Descriptions

Variable Name	**Notation**
Probability of a cyber attack incident for agent i	p_i
Wealth of agent i after the insurance period	W_i
Initial wealth of agent i	W_i^0
Utility function of agent i	U_i
Cost of self-protection for agent i	C_i
Insurance premium for agent i	π_i
Insurer's profit on agent i	Π_i
Level of self-protection for agent i	x_i

Next, it is necessary to examine the utility associated with each cyber insurance actor, i.e., the measure of satisfaction or well-being each actor derives from their decisions. The company seeking insurance aims to reduce its exposure to risk, and its utility function should reflect this concern. Two commonly used utility functions in insurance can be applied in this context:

- *Constant Relative Risk Aversion* (CRRA utility functions)

$$U(x) = \frac{x^\alpha}{\alpha},\ \alpha \neq 0 \tag{4}$$

- *Constant Absolute Risk Aversion* (CARA utility functions)

$$U(x) = -\frac{1}{\alpha}e^{-\alpha x},\ \alpha > 0 \tag{5}$$

Available Databases

A crucial part of the study focuses on evaluating available databases for modeling cyber risks. The PRC and VERIS databases are among the most popular and are frequently used in most cyber insurance research. Comparing these two databases both qualitatively and quantitatively, VERIS emerges as more relevant for our study. However, it has certain limitations, particularly its predominant focus on the U.S. market. By combining VERIS data with LUCY reports, we can adapt and enhance the relevance of this database for the French market while providing a more accurate estimate of attack severity.

As a result, we obtain a combined database structured as follows:

Name	Year	Type	Sector	Size	Amount	Attack Types
Cameron Univ	2023	ETI	EDU	XS and S	38,461	['malware', 'hacking', 'social']
Tokopedia	2020	ETI	BSR	XS and S	71,194	['hacking']
SCUF Gaming	2020	ME	BSO	XS and S	181,538	['error']

Table 5: Three claims from the resulting database

Pricing

Finally, this study proposes an optimized pricing model for cyber insurance based on microeconomic principles and the previously constructed database. The goal is to define an insurance premium that maximizes both insurer interest and insured companies' benefit.

The model relies on an optimization approach balancing insurer profit and perceived utility of client companies:

$$\max \Pi_i = (1 - p_i) \cdot \pi_i + p_i \cdot (\pi_i - X_i)$$

with the following conditions:

$$\mathbb{E}\left[U_i(W_i)\right] \geq \mathbb{E}\left[U_i(W_i)\right]_r$$

We derive the optimal pure premium equation:

$$\pi_i^* = W_i^0 - C_i - U^{-1}((1 - p_i) \cdot U_i(W_i^0 - C_i) + p_i \cdot U_i((W_i^0 - L_i - C_i)) \tag{6}$$

The introduction of deductibles allows for a cost-sharing mechanism between the insurer and the insured, thereby modifying the expected utility and premium calculation. The adjusted premium function based on the applied deductible threshold is:

$$\pi_i^* = (1 + \lambda)(L_i - \delta_i^* \cdot L_i)p_i$$

where δ_i^* represents the optimal deductible applied to the insured. This modification directly impacts the model equilibrium and better reflects real-world conditions.

Sensitivity analysis shows that the optimal premium evolves based on variations in the probability of cyber incidents (p_i) and the initial wealth of the insured i.

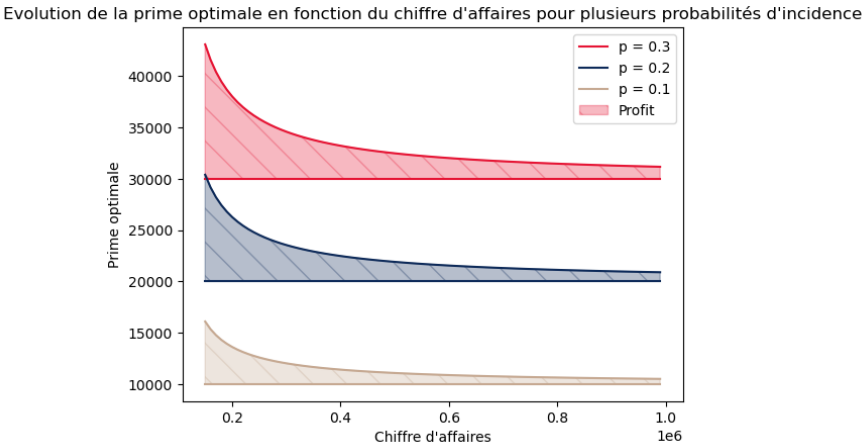

Figure 7: Evolution of the optimal premium for the utility function $U(x) = ln(x)$

This variation highlights the importance of accurately estimating p_i and demonstrates that to maintain a balance between profitability and attractiveness, the insurer's profit margin tends to decrease as the insured's initial wealth increases.

Several scenarios were analyzed to evaluate the probability p_i based on different types of businesses in our model:

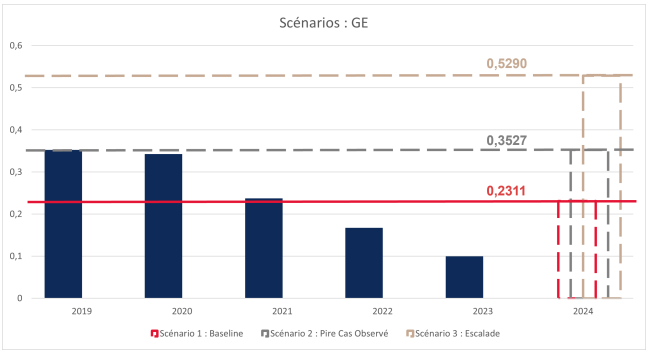

Figure 8: Different scenarios applied to large enterprises

Applying the previously constructed database, we derive the pure premium for each business type and scenario:

Scenario	**Baseline**	**Historical Maximum**	**Escalation**
Large Enterprise	127,786	154,285	72,387
Mid-Sized Enterprise	25,532	39,645	46,168
Medium Enterprise	5,272	11,389	16,500
Small Business	1,800	4,312	6,355

Table 6: Optimal Average Pure Premium per insured business and scenario

These results show significant variations depending on company size, with higher premiums for

large organizations due to their increased exposure to cyber risk. The integration of deductibles also allows for more refined coverage adjustments and more attractive pricing.

Thus, this approach provides a rigorous and adaptable methodological framework, contributing to better structuring of the cyber insurance market, while also offering a relevant basis for the risk pricing, even when the available data is less reliable.

Remerciements

Je tiens à exprimer ma profonde gratitude à Mathieu VILTIE, qui m'a inspiré le sujet de ce mémoire et m'a accompagné en tant qu'encadrant dans sa mise en place.

Un immense merci également à Romain NOBIS pour son accompagnement, pour avoir repris ce sujet avec moi et pour m'avoir permis de progresser sur le plan technique.

Enfin, je remercie chaleureusement l'équipe actuarielle des juniors de Seabird, avec qui la rédaction de ce mémoire a été non seulement enrichissante, mais aussi particulièrement agréable.

Table des matières

Introduction

L'assurance cyber représente aujourd'hui un enjeu crucial pour les entreprises confrontées à une augmentation constante des attaques cyber. À mesure que les infrastructures numériques deviennent essentielles aux activités économiques, les risques associés aux intrusions, vols de données et attaques par *ramsomware* s'intensifient. Dans ce contexte les assureurs doivent faire face à plusieurs défis : la volatilité du risque cyber, le manque de données fiables et la difficulté de proposer des modèles de tarification adaptés aux différentes structures d'entreprise.

Le marché de l'assurance cyber reste encore en développement et souffre d'une instabilité marquée par des variations importantes de primes et des couvertures proposées. Contrairement aux autres branches d'assurances, la modélisation du risque cyber est particulièrement complexe en raison de son caractère évolutif et des difficultés de collecte des données. Les entreprises, notamment les grandes structures, restent souvent réticentes à signaler les incidents, ce qui empêche d'obtenir une vision exhaustive des sinistres et de leurs impacts financiers.

Dans ce mémoire, nous proposons une approche fondée sur des modèles microéconomiques pour estimer des primes d'assurances cyber en prenant en compte la richesse initiale des entreprises, leur exposition aux risques et leurs investissements en cybersécurité. Pour pallier le manque de données exploitable et pour mieux représenter le marché de l'assurance français, nous avons croisé deux bases de données majeures : **VERIS**, qui fournit une classification détaillée des incidents cyber, et **LUCY**, qui offre une vision plus adaptée au marché français en intégrant des données sur les coûts des sinistres et les primes observées.

L'objectif de cette étude est de proposer une méthode de tarification optimisée permettant d'assurer un équilibre entre rentabilité pour les assureurs et accessibilité pour les entreprises assurées. Pour ce faire, nous appliquons un modèle d'optimisation basé sur les fonctions d'utilité et nous introduisons des franchises adaptées afin de refléter la réalité du marché.

Dans un première partie, nous analyserons le marché de l'assurance cyber et les défis qu'il pose en terme de tarification. Puis, dans une deuxième partie, nous présenterons les concepts fondamentaux en microéconomie permettant d'établir un modèle de tarification adapté à la tarification du risque cyber. Ensuite, dans une troisième partie, nous analyserons les principales bases de données utilisées pour évaluer le risque cyber, en croisant notamment las base VERIS et LUCY afin d'obtenir une vision plus complète et adaptée au marché français. Enfin, dans une quatrième partie, nous mettrons en oeuvre une modèle de tarification basé sur les résultats précédents et analyserons les primes obtenues sous différents scénarios de risque.

En structurant ainsi cette approche, nous chercherons à répondre à la question essentielle : **Comment établir un modèle de tarification optimisé pour l'assurance cyber, tenant compte du manque de données, de l'incertitude liée à l'évolution du risque et de l'équilibre entre attractivité pour l'assuré et viabilité pour l'assureur ?**

Ce travail vise ainsi à fournir une contribution méthodologique à la tarification du risque cyber en combinant une analyse empirique de données disponibles et une approche microéconomique rigoureuse.

Chapitre 1

Cadre du Risque Cyber : contexte et enjeux

Pour aborder efficacement la tarification d'un risque cyber, il est primordial de comprendre en profondeur la nature et l'évolution des risques cyber. Ces derniers représentent un défi unique en raison de leur dynamisme constant et de la sophistication croissante des menaces. Par conséquent, l'adaptation et la mise à jour des produits d'assurance cyber sont essentielles pour fournir une couverture adéquate et pertinente face à ces risques.

1.1 Définition du risque cyber

L'une des complexités majeures dans la tarification en assurance cyber réside dans la définition et la compréhension du "risque cyber". Actuellement, il n'y a pas d'unanimité sur ce terme, ce qui reflète la diversité des perspectives parmi les experts en sécurité, les gouvernements, les entreprises et les chercheurs. Pour certains, il s'agit principalement de risques opérationnels liés à la sécurité des données et des systèmes d'information, affectant leur confidentialité, leur intégrité ou leur disponibilité. D'autres, comme la Banque de France (n.d.), le voient comme la probabilité d'incidents pouvant compromettre la cybersécurité. De même, des assureurs tels que North Bridge Assurance (n.d.) le définissent en termes de pertes financières, d'interruption des activités ou de dommages à la réputation découlant de défaillances des systèmes informatiques. Cette diversité de définitions souligne les défis dans l'établissement de politiques de sécurité efficaces et dans la gestion adéquate des incidents cyber.

Afin de faire face à ces défis, il est essentiel d'établir un périmètre d'étude, de définir et de souligner les fondamentaux du risque cyber, de présenter l'état des lieux du marché de l'assurance cyber et d'analyser l'ensemble des lois et régulations qui encadrent ce risque. Tout ce travail en amont permettra de clarifier la définition que l'on souhaite donner au risque cyber dans le cadre de la tarification de l'assurance cyber.

Pour mieux comprendre le risque cyber, il faut d'abord étudier les menaces qui composent ce risque. Chaque menace a des conséquences différentes et leur mode d'actions varie selon le type d'attaque utilisé. Selon le Gouvernement Français (2023), les différentes menaces se présentent de la façon suivante :

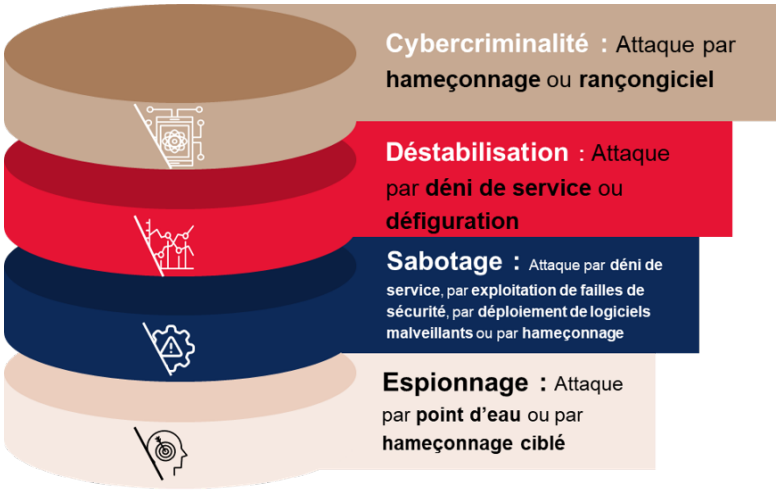

FIGURE 1.1 : Les différentes menaces cyber

1.1.1 Menace de cybercriminalité

La cybercriminalité englobe les attaques visant à obtenir des informations personnelles qui seront ensuite exploitées ou revendues. Les victimes de ces attaques sont à la fois les particuliers mais également les entreprises ainsi que les administrations. Les informations bancaires et les identifiants des commerces en ligne sont les principales données ciblées par les cybercriminels. Deux sortes d'attaques ont été différenciées :

- **Attaque par hameçonnage (ou *phishing*)**
  L'attaque par hameçonnage ou phishing est une méthode très répandue sur Internet. Les cybercriminels usurpent l'identité des personnes afin d'obtenir des renseignements personnels ou encore des identifiants bancaires qui permettront d'être utilisés ultérieurement. L'usurpation se fait par le biais de personnes physiques ou morales de confiance. Les hackers diffusent un message ou un mail frauduleux pouvant contenir une pièce jointe piégée. Ce dernier invite l'utilisateur à entrer ses informations personnelles, notamment ses coordonnées bancaires sur des sites fictifs vers lesquels ils sont redirigés. Ce type d'attaque ne cible pas une personne en particulier mais plutôt un grand nombre de contacts. En effet, plus le nombre de personnes contactées est grand, plus les chances que l'un d'entre eux ouvre la pièce jointe et/ou entre ses données personnelles sont importantes.

- **Attaque par rançongiciel (ou *ramsomware*)**
  L'attaque par rançongiciel ou ransomware est de plus en plus répandue. Les cybercriminels chiffrent les données puis demandent aux propriétaires de ces dernières d'envoyer de l'argent en échange d'une clé qui permettra (« théoriquement ») de les déchiffrer. Pour ce faire, les pirates diffuseront un mail ou un message contenant des liens ou pièces jointes piégées. Par exemple, la victime peut recevoir un mail lui indiquant de payer rapidement une facture qui ne l'a pas été. Dès lors que l'utilisateur cliquera sur le lien ou les pièces jointes, un logiciel se téléchargera directement sur son poste de travail et commencera à chiffrer ses données personnelles. Les données ciblées sont de toutes sortes : bureautique, vidéos, musiques ou encore photos.

1.1.2 Menace de déstabilisation

Avec une fréquence croissante, les cyberattaques visant à déstabiliser les administrations et entreprises utilisent des outils et services accessibles en ligne. Leur objectif est de nuire à la réputation de la victime. Cette menace compte deux principales attaques.

- **Attaque par déni de service (*Distributed Denial of Service* ou DDoS)**
  Une attaque de déni de service, qui peut nuire à la réputation de la victime, représente une menace pour toute organisation ayant un système d'information en ligne. L'objectif est de rendre le site, et donc le service attendu, indisponible. Les motivations des attaquants sont variées, allant des manifestes idéologiques à la vengeance, en passant par le chantage financier. Le cybercriminel peut exploiter une faiblesse dans le logiciel ou le matériel, ou encore surcharger une ressource spécifique (comme la bande passante du réseau, la capacité de traitement d'une base de données, etc.) du système d'information de la victime jusqu'à son "épuisement". Des signes courants incluent une augmentation inexplicable de l'utilisation de la bande passante, des interruptions de communication en raison d'un délai d'attente (*timeout*) ou signalées par un message d'erreur (*host unreachable*), etc. Il existe plusieurs méthodes pour atteindre un résultat unique : des dysfonctionnements ou une paralysie complète d'un ou de plusieurs services de la victime.

- **Attaque par « défiguration » (*defacement*)**
  Ce type d'attaque est souvent revendiqué par des hacktivistes (Un hacktiviste est un individu ou un groupe qui utilise le piratage informatique pour défendre une cause politique ou sociale, souvent par le biais de méthodes telles que le piratage de sites Web ou la publication d'informations volées) et peut être réalisé dans un but politique ou idéologique, ou simplement comme un défi technique entre attaquants. L'objectif est de changer l'apparence ou le contenu d'un site, altérant ainsi l'intégrité de ses pages. Le cybercriminel exploite souvent des failles dans le site, parfois connues mais non rectifiées. Qu'elle soit visible ou plus subtile pour le visiteur, la réussite de l'attaque peut se manifester de différentes manières, par exemple par l'ajout d'informations sur une page ou le remplacement complet d'une page par une revendication.

1.1.3 Menace de Sabotage

Le sabotage informatique consiste à rendre inutilisable une partie ou l'ensemble d'un système d'information d'une organisation par le biais d'une cyberattaque. Il est similaire à une "panne orchestrée" qui peut affecter une portion ou la totalité des systèmes, selon le type de dommage visé. Plusieurs méthodes d'attaque sont employées, parmi lesquelles le déploiement de logiciels malveillants, les attaques par déni de service, l'exploitation de failles de sécurité ou par hameçonnage. Le sabotage et la destruction de systèmes informatiques peuvent avoir des conséquences catastrophiques sur l'économie d'une organisation, sur la vie des individus, voire sur la stabilité nationale s'ils affectent des secteurs d'activité essentiels.

1.1.4 Menace d'Espionnage

Les attaques visant l'espionnage — qu'il soit économique, scientifique ou politique — sont généralement très spécifiques et sophistiquées. Elles sont souvent perpétrées par des groupes organisés et peuvent gravement affecter les intérêts nationaux. Une organisation peut mettre des années à découvrir qu'elle

a été victime d'espionnage, l'objectif de l'attaquant étant de maintenir un accès discret et durable pour récupérer des informations stratégiques au moment opportun. On y compte deux attaques majeures :

- **Attaque par point d'eau (*watering hole*)**
  Cette technique consiste à piéger un site en ligne légitime afin d'infecter les équipements des visiteurs du secteur d'activité visé par l'attaquant. L'objectif étant d'infiltrer discrètement les ordinateurs de personnels œuvrant dans un secteur d'activité ou une organisation ciblée pour récupérer des données.

- **Attaque par hameçonnage ciblé (*spearphishing*)**
  Cette attaque repose généralement sur une usurpation de l'identité de l'expéditeur, et procède par ingénierie sociale forte afin de lier l'objet du courriel et le corps du message à l'activité de la personne ou de l'organisation ciblée l'objectif étant d'infiltrer le système d'information d'une organisation d'un secteur d'activité ciblé.

1.1.5 Retour sur quelques évènements marquants

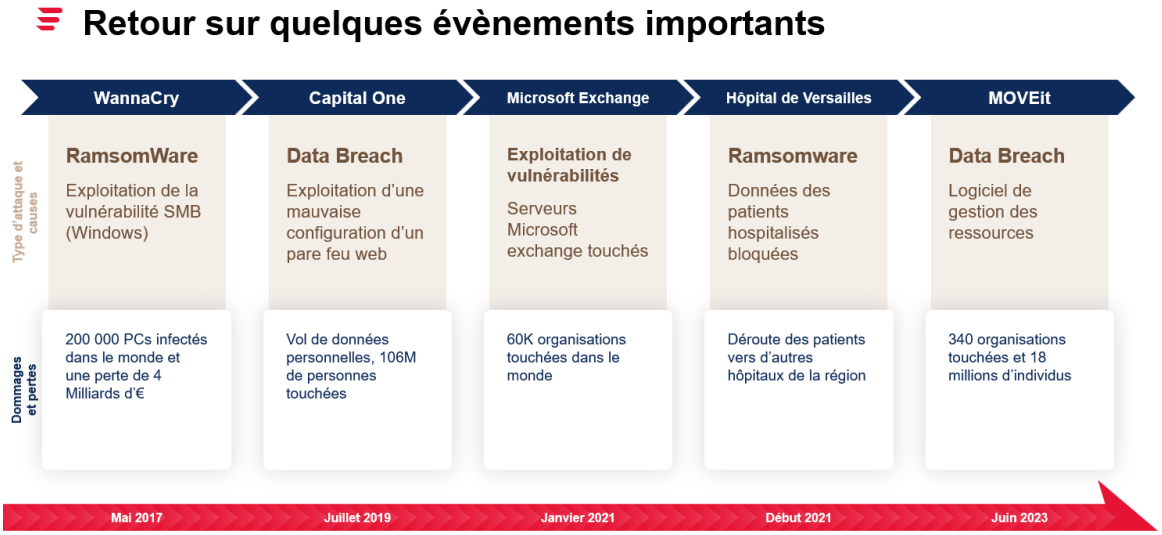

FIGURE 1.2 : Différentes attaques cyber survenues ces dernières années

Les attaques cyber présentées dans la frise ci-dessus ont démontré une fréquence croissante de la sinistralité et une sévérité accrue ces dernières années. Elles montrent que les secteurs des organismes touchés peuvent être très différents d'une attaque à l'autre. Ces attaques ont également eu un impact significatif sur les systèmes informatiques et les infrastructures entraînant des perturbations majeures. Les coûts associés à ces attaques sont considérables, allant des pertes financières directes aux coûts indirects tels que la perte de clients, la réputation ternie, les litiges potentiels, l'interruption des activités et la baisse de productivité.

1.2 État des lieux du marché cyber

Pour pouvoir tarifer le risque cyber, il est essentiel d'examiner d'abord l'importance de l'assurance cyber sur le marché actuel. De nombreux documents nous donnent un aperçu de la situation actuelle du marché de l'assurance cyber et des défis qu'elle présente. Notamment les études LUCY de l'AMRAE qui nous donne une vision globale du marché français de l'assurance cyber et une étude plus focalisée sur les assurés, le rapport du CESIN, qui surligne les difficultés à mettre en place une assurance cyber.

1.2.1 Rapports de l'AMRAE

L'AMRAE (2020 - 2024) (Association pour le Management des Risques et des Assurances de l'Entreprise) est une organisation qui se consacre à la promotion et à la gestion des risques au sein des entreprises. Dans le cadre de son engagement, l'AMRAE publie chaque année depuis 2019 une étude appelée LUCY (LUmière sur la CYberassurance), qui constitue la première analyse du risque cyber et de sa couverture assurantielle en France. Elle vise à comprendre les conséquences d'un renouvellement difficile, à évaluer la pénétration du marché de la cyber-assurance dans l'économie et à clarifier les enjeux liés à ce risque. L'objectif de l'étude LUCY est de favoriser un dialogue entre assureurs, courtiers et assurés pour renforcer la protection de l'environnement économique face aux menaces cyber.

Voici les points importants de l'étude de 2024 :

FIGURE 1.3 : Points clés du rapport de l'AMRAE

D'après l'étude de 2023, le marché de l'assurance cyber en France a continué de se stabiliser, prolongeant les tendances amorcées en 2022. Le montant des sinistres enregistrés a chuté de manière significative, atteignant une baisse de 46 %, avec une indemnisation totale de 38 millions d'euros

contre 70,8 millions en 2022. Cette réduction de sinistralité a été observée dans toutes les catégories d'entreprises, y compris les grandes entreprises, où les sinistres ont diminué de 45 %, et les entreprises de taille intermédiaire qui ont enregistré une baisse de 48 % des sinistres.

Le volume des primes collectées en 2023 s'élève à 328 millions d'euros, une légère augmentation par rapport aux 316 millions de 2022, témoignant d'un marché qui reste fragile. En effet, malgré cette hausse, le marché pourrait être vulnérable face à quelques sinistres majeurs. Les grandes entreprises ont maintenu leurs budgets constants, avec une souscription quasi similaire à 2022, et le nombre de grandes entreprises assurées est resté stable à 280. Cette stagnation contraste avec la croissance observée dans les segments des entreprises de taille intermédiaire et moyenne, où le nombre d'assurés a augmenté respectivement de 47 % et de 194 %.

Le ratio sinistres/primes a continué de s'améliorer, passant de 22 % en 2022 à 12 % en 2023, signe que les investissements en prévention commencent à porter leurs fruits. Pour les grandes entreprises, ce ratio est même descendu à 9 %, tandis que pour les entreprises de taille intermédiaire, il s'établit à 21 %.

Toutefois, le marché reste sous-assuré, particulièrement pour les entreprises de taille intermédiaire, où seulement 15 % d'entre elles sont couvertes. Le potentiel de croissance dans ce secteur reste donc important.

En conclusion, bien que 2023 ait été une année de consolidation pour le marché de l'assurance cyber en France, avec une sinistralité en forte baisse et une stabilisation des primes, le marché demeure fragile, volatile et sous-assuré, particulièrement face à un contexte géopolitique tendu et à l'émergence de nouvelles menaces comme celles liées à l'intelligence artificielle.

D'après le graphique ci-dessous, il est clairement observé une forte augmentation du montant des sinistres en 2020. Cette augmentation peut être expliquée par l'évolution technologique des attaques cyber ainsi que par la crise du COVID-19 (4 sinistres de haute sévérité), qui a entraîné une augmentation du nombre de personnes travaillant à distance et donc une augmentation de la vulnérabilité des entreprises. Afin de faire face à ce ratio sinistres/primes (S/P) élevé (167%), les assureurs ont continuellement augmenté leurs primes (jusqu'à 316 millions d'euros en 2022). Parallèlement, la fréquence des sinistres a diminué, ce qui a conduit à un ratio S/P très bas (22%), et ce ratio est resté bas en 2023 (12%).

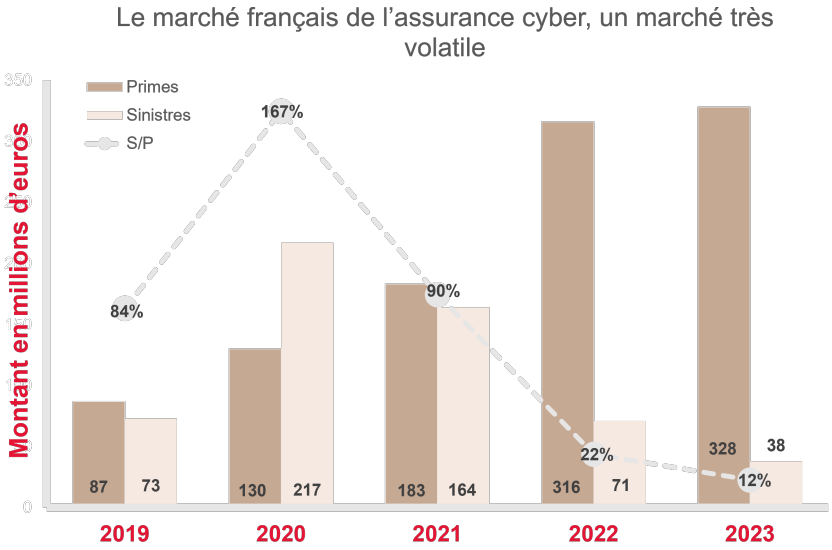

FIGURE 1.4 : Évolution des ratios S/P du marché de l'assurance cyber

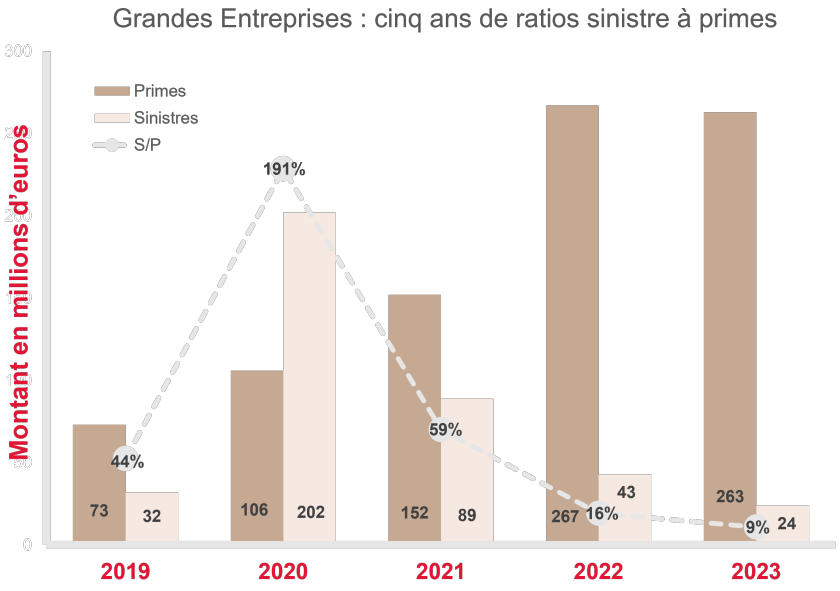

FIGURE 1.5 : Évolution des ratios S/P du marché de l'assurance cyber pour les grandes entreprises de 2019 à 2023

Les grandes entreprises représentent la quasi-totalité du marché français (environ 83%), ainsi la tendance des ratios S/P pour les grandes entreprises de 2019 à 2022 suit donc celle décrite au-dessous. On observe ainsi une baisse particulièrement importante du ratio S/P jusqu'à 16% en 2022 qui

s'explique par une hausse des primes et une baisse de la sinistralité. Ainsi les rapports LUCY montrent une volatilité importante des ratios S/P de 2019 à 2022 et souligne alors l'importance de trouver des primes convenables et adaptées pour obtenir une plus grande stabilité du secteur.

1.2.2 Baromètre du CESIN

Pour approfondir l'étude LUCY, le Club des Experts de la Sécurité Informatique (CESIN (2023)) a publié en 2023, un article intitulé "Le baromètre du CESIN" qui est une étude basée sur les réponses d'un questionnaire auquel participent plusieurs centaines d'entreprises distinctes (328 en 2022), portant sur les défis liés à la cybersécurité. Cette étude comprend également une section consacrée à l'assurance cyber, et nous éclaire sur les difficultés rencontrées par l'assurance cyber. Voici les éléments clés qui en ressortent :

- **Encore 33% d'entreprises n'ont pas souscrit une cyber assurance**
  Deux tiers des entreprises ont souscrit une cyber-assurance, mais plus d'une sur dix hésite à renouveler sa police et 2 % des entreprises y ont déjà renoncé

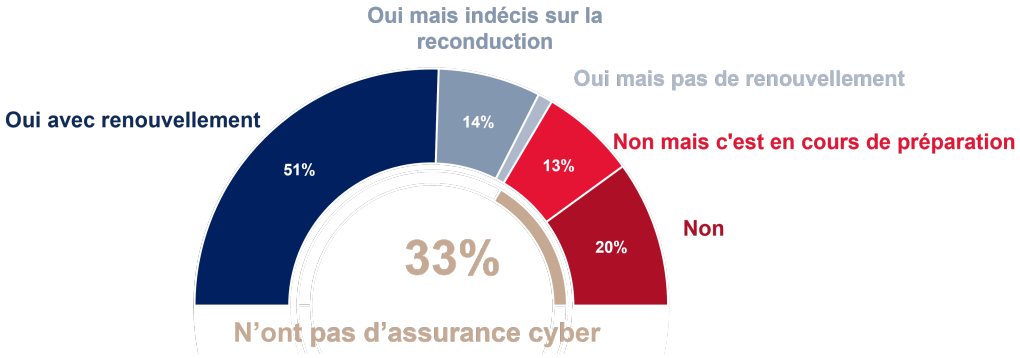

FIGURE 1.6 : Souscription d'une cyber assurance

Le fait que seulement 2/3 des entreprises aient souscrit une cyber assurance suggère qu'il existe encore un certain nombre d'entreprises qui ne considèrent pas cette forme d'assurance comme une priorité. Cela peut être attribué à divers facteurs, tels que le manque de sensibilisation aux risques de cybersécurité, les contraintes budgétaires ou encore une confiance excessive dans les mesures de sécurité internes.

D'autre part, le fait qu'un peu plus d'1/10 des entreprises hésitent à renouveler leur cyber assurance soulève des interrogations quant à la satisfaction ou à l'efficacité perçue de cette forme d'assurance. Les raisons de cette hésitation peuvent être multiples, allant de la complexité des polices d'assurance et des processus de réclamation à la perception d'une offre insuffisante en termes de couverture ou de services.

Ces observations mettent en évidence un double enjeu pour le secteur des assurances cyber. D'une part, il est impératif d'intensifier les efforts de sensibilisation auprès des entreprises sur l'importance de l'assurance cyber pour la gestion des risques de cybersécurité. D'autre part, il est tout aussi vital que les assureurs s'attachent à élaborer des offres non seulement transparentes et ajustées aux réalités du marché, mais également assorties de primes d'assurance cohérentes avec les risques et les capacités financières des entreprises. Adapter les primes d'assurance aux

risques particuliers et à la capacité de résilience de chaque entreprise représente donc une étape essentielle vers l'obtention d'une protection plus pertinente.

- **Parmi les entreprises ayant souscrit une cyber assurance, les trois quarts des entreprises assurées n'ont jamais utilisé leur cyber-assurance**

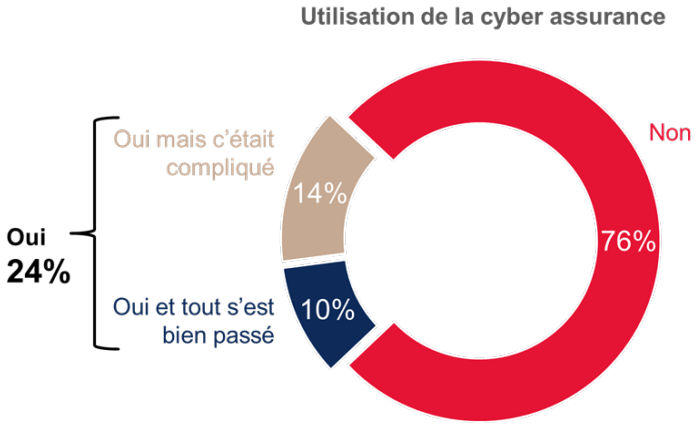

FIGURE 1.7 : Souscription d'une cyber assurance

Le fait que la majorité des entreprises n'aient pas eu besoin de faire appel à leur cyber assurance suggère que la prévention et la gestion des risques de cybersécurité peuvent être efficaces ou alors que celles-ci n'aient pas pris conscience d'un sinistre ayant eu lieu. Cela peut témoigner de la mise en place de mesures de sécurité solides et d'une bonne gestion des incidents par ces entreprises. Cependant, cela ne doit pas conduire à une complaisance, car les menaces cyber continuent d'évoluer et de représenter un risque permanent.

Enfin, le constat que la moitié des entreprises ayant utilisé leur cyber assurance ont jugé le processus compliqué soulève des préoccupations quant à l'expérience client et à l'efficacité des services d'assurance. Cela peut indiquer un manque de clarté dans les polices d'assurance, des procédures de réclamation complexes ou une communication insuffisante entre l'assuré et l'assureur. Ces éléments peuvent entraver la satisfaction des entreprises et leur confiance dans l'assurance cyber.

Ces conclusions soulignent l'importance pour les assureurs de simplifier et de clarifier les processus liés à la cyber assurance. Une meilleure communication, des contrats plus transparents et des procédures de réclamation simplifiées peuvent contribuer à améliorer l'expérience client et renforcer la confiance des entreprises dans leur assurance cyber.

Il est également important que les entreprises qui souscrivent une cyber assurance comprennent clairement les conditions et les limitations de leur couverture, ainsi que les étapes à suivre en cas d'incident de cybersécurité. La sensibilisation, la formation et l'accompagnement des assurés dans la gestion des risques et des sinistres peuvent contribuer à faciliter le processus et à optimiser les avantages de la cyber assurance.

- **En 2021, près de la moitié des entreprises ayant subi une attaque ont déposé une plainte, mais l'identification et l'interrogatoire des attaquants sont rarement effectués**

  Plus de la moitié des entreprises attaquées (54%) ont déposé une plainte, ce qui suggère que ces attaques sont prises très au sérieux et qu'elles sont probablement nuisibles pour les activités des

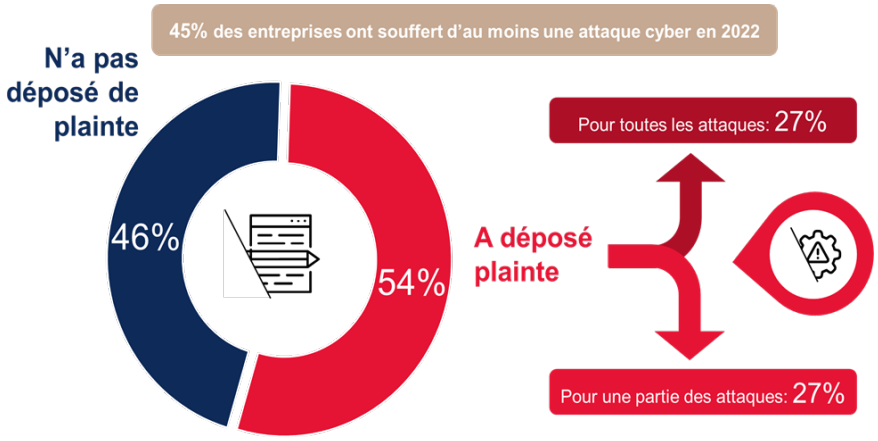

FIGURE 1.8 : Dépôt de plainte après une attaque cyber

entreprises. Cela pourrait aussi indiquer que les entreprises sont de plus en plus conscientes de leurs droits et des voies légales disponibles pour faire face à ces cyberattaques.

L'information sur la nature des plaintes est également intéressante. Elle montre que les entreprises se soucient autant des attaques spécifiques que de l'ensemble des attaques subies. En effet, 27% des plaintes concernent un sinistre en particulier et le même pourcentage concerne tous les sinistres ayant eu lieu. Cela pourrait indiquer que certaines entreprises ont été particulièrement touchées par une attaque spécifique, tandis que d'autres ont subi une série d'attaques au cours de l'année. Pourtant ceci explique bien le problème récurrent de la cyber assurance : en déclarant tous les sinistres en une seule fois, les informations concernant la date d'apparition des sinistres sont faussées et cela affaiblit la pertinence des bases de données et rend difficile la mise en place de modèles précis.

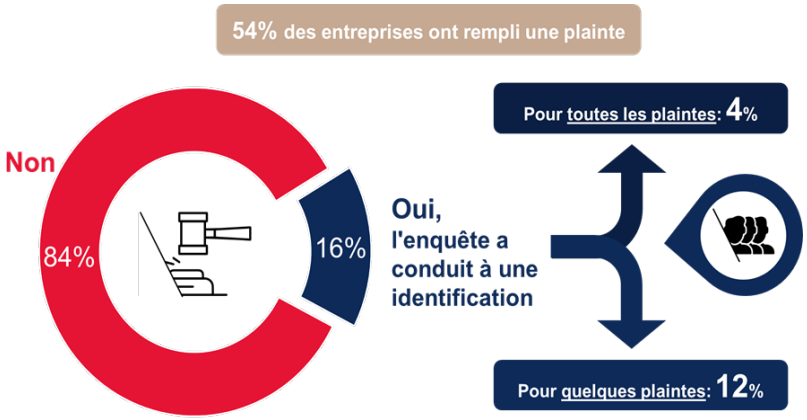

FIGURE 1.9 : Identification après une attaque cyber

Ces statistiques révèlent que malgré le nombre important d'entreprises ayant déposé une plainte suite à une cyberattaque, seulement une faible proportion a conduit à une identification réussie de l'attaque et des données du sinistre. Plus précisément, seulement 16% des plaintes ont abouti

à une telle identification.

Seulement 4% concernent l'identification de toutes les plaintes, ce qui suggère que la majorité des cyberattaques restent non résolues ou non identifiées complètement. Cela peut être dû à la complexité des méthodes d'attaques, à l'expertise nécessaire pour retracer les cybercriminels, ou encore au manque de coopération internationale en matière de cybercriminalité.

Les 12% restants concernent l'identification partielle des plaintes. Cela pourrait signifier que dans certains cas, il est possible d'identifier certains éléments ou aspects de l'attaque, mais pas l'ensemble de la situation. Cette réalité peut être frustrante pour les entreprises qui cherchent à obtenir justice et à prévenir de futures attaques.

Encore une fois, cela montre la difficulté de mise en place de bases de données pertinentes et donc la complexité de créer des produits d'assurance cyber efficaces.

1.2.3 Produits d'assurance cyber présents sur le marché

Pour comprendre le marché d'assurance cyber, on peut s'intéresser aux garanties déjà existantes sur le marché.

Assureurs	Garanties
Groupama	Gestion de crise, Perte d'exploitation, Dommages, dans la limite actuelle de 50 000€
gan	Gestion de crise, Dommages, RC. Formule sur mesure : Pertes d'exploitation, RC étendue, Amendes et pénalités, Dommages en cas d'erreur humaines, Cyber-extorsion, Paiement rançon
GENERALI	Gestion de crise, Perte d'exploitation, Dommages. En option : Fraude
AVIVA	Gestion de crise, Pertes d'exploitation, Dommages.
MMA Entrepreneurs d'Assurances	Gestion de crise avec des garanties classiques (Frais de notification, fraude, etc)
Allianz	Gestion de crise, Pertes d'exploitation, Dommages
COOVER	Perte de données, perte d'exploitation, fraude, cyber-extorsion, garanties RGPD

FIGURE 1.10 : Tableau présentant plusieurs garanties existantes sur le marché français

Ainsi, la plupart des assurance proposent une garantie "gestion de crise", il s'agit d'une intervention de techniciens pour résoudre le problème cyber. D'autres compagnies ajoutent également des garanties comme perte d'exploitation. Peu de compagnies d'assurance rentrent dans les détails et les grandes compagnies comme Allianz couvrent alors tous les dommages liés aux cyber attaques.

De plus, d'autre assurances proposent des franchises ou des plafonds de couverture dans leur garanties cyber. Cela leur permet de réduire leur exposition au risque

Assurance	**Couverture (CHF)**	**Exclusions**
Frais de reconstitution des données numériques et des logiciels suite à un dommage résultant de causes criminelles (cybercriminalité : accès non autorisé ; attaques DDoS)	5'000	Les dommages résultant de l'utilisation de contenu pornographique ; Les dommages résultant d'une défaillance des services publics et de l'infrastructure ; Les dommages résultant d'une négligence grave ou d'actes intentionnels de la part du preneur d'assurance ; Les dépenses encourues par les prestataires de services externes (Service Provider) ; Les dommages déjà couverts par un autre contrat.
Frais pour la suppression/modification de contenus portant atteinte à la personnalité (Cyber-Mobbing)	5 000	
Usurpation d'identité	5'000	
Atteinte aux droits d'auteur, au droit au nom et au droit des marques par des tiers	5 000	
Online-Banking/Usage abusif de cartes de crédit (phishing, hacking, skimming)	5 000	
Protection des achats : Dommages matériels résultant d'un achat online	2 000 (sans déduction d'une franchise)	

TABLE 1.1 : Tableau de garanties risque cyber de la compagnie d'assurance Helvetia, disponible en ligne

1.3 Loi française et assurance cyber

Une autre dimension du risque, qui évolue aussi, concerne la législation. De nouvelles lois et réglementations ont été mises en place et d'autres le seront bientôt. Ceci va transformer le contexte de l'assurance cyber. Parmi ces documents intéressants à étudier, nous comptons *l'assurance en mouvement* de Valéria Laure-Mundian, la loi DORA, la loi LOPMI et les autorités de contrôle avec notamment le RGPD.

1.3.1 L'assurance en mouvement

Afin d'appréhender la difficulté législative qui accompagne le risque cyber, Valéria Faure-Muntian (ex-députée de la Loire et présidente du groupe d'études assurances de l'Assemblée nationale) a rédigé un rapport évoquant les principaux problèmes que rencontre le gouvernement lors de la mise en place de règles communes et y présente plusieurs solutions. Bien que ces règles communes n'aient pas été appliquées par le gouvernement, le rapport souligne les différents enjeux de l'assurance cyber et pose les bases de la loi DORA qui sera appliquée en 2025

Le rapport suggère d'adopter des définitions juridiques pour le cyber-risque et la cyber-attaque.

Il propose une interdiction légale pour les assureurs de garantir, couvrir ou indemniser les rançons demandées suite à une cyber-attaque, encourageant plutôt un focus sur la prévention, l'accompagnement et l'assurance des conséquences pour une entreprise. Il recommande aussi des sanctions pour les entreprises qui procèdent au paiement des rançons, que ce soit directement ou par l'intermédiaire d'un

tiers.

Valeria Faure-Muntian recommande de permettre aux assureurs de couvrir et de prendre en charge les amendes administratives. Pour une meilleure comptabilisation des attaques cyber par les forces de l'ordre, elle suggère de lier l'activation des garanties de cyber-assurance à un dépôt de plainte auprès des services compétents.

1.3.2 Loi DORA

Dans la continuité du rapport de Mme Faure-Muntian, le 16 janvier 2023, la Commission Européenne vote le règlement DORA (Digital Operational Resilience Act) et la directive associée qui visent à combattre les risques liés à la transformation numérique des services financiers et la multiplication des cyberattaques. Il s'agit d'une initiative de la Commission européenne pour favoriser l'innovation et l'adoption de nouvelles technologies tout en assurant la stabilité financière et la protection des consommateurs.

DORA propose un cadre réglementaire pour la résilience opérationnelle numérique, obligeant les entités financières à garantir leur capacité à résister, répondre et se rétablir face à toute perturbation grave liée aux technologies de l'information et de la communication (TIC). Plutôt que de simplement prévenir les risques, cette approche plus large et pro-active exige une préparation aux incidents et une assurance de la continuité des activités et services critiques.

Le règlement DORA concerne un large éventail d'entités financières et de prestataires de services TIC qui opèrent au sein de l'Union européenne. Il entrera en vigueur dans tous les États membres de l'UE à partir du 17 janvier 2025.

Le règlement DORA comprend cinq piliers clés de la résilience opérationnelle numérique que les institutions financières doivent mettre en œuvre :

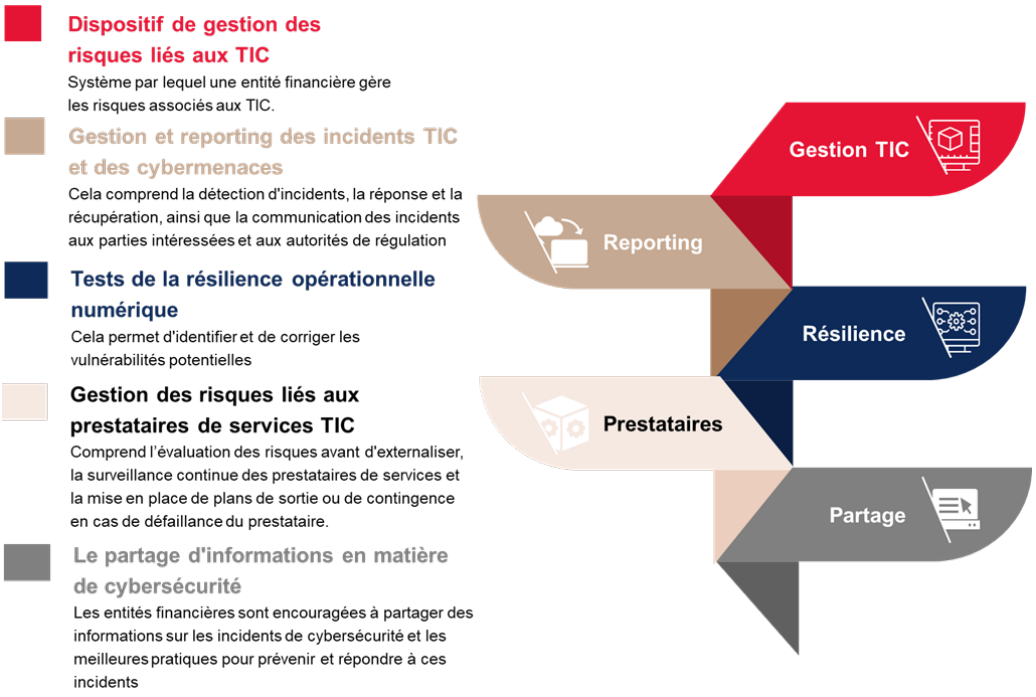

FIGURE 1.11 : Les différents points de la loi DORA

1.3.3 Loi LOPMI

De plus, le 7 décembre 2022 a marqué une étape importante dans la lutte contre la cybercriminalité avec l'adoption par le gouvernement de la loi LOPMI (Loi d'Orientation et de Programmation du ministère de l'Intérieur). Cette loi intervient à un moment où les cyber-attaques sont en pleine expansion, touchant 54% des entreprises.

La loi LOPMI comporte deux dispositions clés qui ont un impact direct sur l'assurance cyber. D'abord, l'article 4, qui vise à réglementer les clauses d'indemnisation des rançons cyber par les compagnies d'assurance. Ensuite, l'article 5 impose aux entreprises de signaler une cyber-attaque dans un délai de 72 heures après en avoir pris connaissance.

Cela est particulièrement pertinent dans le contexte actuel, comme le démontre une étude du CESIN, où la majorité des entreprises tendent à signaler plusieurs incidents à la fois. Ce phénomène peut entraîner une distorsion des données et par conséquent rendre les modèles de provisionnement moins précis : avec la loi LOPMI en vigueur les entreprises auront alors un devoir de déclaration des sinistres ce qui rendra les bases de données plus pertinentes vis-à-vis de leur fréquence de sinistre.

1.3.4 Règlement Général de la Protection des Données (RGPD)

Parallèlement à la future loi LOPMI, les entreprises doivent se conformer au Règlement Général sur la Protection des Données (RGPD). Le RGPD est un règlement qui établit des normes strictes pour la collecte, l'utilisation, la gestion, la protection et le partage des données personnelles par les organisations. Les amendes pour non-conformité au RGPD peuvent atteindre jusqu'à 20 millions d'euros ou 4% du revenu annuel global d'un groupe. Les entreprises doivent se conformer au RGPD

en prouvant leur conformité, en accordant aux individus des droits liés à leurs données personnelles et en prenant en compte les risques liés à la protection de la vie privée dans la conception de leurs produits ou services. Les conséquences d'une violation du RGPD pour une entreprise comprennent des coûts financiers, des interruptions d'activité, des demandes d'indemnisation civile et des dommages à la réputation. Les entreprises doivent prendre des mesures telles que réaliser des audits de sécurité fréquents, développer des plans de conformité des données, veiller à ce que les sous-traitants respectent les normes du RGPD et mettre en place des procédures de notification des violations de données.

Ainsi, l'assurance cyber peut être utile pour réduire les coûts liés à une violation de données en couvrant les dépenses liées à la gestion de crise mais peut également être utile à la remise en ligne des systèmes défaillants, à l'intervention d'experts et à la représentation juridique en cas de réclamations civiles.

Cependant, il y a des limites à l'assurance cyber en ce qui concerne les amendes prononcées par les autorités de contrôle dans le cadre du RGPD. Les amendes réglementaires peuvent ne pas être couvertes par l'assurance, car elles sont considérées comme des conséquences pénales et non recouvrables en droit. De plus, l'assurance ne couvrira pas les pertes de revenus résultant de la perte de clients due à une atteinte à la réputation.

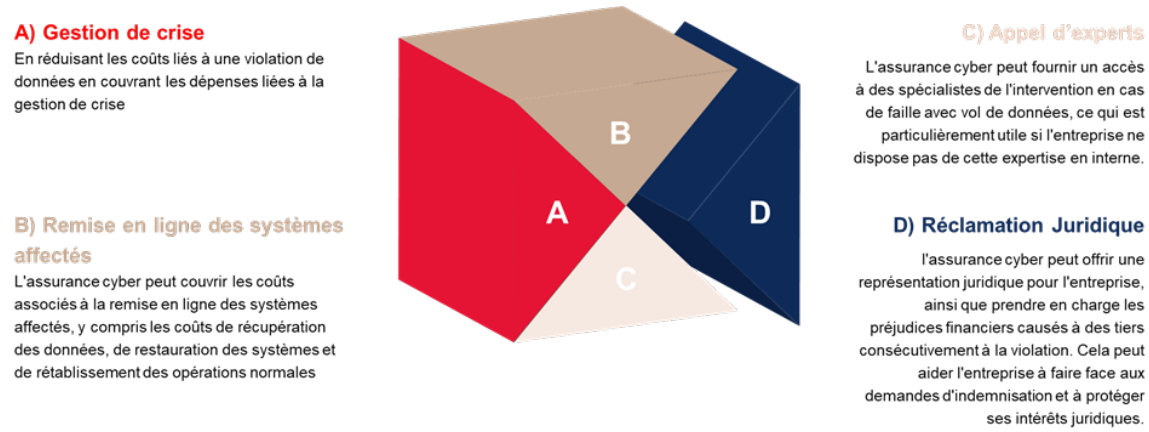

FIGURE 1.12 : Les garanties cyber possibles vis à vis des autorités de contrôle

1.3.5 Autres autorités de contrôle

Enfin, les entreprises doivent se soumettre aux différentes autorités de contrôle qui viennent compléter le RGPD. En effet, l'Agence Française Anti-corruption (AFA), la Commission Nationale de l'Informatique et des Libertés (CNIL), l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), la DGSI (Direction Générale de la Sécurité Intérieure) ou encore l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) peuvent être des acteurs de l'assurance du risque cyber. Que ce soit pour la prévention ou pour infliger des amendes aux compagnies d'assurance ne respectant pas la législation, ces autorités jouent ainsi un rôle clé dans la régulation du risque cyber.

Chapitre 2

Micro-économie de l'assurance cyber

Dans l'écosystème complexe et interconnecté de l'assurance cyber, la compréhension et la modélisation du risque cyber constituent des défis majeurs pour les assureurs et les participants au marché. L'exposition au risque cyber n'est pas seulement un phénomène isolé affectant les entités de manière indépendante, mais elle est également influencée par le comportement interdépendant des différents acteurs au sein de ce réseau. Cette dynamique, caractérisée par des objectifs potentiellement divergents et des interactions entre les acteurs, souligne l'importance d'une approche systémique pour évaluer et gérer le risque cyber.

Le risque cyber est ainsi particulièrement adapté à une analyse par la théorie des jeux, qui permet d'examiner les interactions stratégiques et les décisions interdépendantes des différents acteurs. En effet, elle offre un cadre d'analyse robuste pour modéliser les comportements et les choix stratégiques des acteurs, en prenant en compte leur influence mutuelle sur l'exposition au risque et les décisions de protection ou d'assurance. Le modèle Awiszus et al. (2023) se distingue dans ce contexte en appliquant les principes de la micro-économie et de la théorie des jeux pour élaborer un modèle de tarification de l'assurance cyber. Ce modèle permet de proposer un problème d'optimisation de prime d'assurance qui tient compte des interactions complexes entre les différents acteurs pour tarifer le risque.

Cette introduction examine les approches micro-économiques appliquées à l'étude du risque et de l'assurance cyber, en s'appuyant sur une revue de littérature et une introduction mathématique succincte aux modèles considérés. Nous nous référerons notamment aux travaux de Marotta et al. (2017) pour adopter une notation cohérente dans l'analyse des modèles. Cette discussion préliminaire permettra de jeter les bases pour évaluer l'efficacité et la pertinence des modèles de tarification dans le contexte spécifique du risque cyber, en mettant en lumière les interactions complexes et les interdépendances au sein de l'assurance cyber.

Initialement, nous établirons les principes fondamentaux de la micro-économie appliqués au domaine de l'assurance. Ensuite, nous distinguerons les notions de risque et d'incertitude, tout en examinant comment le risque est modélisé en micro-économie. Par la suite, nous examinerons les caractéristiques des participants dans le secteur de l'assurance cyber. Enfin, nous étudierons leur comportement vis-à-vis du risque.

2.1 Définitions et principes de base en assurance

2.1.1 Offre et demande

Dans le domaine de l'assurance, comme dans de nombreux autres secteurs, les principes de la micro-économie jouent un rôle fondamental. Au cœur de ces principes se trouvent les concepts d'offre et de demande, qui déterminent la dynamique du marché. La **valeur de réserve** est un élément clé dans cette dynamique, représentant le prix maximal qu'un consommateur est prêt à payer pour un bien ou service, ou le prix minimal auquel un producteur est disposé à vendre. Dans le secteur de l'assurance, cela peut se traduire par le montant maximal qu'un individu est prêt à payer pour une police d'assurance, ou par le montant minimum pour lequel une compagnie d'assurance est disposée à offrir cette couverture. Pour quantifier la satisfaction qu'entraîne la signature d'un contrat d'assurance par un assuré, il nous faut introduire la notion d'utilité. C'est cette notion d'utilité qui permet d'expliquer comment les consommateurs évaluent les avantages de différentes polices d'assurance et décident de celle qui offre le meilleur équilibre entre coût et couverture. En fin de compte, c'est l'utilité perçue qui guide les choix des assurés, les amenant à opter pour des décisions qui maximisent leur satisfaction dans un contexte d'incertitude et de risque.

2.1.2 Équilibre du consommateur

Dans le contexte de l'assurance, l'équilibre des consommateurs est lié à leur utilité, spécifiquement évaluée par les **fonctions d'utilité conditionnelles**, communément appelées simplement fonctions d'utilité. Elles évaluent la satisfaction ou le bien-être que les individus tirent de leur consommation sous différentes conditions ou états possibles. Il est essentiel de préciser que, en assurance, lorsque nous parlons de fonctions d'utilité, nous faisons référence aux fonctions d'utilité conditionnelles.

Nous pouvons également introduire les **fonctions d'utilité marginales** associées à ces fonctions d'utilité. Les fonctions d'utilité marginales font référence au changement dans l'utilité qu'un individu obtient en consommant une unité supplémentaire d'un bien ou service. En assurance, cela se traduit par la valeur supplémentaire perçue par l'assuré pour chaque augmentation unitaire de la couverture d'assurance. Elles sont calculées en dérivant la fonction d'utilité associée.

Dans les problèmes de tarification en assurance, ces deux fonctions jouent un rôle important. Les individus et les compagnies d'assurance cherchent à maximiser l'utilité à travers l'achat et la vente de polices d'assurance. L'assuré utilise la fonction d'utilité conditionnelle pour évaluer les politiques d'assurance des différents scénarios de risque, choisissant la quantité de couverture qui maximise son utilité compte tenu des risques encourus. La fonction d'utilité marginale aide à comprendre comment l'utilité de l'assurance change avec des niveaux de couverture supplémentaires. Les assureurs, quant à eux, les utilisent pour fixer des primes qui attirent les assurés tout en garantissant la rentabilité, comme par exemple, en se fixant un objectif de ratio Sinistres / Primes inférieur à 100%. Le problème d'optimisation consiste donc à trouver un équilibre entre le coût de la prime et l'utilité perçue de la couverture.

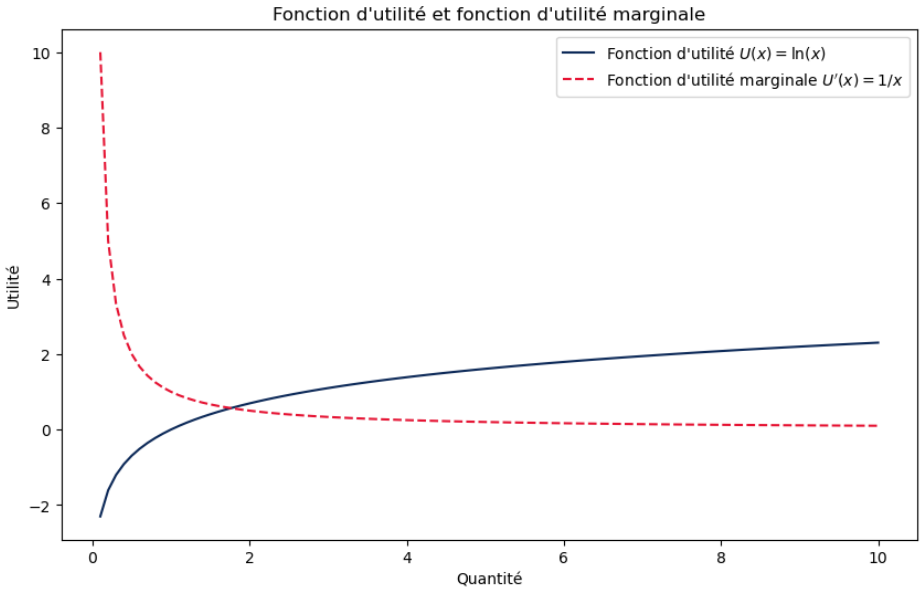

FIGURE 2.1 : Une fonction d'utilité quelconque et sa fonction d'utilité marginale associée

2.2 Risque et incertitude

La distinction entre **risque et incertitude** est importante pour l'étude microéconomique de l'assurance. Comme le souligne Jokung-Nguéna (2001), l'incertitude peut être classée en deux catégories : mesurable et non mesurable. Lorsque nous pouvons mesurer l'incertitude, c'est-à-dire, lorsque les probabilités associées à différents événements sont connues ou peuvent être estimées, nous parlons alors de *risque*. Cette situation permet d'adopter une démarche méthodique dans la prise de décision, en se basant sur des calculs précis. À l'inverse, nous faisons face à une *incertitude non mesurable* lorsque les probabilités des événements ne peuvent être déterminées, complexifiant ainsi significativement le processus décisionnel.

2.2.1 Modélisation du risque en micro-économie

La **fonction d'utilité espérée** joue un rôle important dans le contexte de risque et d'incertitude en assurance. Elle permet aux individus et aux compagnies d'assurance d'évaluer les différentes stratégies de tarification et les niveaux de couverture, en tenant compte à la fois des probabilités des divers événements et de l'utilité associée à leurs résultats possibles. Cette approche aide les assurés à décider de la quantité de couverture à acheter et les assureurs à déterminer les primes à appliquer pour différents niveaux de risque, en cherchant à maximiser l'utilité espérée dans un environnement incertain.

2.2.2 L'axiomatique de von Neumann et Morgenstern

Les axiomes de von Neumann et Morgenstern sont à la base de la théorie de l'utilité attendue, qui est un cadre conceptuel utilisé pour modéliser la prise de décision en situation d'incertitude. Ces axiomes permettent de définir mathématiquement la notion d'utilité d'un individu de manière cohérente avec ses préférences. Les axiomes utilisent la notion de "loterie", qui représente un choix sous incertitude

où chaque option est associée à des probabilités spécifiques de résultats différents. Voici les axiomes principaux :

1. **Comparabilité** : Pour tous les événements A et B, un individu peut toujours dire s'il préfère A à B, B à A, ou est indifférent entre A et B. En d'autres termes, toutes les paires d'événements peuvent être comparées.
2. **Transitivité** : Si un individu préfère A à B et B à C, alors il préfère A à C. Si l'individu est indifférent entre A et B, et entre B et C, alors il est également indifférent entre A et C.
3. **Indépendance (ou substituabilité)** : Si un individu préfère A à B, il préfère également une loterie qui offre A avec une probabilité p et C avec une probabilité $(1-p)$ à une loterie qui offre B avec une probabilité p et C avec la même probabilité $(1-p)$, et ce pour tout C. En d'autres termes, l'attitude d'un individu face aux deux loteries ne devra dépendre que de son attitude face à A et B et non pas la façon d'obtenir A et B.
4. **Continuité** : Si un individu préfère A à B et B à C, alors il existe une probabilité p telle que l'individu est indifférent entre B et une loterie qui offre A avec une probabilité p et C avec une probabilité $(1-p)$.

Ces axiomes ont été établis pour formaliser l'idée que les décisions économiques peuvent être représentées comme des choix entre différentes "loteries", ou distributions de probabilité sur un ensemble d'issues. Ils permettent de définir une fonction d'utilité représentant les préférences d'un individu sur un ensemble de loteries, de manière à ce que ses choix maximisent l'utilité attendue.

2.3 Profils des acteurs de l'assurance cyber

Dans l'analyse du risque cyber, la théorie des jeux met souvent l'accent sur l'autoprotection des acteurs interdépendants, en présence ou en absence d'assurance cyber. Une question centrale réside dans les conditions sous lesquelles l'assurance cyber incite à l'autoprotection et contribue à améliorer la sécurité informatique globale. Cette section aborde les idées principales et les caractéristiques de tels modèles, en distinguant trois types d'acteurs stratégiques aux objectifs variés : les acheteurs potentiels d'assurance (nommés agents pour simplifier), les compagnies d'assurance, et le régulateur. Cette classification émane directement de la contribution de Awiszus et al. (2023), fournissant ainsi un cadre structuré pour l'étude de l'interaction entre les différentes parties prenantes de l'assurance cyber.

2.3.1 Agents

Ces acteurs sont les détenteurs potentiels de polices d'assurance cyber. Pour refléter l'interdépendance, il est courant de modéliser les agents comme formant un réseau. Chaque agent vise à maximiser son utilité attendue, exprimée par la fonction d'utilité U_i qui suit généralement les axiomes classiques de von Neumann-Morgenstern (cf. 1.4.2) :

$$\max \mathbb{E}[U_i(W_i)] \text{ où } \begin{cases} U_i & \text{est la fonction d'utilité de l'individu } i, \\ W_i & \text{est la richesse de l'individu } i. \end{cases}$$

Il est possible de représenter la situation d'un agent sans assurance par un arbre et ainsi étudier sa richesse en cas de survenance d'un sinistre ou non. Pour cela, nous définissons la probabilité que le

sinistre cyber se réalise, notée p_i, le coût potentiel associé à ce sinistre pour l'assuré, indiqué par L_i, ainsi que le budget alloué à la cybersécurité C_i. W_i^0 correspond à la richesse initiale de l'agent i

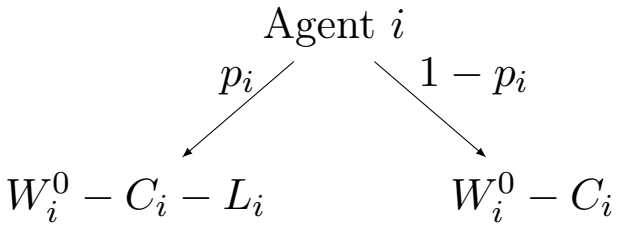

FIGURE 2.2 : Arbre représentant le risque de l'agent i sans assurance.

Retour sur la probabilité d'incidence du risque : Awiszus et al. (2023) apporte des précisions sur la probabilité d'incidence d'un sinistre cyber p_i. La probabilité p_i dépend d'un niveau d'autoprotection x_i qui est une fonction de C_i, budget alloué à la cybersécurité. Ce niveau d'autoprotection x_i est alors soumis à interprétation. Selon Awiszus et al. (2023), le niveau d'autoprotection x_i de l'agent i peut être ainsi assimilé soit à un état binaire de sécurité (sécurisé ou non), soit un spectre palliatif de niveaux de sécurité.

2.3.2 Compagnies d'assurance

Les compagnies d'assurance établissent les montants des primes cyber π_i ainsi que des couvertures X_i. La détermination de ces primes est fortement influencée par la structure du marché d'assurance, qui peut se diviser en plusieurs catégories :

- **Marché compétitif** : Les assureurs tendent à fixer leurs marges vers zéro, ce qui permet aux clients de bénéficier de primes correspondant de manière équitable aux risques couverts. Cependant, cette pratique peut conduire à terme à la faillite des compagnies d'assurance.
- **Marché monopolistique ou assureur représentatif** : Cette situation examine l'impact d'un acteur seul et donc dominant sur le marché. L'assureur peut viser des objectifs autres que la maximisation du profit, notamment pour encourager un niveau spécifique de sécurité informatique dans un contexte réglementé.
- **Marché immature ou oligopole** : Dans ce contexte, on observe une concurrence imparfaite avec plusieurs assureurs qui réalisent des profits. L'écart entre le prix équitable et la prime d'assurance est déterminé par la structure du marché.

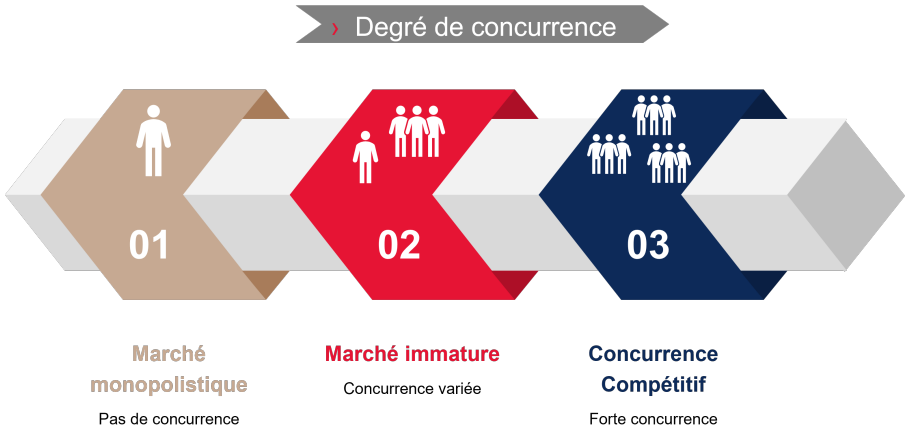

FIGURE 2.3 : Les différents types de marchés

Dans la suite de notre étude, nous considérerons que le marché de l'assurance cyber peut être assimilé à un **marché immature**. Ceci est dû au fait que le marché est encore étroit et instable, comme mentionné dans la section 1.2, et que le cadre législatif reste incomplet, comme discuté dans la section 1.3. Cette analyse s'aligne sur les observations faites par Deblock (2022), où le marché est décrit comme étant instable et immature, marqué par des prix volatils, des critères de souscription changeants, et une couverture limitée pour les petites entreprises.

La modélisation du risque pour un assuré, désigné par l'agent i, prend en compte à la fois la prime d'assurance π_i et la couverture X_i, comme illustré par l'arbre suivant. Cet arbre détaille la richesse de l'agent i en cas de survenance ou non d'un sinistre de coût L_i, incluant le coût de la prime, l'avantage de la couverture d'assurance et le coût de l'autoprotection C_i.

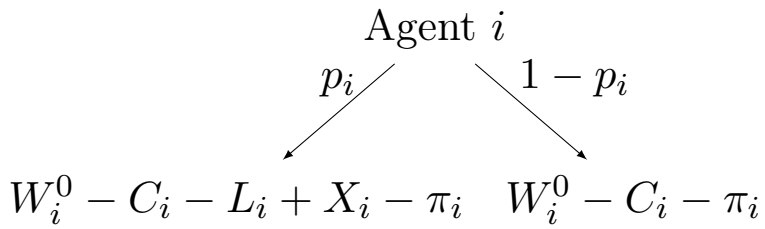

FIGURE 2.4 : Arbre représentant le risque de l'agent i avec assurance.

De façon similaire, on peut représenter les gains potentiels pour l'assureur qui couvre l'agent i, illustrant les résultats financiers en fonction de la réalisation ou non du sinistre. Cet arbre de décision permet de comprendre comment les primes perçues et les potentiels paiements d'indemnisation influencent les gains de l'assureur.

2.3.3 Régulateur

Les inefficacités du marché et les lacunes en matière de cybersécurité peuvent être atténuées par des politiques réglementaires, incluant des assurances obligatoires, des amendes, des remises, ou des responsabilités en cas de contagion. Le régulateur, visant à maximiser une fonction de bien-être social, peut influencer le marché en adoptant des politiques qui modulent les comportements des agents et

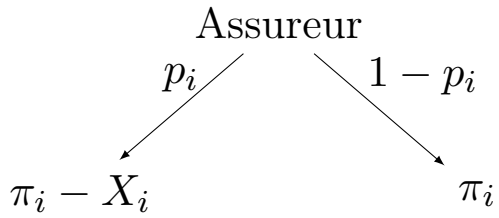

FIGURE 2.5 : Arbre représentant le gain de l'assureur assurant l'agent i.

des assureurs en faveur d'une meilleure sécurité IT globale. Par exemple, le régulateur, dans le marché français de l'assurance cyber peut être assimilé au RGPD (cf 1.3).

Cette structure à trois acteurs permet d'explorer la dynamique complexe du marché de l'assurance cyber, en analysant comment les politiques d'assurance et les niveaux de protection individuels interagissent au sein d'un écosystème interconnecté, avec pour objectif d'améliorer la résilience face aux risques cyber.

2.4 L'attitude face au risque

L'attitude des acteurs vis à vis du risque est importante car elle influence directement la valeur perçue de l'assurance par les clients et par l'assureur. En examinant comment les acteurs du marché de l'assurance cyber réagissent face au risque, nous serons en mesure de définir des fonctions d'utilité adéquates pour aborder notre problème d'optimisation. Pour analyser l'attitude des acteurs face au risque, il est essentiel de commencer par définir ce qu'est l'aversion au risque. Ensuite, nous explorerons comment cette aversion influence les caractéristiques des fonctions d'utilité. Nous passerons en revue diverses fonctions d'utilité couramment utilisées dans le secteur de l'assurance, avant de spécifier comment ces concepts s'appliquent au contexte particulier du risque cyber.

2.4.1 Aversion au risque

À travers les fonctions d'utilité, qui mesurent la satisfaction relative à différents niveaux de richesse, l'aversion au risque reflète la préférence des individus pour la certitude plutôt que pour l'incertitude. Les assureurs utilisent ce concept pour déterminer comment les assurés évaluent le transfert du risque à l'assureur contre le paiement d'une prime. En comprenant le degré d'aversion au risque de leurs assurés, les assureurs peuvent moduler des produits qui offrent une protection adéquate tout en étant attractifs et financièrement justifiables pour les assurés.

Selon Jokung-Nguéna (2001), l'aversion au risque se décrit de la sorte : considérons un agent i possédant une richesse initiale égale à W_i^0 et faisant face à un choix incertain, souvent appelé "loterie" en économie, noté $\tilde{x}$. L'individu est alors confronté à un choix entre deux options : l'option risquée, $W_i^0 + \tilde{x}$, notée $\tilde{W_f}$, qui est soumise au risque en raison de sa dépendance à l'issue de la loterie, ou opter pour la valeur espérée de cette richesse finale, $\mathbb{E}(W_i^0 + \tilde{x})$, notée $\mathbb{E}(\tilde{W_f})$, qui représente une option sûre. Ce dilemme illustre clairement l'attitude de l'individu vis-à-vis du risque :

- s'il préfère $\mathbb{E}(\tilde{W_f})$ à $\tilde{W_f}$, il sera alors réputé averse au risque (ou risquophobe)
- s'il préfère $\tilde{W_f}$ à $\mathbb{E}(\tilde{W_f})$, il sera alors réputé risquophile

- s'il est indifférent entre $\tilde{W_f}$ et $\mathbb{E}(\tilde{W_f})$, alors il sera considéré comme neutre vis-à-vis du risque

En d'autres termes, l'attitude d'un individu face au risque se détermine par son choix entre garder sa richesse finale incertaine, $\tilde{W_f}$, ou opter pour une valeur fixe, $\mathbb{E}(\tilde{W_f})$. En préférant la certitude, il révèle une aversion au risque ; s'il choisit l'incertitude, il montre une préférence pour le risque ; et s'il est indifférent, sa position est neutre envers le risque.

Exemple : Pour illustrer le concept d'aversion au risque de manière simple, considérons l'exemple suivant d'un individu, nommé A, qui doit décider comment investir 1000 €. A se voit proposer deux options :

1. **Option sûre** : Placer l'argent dans un compte d'épargne avec un taux d'intérêt garanti de 2.5%. À la fin de l'année, A aurait $1000 \times (1 + 0.025) = 1025$ €, garantissant ainsi un gain sûr de 25 €.
2. **Option risquée** : Investir l'argent dans des actions, avec une chance de 50% de gagner 40% (ce qui augmenterait son investissement à 1400 €) et une chance de 50% de perdre 35% (ce qui réduirait son investissement à 650 €). L'espérance mathématique de cette option est calculée comme suit : $\mathbb{E}(\tilde{W_f}) = 0.5 \times 1400 + 0.5 \times 650 = 1025$ €.

Malgré l'espérance de gain identique de 1025 € pour les deux options, un individu averse au risque comme A préférerait l'option sûre et accepterait le gain garanti de 25 €, évitant ainsi le risque de perdre de l'argent avec l'option risquée. Ceci démontre une préférence pour la certitude et une aversion au risque.

À l'inverse, un individu risquophile pourrait préférer l'option risquée, attiré par la possibilité de gagner 400 €, même si cela comporte un risque élevé de perdre une partie significative de l'investissement initial. Enfin, quelqu'un de neutre vis-à-vis du risque serait indifférent entre les deux options.

Cet exemple simple illustre comment l'aversion au risque influence les décisions financières et pourquoi les assureurs doivent comprendre ces profils des assurés pour proposer des primes d'assurance en raccord avec l'utilité des assurés.

2.4.2 Propriétés des fonctions d'utilité vis-à-vis de l'aversion face au risque

Les trois attitudes citées plus haut peuvent se traduire à l'aide de l'attitude de l'agent i via sa fonction d'utilité (notée U_i)

- $\mathbb{E}(\tilde{W_f})$ sera préféré à $\tilde{W_f}$ si et seulement si $\mathbb{E}(U_i(\tilde{W_f})) < U_i(\mathbb{E}(\tilde{W_f}))$
- $\tilde{W_f}$ sera préféré à $\mathbb{E}(\tilde{W_f})$ si et seulement si $\mathbb{E}(U_i(\tilde{W_f})) > U_i(\mathbb{E}(\tilde{W_f}))$
- $\mathbb{E}(\tilde{W_f})$ sera équivalent à $\tilde{W_f}$ si et seulement si $\mathbb{E}(U_i(\tilde{W_f})) = U_i(\mathbb{E}(\tilde{W_f}))$

Le lien entre l'attitude face au risque et les mathématiques s'établit via la fonction d'utilité, traduisant les préférences de risque d'un agent en termes mathématiques. Le Théorème de Jensen, en explorant les propriétés des fonctions convexes et concaves, clarifie pourquoi une fonction d'utilité concave reflète une aversion au risque, illustrant mathématiquement les comportements face à l'incertitude.

Théorème de Jensen : Soit $f : [a, b] \to \mathbb{R}$ une fonction intégrable et $\varphi : \mathbb{R} \to \mathbb{R}$ une fonction convexe. Alors, le théorème de Jensen pour les intégrales s'énonce comme suit :

$$\varphi\left(\frac{1}{b-a}\int_a^b f(x)\,dx\right) \leq \frac{1}{b-a}\int_a^b \varphi(f(x))\,dx$$

où l'intégrale de f est prise sur l'intervalle $[a, b]$, et $\frac{1}{b-a}$ est le facteur de normalisation pour la moyenne de f sur cet intervalle.

Cela permet de faire le lien entre l'attitude des individus face au risque et la forme de la fonction d'utilité de l'agent i. Ainsi, l'agent i peut être caractérisé comme suit :

- Averse au risque si et seulement si sa fonction d'utilité est concave ;
- Risquophile si et seulement si sa fonction d'utilité est convexe ;
- Neutre au risque si et seulement si sa fonction d'utilité est linéaire.

Nous pouvons ainsi résumer, l'attitude des acteurs de l'assurance suivant le tableau 1.1 :

TABLE 2.1 : L'aversion au risque et ses conséquences

Aversion au risque	**Neutralité au risque**	**Prise de risque**
$\mathbb{E}[U_i(\tilde{W}_f)] < U_i(\mathbb{E}[\tilde{W}_f])$	$\mathbb{E}[U_i(\tilde{W}_f)] = U_i(\mathbb{E}[\tilde{W}_f])$	$\mathbb{E}[U_i(\tilde{W}_f)] > U_i(\mathbb{E}[\tilde{W}_f])$
$\mathbb{E}[\tilde{W}_f]$ est préféré à $\tilde{W}_f$	$\mathbb{E}[\tilde{W}_f]$ est équivalent à $\tilde{W}_f$	$\tilde{W}_f$ est préféré à $\mathbb{E}[\tilde{W}_f]$
U_i concave	U_i linéaire	U_i convexe

2.4.3 Les fonctions d'utilités usuelles applicables au risque cyber

Il existe plusieurs types de fonctions d'utilité en micro-économie. Selon Duguet (n.d.), les fonctions d'utilités usuelles applicables au domaine de l'assurance se distinguent en deux familles de fonctions d'utilité :

- *Constant Relative Risk Aversion* (ou fonctions d'utilité **CRRA**)
  Les fonctions CRRA caractérisent une aversion au risque qui s'ajuste proportionnellement à la richesse de l'individu. Elles sont exprimées par :

$$U(x) = \frac{x^\alpha}{\alpha},\ \alpha \neq 0 \tag{2.1}$$

  Avec $\rho = 1 - \alpha$ représentant le coefficient d'aversion relative au risque.

  Remarque : Si $\alpha \to 0$, on a $U(x) = log(x)$

- *Constant Absolute Risk Aversion* (ou fonctions d'utilité **CARA**)
  Les fonctions CARA modélisent une aversion au risque constante, indépendante du niveau de richesse de l'individu, via l'équation :

$$U(x) = -\frac{1}{\alpha}e^{-\alpha x},\ \alpha > 0 \tag{2.2}$$

Où α est le coefficient d'aversion absolue au risque. Cette caractéristique rend les fonctions CARA idéales pour des contextes où l'impact du risque ne dépend pas des ressources financières disponibles.

2.4.4 Conditions d'optimalité des fonctions d'utilité pour un contrat d'assurance

Pour la suite de notre étude, et en conformité avec les conclusions de Duguet (n.d.), nous nous concentrerons uniquement sur les cas où l'entreprise démontre une aversion au risque. Cette orientation est corroborée par Eling & Schimt (2012) et repose sur des fondements mathématiques présentés dans Duguet (n.d.), soulignant ainsi l'importance et la pertinence de cette hypothèse dans notre contexte d'analyse. En effet, si l'entreprise n'est pas averse au risque, il est impossible de lui proposer une assurance car cette dernière ne prendra que l'option plus risquée, c'est à dire sans assurance. Il s'agira néanmoins de comprendre le degré d'aversion au risque de l'entreprise assurée (si son profil est très averse au risque et évite tout type de risque, ou alors un profil averse au risque se rapprochant de neutre vis à vis du risque)

Ainsi, par 1.4.2, la fonction d'utilité de l'agent i est concave. Cette condition implique au paramètre α de se trouver dans les ensembles de définition suivants :

Fonction CRRA	Fonction CARA
$\alpha < 1$	$\alpha > 0$

TABLE 2.2 : Conditions sur le coefficient α

En prenant en compte ces conditions, nous pouvons alors réaliser des tests de sensibilité. Nous traçons les courbes associées aux fonction d'utilité CRRA et CARA pour différentes valeurs de α :

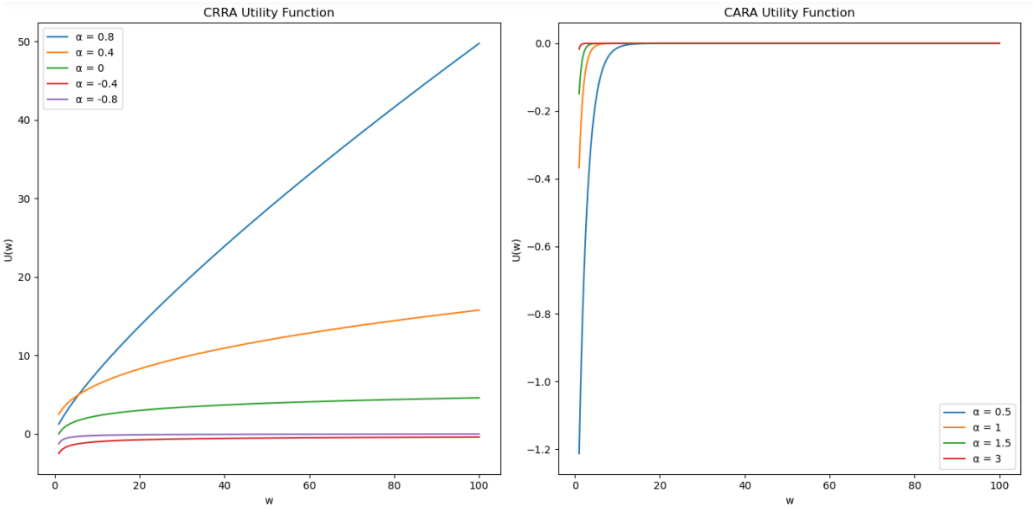

FIGURE 2.6 : Les courbes des fonctions d'utilités CARA et CRRA pour différentes valeurs de α

On remarque que, pour les fonctions CRRA, pour les valeurs de $\alpha < 0.5$, la fonction semble

converger. De plus, plus la valeur de α est faible, plus la convergence est rapide. Lorsque $\alpha \to 1$, la fonction d'utilité semble linéaire.

Pour les fonctions CARA, plus la valeur de α est grande, plus la fonction converge rapidement (vers 0).

Chapitre 3

Études de bases de données cyber

L'un des enjeux majeurs dans la modélisation des risques cyber réside dans la qualité des données exploitées. La rareté et parfois le peu de précision des données disponibles exercent une influence notable sur la qualité des modèles dérivés.

Ainsi, pour la tarification des risques cyber, choisir une base de données appropriée est important pour assurer la cohérence et la pertinence des informations recueillies. Ces bases doivent non seulement être exhaustives mais aussi suffisamment étendues pour permettre l'élaboration de modèles robustes et fiables.

3.1 Les bases de données PRC et VERIS

Nous commençons par étudier les bases de données PRC (*Privacy Rights Clearinghouse*) et VERIS (*Vocabulary for Event Recording and Incident Sharing*), des bases de données américaines référençant les attaques cyber. Nous cherchons ainsi à acquérir une compréhension la plus complète possible des entreprises, incluant des informations telles que la taille des entreprises, leurs secteurs financiers, et leur exposition aux risques. Ces détails sont indispensables pour les utiliser comme variables dans un outil de tarification décrit précédemment. Chaque base offre une méthode unique de collecte et de traitement des incidents de sécurité, fournissant des perspectives variées et complémentaires qui sont essentielles pour l'évaluation et la tarification précise des risques cyber. Cette démarche nous aidera à identifier les forces et les faiblesses de chaque base, afin de les intégrer efficacement dans nos modèles.

3.1.1 La base de données PRC

La base de données PRC est la plus connue et est la plus populaire pour modéliser le risque cyber. La base est accessible via Privacy Rights. Privacy Rights Clearinghouse est une organisation à but non lucratif établie en 1992, dédiée à la protection de la vie privée des citoyens américains. Elle s'engage à informer le public sur les droits individuels et offre des ressources pour la défense de ces droits. La base de données est alimentée par des agences gouvernementales étasunienne et des pertes de données reportées dans les médias ainsi que par des organisations à but non lucratif.

La base de données PRC se focalise uniquement sur les *Data Breaches*, les violations de données (cf 1.1)

La base de données se décompose à travers les 13 variables principales :

Variable	**Description**
Date_Made_Public	Date à laquelle l'incident a été rendu public.
Company	Nom de l'entreprise concernée.
City	Ville où l'entreprise est basée.
State	État où l'entreprise est basée.
Type_of_breach	Type de violation de données (par exemple, piratage, perte de données).
Type_of_organization	Type d'organisation touchée (par exemple, éducative, entreprise).
Total_Records	Nombre total d'enregistrements concernés par la violation.
Description_of_incident	Description de l'incident.
Information_Source	Source de l'information sur l'incident.
Source_URL	URL de la source d'information (peut être vide).
Year_of_Breach	Année de l'incident.
Latitude	Latitude géographique de l'entreprise.
Longitude	Longitude géographique de l'entreprise.

L'avantage de la base PRC est sa popularité et sa facilité d'accès. En effet, la base PRC a fait l'objet de nombreuses études comme notamment Erling & Loperfido (2017) et est donc largement documentée ce qui en fait un socle solide pour les travaux sur l'assurance cyber.

Analyse de la variable $Type\_of\_breach$

La variable $Type\_of\_breach$ est très intéressante car elle nous permet d'obtenir la proportion de type d'attaque cyber de la base PRC, ce qui va nous permettre de comparer avec la base VERIS pour analyser d'éventuelles similarités. Les types d'attaques dans la base PRC sont référencés selon le tableau suivant :

TABLE 3.2 : Description variable Type of breach

Valeurs	Descriptions
HACK	Piratage à l'aide de logiciels malveillants
PORT	Équipements électroniques (clé usb, téléphone, ...) perdus, volés ou piratés
STAT	Ordinateur fixe perdu, volé ou piraté
INSD	Personne de l'entreprise enfreignant les données intentionnellement
DISC	Divulgation non intentionnelle (mauvais destinataire, ...)
UNKN	Type d'attaque non déterminé
PHYS	Documents papiers perdus/volés
CARD	Fraude à la carte bancaire

On obtient ainsi la proportion d'attaques suivante :

Type d'organisation	Nombre de sinistres
CARD	68
DISC	1 861
HACK	2 533
INSD	606
PHYS	1 733
PORT	1 172
STAT	249
UNKN	793

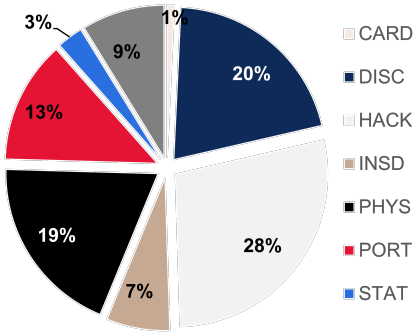

FIGURE 3.1 : Proportion des types d'attaques de la base PRC

On observe ainsi que même si la plupart des violations de données proviennent de logiciels pirates venant de menaces extérieures (**HACK**), une part importante des violations de données provient d'erreurs internes à l'entreprise, comme **DISC**.

Analyse de la variable *Type_of_organization*

La variable *Type_of_organization* nous permet de comprendre les types d'organisations touchées par les attaques cyber et d'en déduire la proportion des organisations attaquées. Leurs différents types sont représentés dans le tableau suivant :

TABLE 3.3 : Description variable Type of organization

Valeurs	Descriptions
EDU	Établissements d'enseignement
BSO	Autres types d'entreprises
MED	Organismes de santé
BSF	Entreprises, services financiers et assurances
BSR	Commerces
GOV	Gouvernement et armée
NGO	Organismes à but non lucratif
UNKN	Type d'entreprise non déterminé

Type d'organisation	Nombre de sinistres
BSF	787
BSO	1 045
BSR	623
EDU	848
GOV	781
MED	4 343
NGO	119
UNKN	469

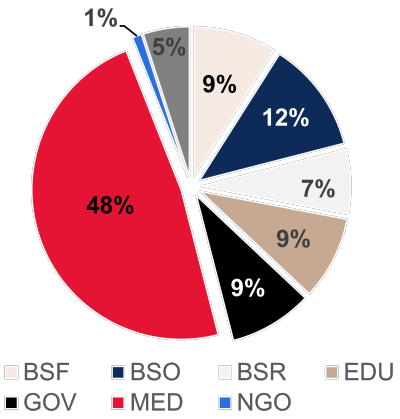

FIGURE 3.2 : Proportion des types d'organismes attaqués de la base PRC

Près de la moitié des organisations touchées et répertoriées dans la base PRC ayant subi des sinistres cyber sont des organismes de santé (**MED**).

3.1.2 Base de données VERIS

La base de données VERIS (Vocabulary for Event Recording and Incident Sharing) est un outil essentiel pour analyser les incidents de sécurité informatique. Elle est accessible via Veris Community. VERIS est une initiative de la communauté qui vise à fournir un langage commun pour la description des incidents de sécurité d'une manière structurée.

La base de données VERIS se concentre sur l'enregistrement détaillé des incidents de sécurité, permettant aux organisations de comprendre les causes et les impacts des violations de sécurité, ainsi que les tactiques utilisées par les attaquants.

La structure de données de VERIS est conçue pour capturer une gamme d'informations sur les incidents de sécurité, telles que :

Variable	Description
Actor	Catégorise l'entité ayant causé l'incident (par exemple, externe, interne, partenaire, multiple).
Action	Méthodes et tactiques utilisées dans l'incident (par exemple, hacking, malware, social).
Asset	Types d'actifs affectés (par exemple, serveur, utilisateur, réseau).
Attribute	Les attributs des informations ou des actifs affectés (par exemple, confidentialité, intégrité).
Impact	Conséquences de l'incident (par exemple, perte de données, interruption de service).
Discovery_Method	Comment l'incident a été découvert.
Timeline	Chronologie de l'incident (par exemple, quand il s'est produit, quand il a été découvert).

VERIS aide les chercheurs et les professionnels de la sécurité à collecter et à analyser des données sur les incidents de manière cohérente, ce qui est important pour développer des stratégies de sécurité

efficaces et pour les recherches académiques en cybersécurité. La base de données VERIS est largement utilisée pour la génération de rapports annuels sur la sécurité et pour les études de cas spécifiques à l'industrie.

Les données collectées par VERIS permettent une analyse globale et détaillée des incidents, rendant cette base de données un outil incontournable pour comprendre les tendances en matière de cybersécurité et pour renforcer les mesures de sécurité informatique.

Nous comptons ainsi 9896 incidents principalement entre 2008 et 2024 (base actualisée en 2024). Ces incidents se sont majoritairement produits aux états-unis en comptant 73% des sinistres et une petite partie provient de Grande Bretagne et du Canada, le reste étant réparti entre les autres pays du monde.

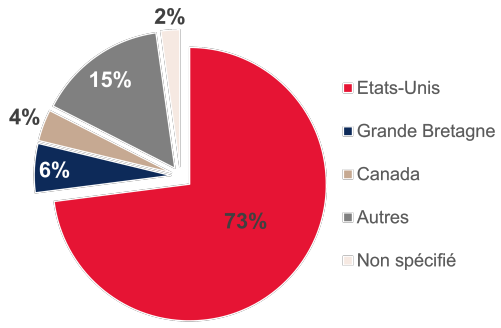

FIGURE 3.3 : Proportion des pays des sinistres de la base VERIS

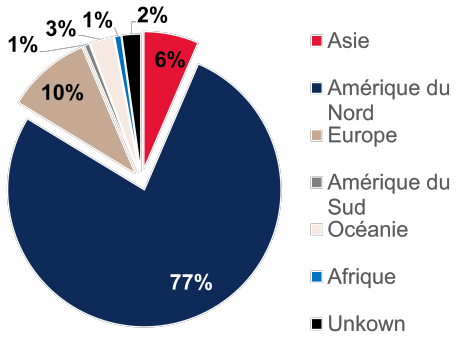

FIGURE 3.4 : Répartition des sinistres VERIS par continent

Les types d'attaques avec la variable *action*

Dans la base de données VERIS, les types d'attaques sont référencés en catégories au sein de la variable *action*. VERIS utilise ainsi 7 catégories pour référencer les types d'attaques :

1. ***Hacking :*** Exploitation des systèmes ou des réseaux par des moyens techniques, comme l'utilisation de vulnérabilités ou l'accès non autorisé via des logiciels malveillants ou des techniques d'intrusion.
2. ***Malware :*** Utilisation de logiciels malveillants tels que virus, chevaux de Troie, ou ransomwares pour compromettre la confidentialité, l'intégrité ou la disponibilité des systèmes ou des données.
3. ***Social :*** Techniques de manipulation humaine comme le phishing, l'ingénierie sociale, ou le prétexte pour inciter les utilisateurs à divulguer des informations sensibles ou à commettre des actions compromettantes.
4. ***Misuse :*** Mauvaise utilisation des privilèges d'accès ou des ressources par des acteurs internes (comme les employés) pour atteindre des objectifs non autorisés, qu'ils soient malveillants ou non intentionnels.
5. ***Physical :*** Actions physiques comme le vol de matériel, l'espionnage physique, ou le sabotage de l'infrastructure matérielle qui compromettent la sécurité des systèmes.

6. ***Error :*** Erreurs humaines involontaires, telles que la mauvaise configuration, la divulgation accidentelle de données, ou l'envoi d'informations à la mauvaise personne, qui entraînent des incidents de sécurité.

7. ***Environmental :*** Incidents causés par des événements naturels ou environnementaux comme les catastrophes naturelles, les pannes de courant, ou les défaillances matérielles dues à des facteurs environnementaux.

Contrairement à la base PRC, une attaque cyber selon VERIS peut faire partie de plusieurs catégories de la variable *action*. Par exemple, une attaque par ransomware qui utilise l'ingénierie sociale pour se propager pourrait être classée selon les catégories suivantes :

- **Malware** : Le ransomware lui-même est un type de logiciel malveillant qui chiffre les fichiers de la victime et exige une rançon pour les déchiffrer.
- **Hacking** : Si le ransomware exploite une vulnérabilité dans le système de la victime pour s'installer ou se propager, cette partie de l'attaque peut être classée comme du hacking. Par exemple, le ransomware pourrait exploiter une faille de sécurité dans un logiciel ou un service de réseau pour s'infiltrer.
- **Social** : Si l'attaque initiale utilise le phishing pour inciter un utilisateur à télécharger le ransomware, cette composante de l'attaque relèverait de l'ingénierie sociale. Par exemple, l'utilisateur pourrait recevoir un email frauduleux l'incitant à cliquer sur un lien ou à ouvrir une pièce jointe infectée.

On peut alors établir les proportions des valeurs de la variables *Action* dans l'ensemble de la base :

Catégories de *action*	Nombre d'occurrences
Hacking	3 238
Malware	1 619
Social	1 373
Misuse	1 788
Physical	1 619
Error	2 676
Environmental	10

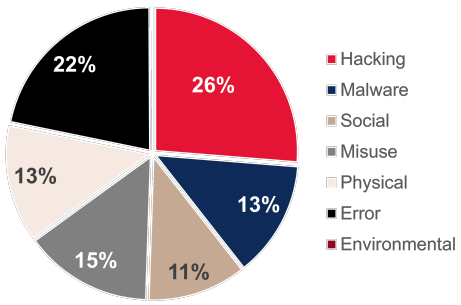

FIGURE 3.5 : Proportion des types d'attaques de la base VERIS

Ainsi la base VERIS présente des attaques cyber variées, chaque type d'attaque est bien représenté avec plus de 1 000 occurrences, sauf la variable *Environmental*.

Les types d'organisations par *victim.industry*

La base VERIS nous renseigne sur le type d'organisation à travers le code NAICS, *The North American Industry Classification System*, qui se présente sous un code composé d'au maximum 6 chiffres. Les

deux premiers nous indiquent le secteur de l'entreprise concernée (par exemple 44-45 pour le commerce de détail). Les chiffres suivants affinent la segmentation de l'entreprise concernée.

Nous pouvons ainsi comparer les proportions des types des organisations touchées avec la base PRC sur la base des deux premiers chiffres NAICS.

Nous utilisons donc la segmentation selon le code NAICS suivante :

Type d'organisation	Code NAICS
EDU	61
MED	62
BSF	52
BSR	44-45
GOV	92
NGO	81
BSO	Autres codes

TABLE 3.5 : Code NAICS pour les différents types d'organisations étudiés

On obtient la proportion de types d'organisations suivante :

Type d'organisation	Nombre de sinistres
BSF	881
BSO	2 420
BSR	469
EDU	1 123
GOV	2 338
MED	2 450
NGO	207

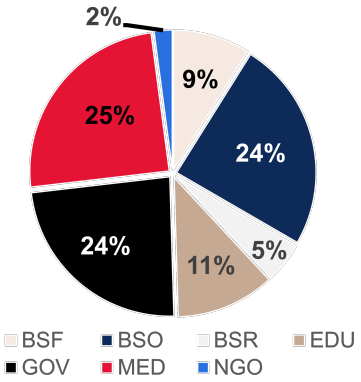

FIGURE 3.6 : Proportion des types d'organismes attaqués de la base VERIS

On remarque que la plupart des organisations touchées sont des entreprises et des organismes de santée et beaucoup sont référencés comme étant hors de la segmentation émise par la base PRC classés alors en BSO.

3.1.3 Comparaison des différentes bases

Comparaison des types de données

Comme mentionné précédemment, la base PRC se concentre principalement sur des sinistres touchant des organisations médicales, tandis que la base VERIS englobe une variété plus large d'organisations, offrant ainsi une perspective plus diversifiée des incidents de cybersécurité. De même pour les types d'attaques où VERIS est une base plus homogène alors que l'on observe une nette dominance des attaques de type **HACK**, **DISC** et **PHYS**, représentant presque 70% de la base PRC.

En termes de détail, la base VERIS est nettement plus riche, avec 175 colonnes de variables contre seulement 13 dans la base PRC. Elle permet ainsi une analyse plus fine des incidents. Enfin, la base VERIS contient environ 10 000 lignes de données, contre 9 000 pour la base PRC, renforçant ainsi sa profondeur analytique.

Comparaison du nombre de sinistres par année

La comparaison entre les temporalités de déclaration de sinistre entre les deux bases présente des disparités (cf graphique ci dessous) : le nombre de sinistres déclarés dans la base PRC est presque constant de 2010 à 2018 pour 800 sinistres par an alors que la base VERIS montre des fortes disparités de déclarations entre les années.

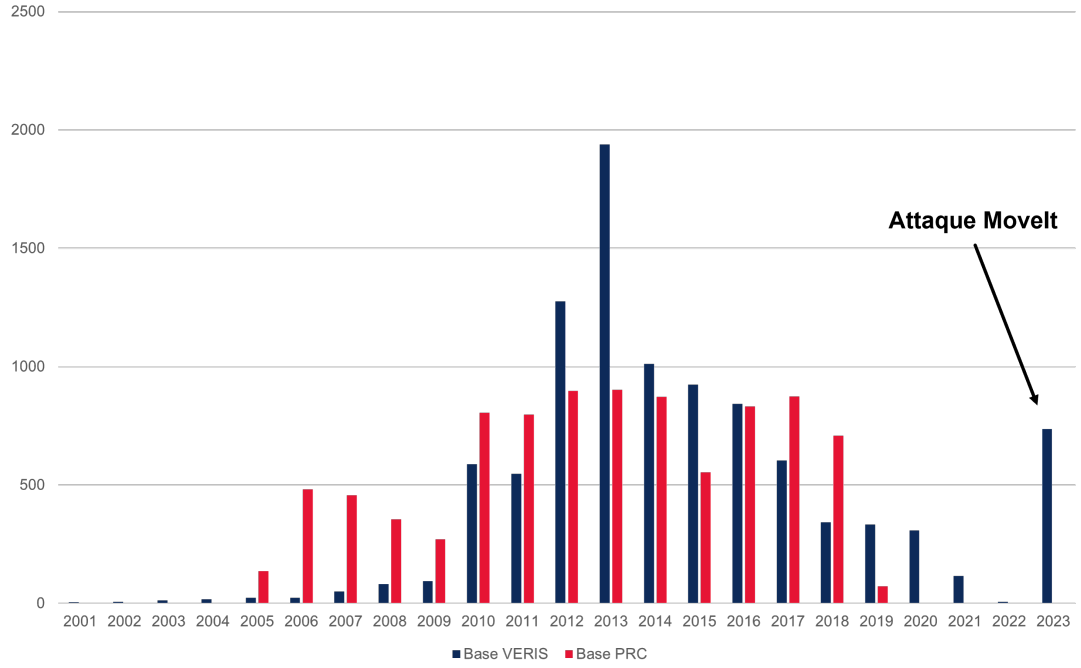

FIGURE 3.7 : Comparaison de la temporalité des sinistres dans les deux bases de données

Ces disparités expliquent les différences dans la répartition des secteurs des organisations touchées, suggérant que les attaques ne sont pas nécessairement les mêmes.

On observe peu de sinistres en 2022, année marquée par un faible nombre d'attaques et un reporting incomplet. La base de données prend du temps pour référencer les sinistres.

Un pic significatif est visible en 2023 pour la base PRC, correspondant à l'attaque MOVEit (voir chapitre 1), comme le souligne la variable **summary** de la base.

Comparaison de la qualité des données

La comparaison des deux bases de données cyber a été réalisée dans le cadre du mémoire de Bastard (2021). Cette comparaison a été réalisée dans le cadre de Solvabilité II et évalue la qualité des deux bases selon les critères principaux suivants :

- **Exhaustivité** : En conformité avec la directive Solvabilité 2, l'exhaustivité concerne l'identification des principaux groupes de risques, une granularité suffisante pour analyser les tendances, et des historiques adéquats.

- **Exactitude** : L'exactitude des données signifie qu'elles doivent être précises et appropriées pour l'usage prévu, telles que la modélisation des risques, et doivent fidèlement représenter les risques auxquels l'assureur est exposé.

- **Pertinence** : Des données pertinentes sont celles sans erreurs majeures ni omissions, avec des informations bien stockées et régulièrement mises à jour, et qui répondent à un niveau de confiance élevé.

FIGURE 3.8 : Comparaison des différentes base selon Bastard (2021)

3.1.4 Problèmes liés à l'utilisation de ces bases

L'utilisation des bases de données PRC et VERIS soulève néanmoins plusieurs problèmes significatifs qui affectent leur fiabilité et leur pertinence.

Pour commencer, la base PRC présente des limitations considérables en termes de mise à jour des données, puisque l'accès libre ne propose des informations que jusqu'en 2019. Cette situation est particulièrement problématique dans un contexte aussi évolutif que l'assurance cyber (cf chapitre I). De plus, la base PRC est affectée par des erreurs de temporalité ; plusieurs incidents ont été signalés bien après leur occurrence réelle, ce qui peut avoir des conséquences sur les modélisations de fréquence.

D'autre part, la base VERIS est moins documentée et se révèle plus complexe à exploiter. Cette complexité et le manque de documentation peuvent rendre son utilisation difficile et contraignante.

De plus, les deux bases ne présentent pas de variable de coût précise. La base PRC ne nous renseigne pas sur les coûts des sinistres et la base VERIS possède une variable présentant le coût de l'attaque, *impact.overall_ amount*, mais cette dernière est très incomplète (seul 323 sinistres possèdent un coût) et très approximative. Elle ne nous permet pas d'effectuer un modèle de sévérité sur l'ensemble de la base.

Enfin, les deux bases sont de conception américaine et reflètent principalement le marché américain. Comme vu dans le chapitre I, la législation américaine étant différente de la législation européenne et française, appliquer ces données au marché français pourrait être sujet à des erreurs. Notre objectif étant de tarifer le risque cyber sur le marché français, il est alors nécessaire de trouver des données françaises spécifiques.

3.2 La base de données LUCY

Chaque année, l'Association pour la Gestion des Risques et des Assurances de l'entreprise (AMRAE (2020 - 2024)) publie une étude intitulée "Lumière sur le cyber" (LUCY) (cf 1.2.1). Cette enquête repose sur des milliers d'entreprises françaises et compile des données liées à la cyber sécurité, notamment les incidents et les pertes financières qui en résultent.

Les rapports LUCY peuvent fournir des données intéressantes à croiser avec la base de données VERIS pour mieux refléter le marché français. Nous allons donc regrouper toutes les données des différents rapports.

3.2.1 Regroupement des données des rapports LUCY

L'AMRAE publie régulièrement des données significatives sur la cybersécurité depuis 2019 à travers un rapport annuel. Dans ce contexte, elle classe les entreprises en différentes catégories en fonction de leur chiffre d'affaires, notamment les "Grandes Entreprises", les "Entreprises Intermédiaires", les "Moyennes Entreprises", les "Petites Entreprises" et les "Micro Entreprises" (qui sont généralement regroupées avec les petites entreprises car leur poids sur le marché de la cyber assurance est peu significatif). De la même manière, elle catégorise les sinistres en fonction de leur coût, allant de "XS et S" pour ceux dont le coût varie de 0€ à 300 000€, à "M et L" pour ceux allant de 300 000€ à 3 millions d'euros, "XL" pour les sinistres de 3 millions d'euros à 10 millions d'euros, et "XXL" pour ceux allant de 10 millions d'euros à 40 millions d'euros.

XS et S	M et L	XL	XXL
0€ - 300K€	300k€ - 3M€	3M€ - 10M€	10M€ - 40M€

TABLE 3.6 : Les différentes catégories de sinistres

Ensuite, elle fournit des données sur les indemnisations globales pour chaque type d'entreprise, ainsi que pour chaque catégorie de sinistre. Cette approche va nous permettre de répartir les indemnisations totales en fonction du nombre d'incidents survenus au cours de l'année.

Les rapports LUCY fournissent également d'autres informations utiles telles que l'effectif total assuré, le taux de primes, le nombre de franchises, la capacité souscrite et les ratios S/P propres aux différentes catégories d'entreprises par année.

Ainsi, par année et par catégorie d'entreprises, nous pouvons regrouper les informations suivantes :

Variable	**Description**
type_entreprise	Catégorie ou type de l'entreprise.
annee	Année de référence des données.
primes	Montant total des primes encaissées par l'entreprise.
capacites_souscrites	Capacité financière souscrite par l'entreprise pour couvrir les risques.
taux_de_primes	Taux des primes par rapport à un certain référentiel ou base de calcul.
effectif_total	Nombre total d'employés au sein de l'entreprise.
effectif_assuré	Nombre d'employés assurés par l'entreprise.
franchises	Montant des franchises dans le cadre des contrats d'assurance.
sin_indemn_tot	Montant total des sinistres indemnisés.
sin_XS_et_S	Nombre de petits sinistres (XS et S).
sin_M_et_L	Nombre de sinistres de taille moyenne (M et L).
sin_XL	Nombre de grands sinistres (XL).
sin_XXL	Nombre de très grands sinistres (XXL).
indemn_tot	Montant total des indemnités versées pour tous les sinistres.
indemn_XS_et_S	Montant des indemnités versées pour les petits sinistres (XS et S).
indemn_M_et_L	Montant des indemnités versées pour les sinistres de taille moyenne (M et L).
indemn_XL	Montant des indemnités versées pour les grands sinistres (XL).
indemn_XXL	Montant des indemnités versées pour les très grands sinistres (XXL).
S/P	Ratio sinistres/primes

TABLE 3.7 : Les différentes variables du rapport LUCY

Type entreprise	GE
Année	2019
Primes	73 118 563
Capacités souscrites	38 085 652
Taux de primes	0,93%
Effectif total	287
Effectif assuré	207
Franchises	3 990 104
Sin indem tot	73
Sin XS et S	62
Sin M et L	7
Sin XL	4
Sin XXL	0
Indemn tot	31 800 000
Indemn XS et S	3 700 000
Indemn M et L	11 500 000
Indemn XL	16 600 000
Indemn XXL	0
S/P	44%

TABLE 3.8 : Exemple pour les Grandes Entreprises en 2019

Hypothèses sur la synthèse de l'AMRAE

Bien que l'AMRAE fournisse des données pertinentes, des lacunes subsistent. Les rapports détaillent davantage les "Grandes Entreprises" et les "Entreprises Intermédiaires", tandis que les données sur les autres catégories, notamment les indemnisations spécifiques pour les "Micro Entreprises", sont incomplètes. Cela s'explique par la prédominance des "Grandes Entreprises", qui représentent plus de 80% du marché de l'assurance cyber en France (cf. 1.2).

Pour combler ces lacunes, nous avons regroupé les données des petites et micro-entreprises. Les rapports de 2021 ne distinguent pas ces catégories, contrairement à ceux de 2023, malgré quelques erreurs sur les capacités souscrites. Nous avons privilégié les informations les plus récentes en cas de contradictions.

Les effectifs sont supposés constants, et le taux des primes est calculé sur la capacité moyenne annuelle par type d'entreprise. L'intégration des données révèle des erreurs et des omissions pour les années 2019, 2020 et 2022, notamment la répartition des types de sinistres pour les moyennes et petites entreprises. Par défaut, ces sinistres sont classés comme 'XS et S', car fortement majoritaires.

Enfin, les rapports présentent des inexactitudes, notamment pour les sinistres de type XL en 2021. Par exemple, pour quatre sinistres XL (entre 3 et 10 millions d'euros) de la base les indemnités totales devraient être entre 12 et 40 millions d'euros mais le rapport indique seulement 11,6 millions d'euros. Nous ajustons ces valeurs pour correspondre aux intervalles définis. La somme de ces quatre sinistres vaut alors 12 millions d'euros.

3.2.2 Étude de la base LUCY créée

À la différence de PRC et VERIS, la base issue de LUCY ne nous renseigne pas sur les secteurs d'entreprises concernées, ni sur le type d'attaque. Cependant, la base obtenue nous informe sur la taille des sinistres cyber.

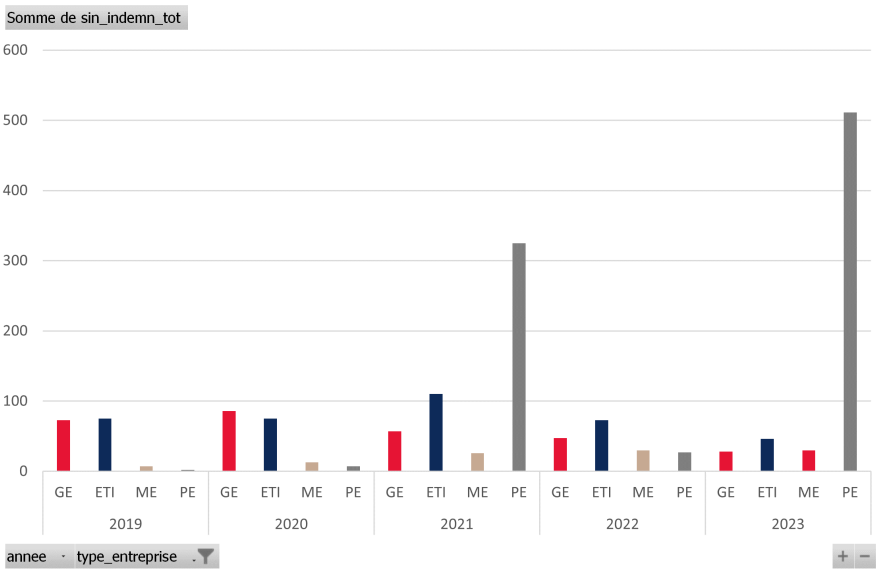

FIGURE 3.9 : Répartition des sinistres de la base LUCY selon l'année et le type d'entreprise

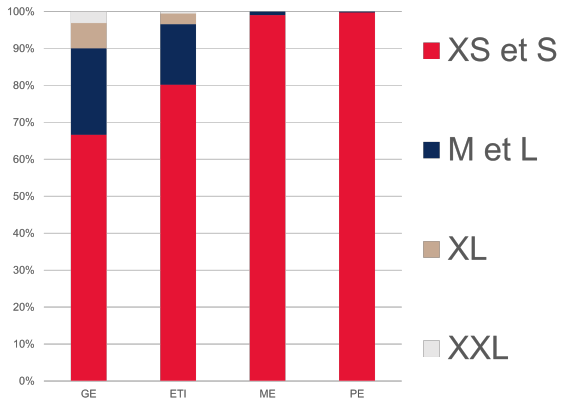

FIGURE 3.10 : Répartition du nombre des différentes tailles de sinistres selon le type d'entreprise

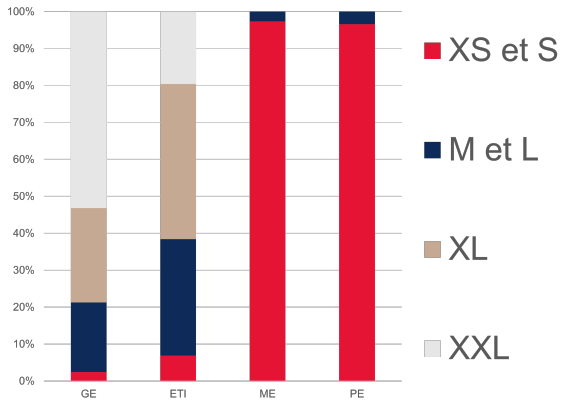

FIGURE 3.11 : Répartition du coût des différentes tailles de sinistres selon le type d'entreprise

Les sinistres XS et S sont majoritaires en nombre pour toutes les catégories d'entreprises, mais ils représentent une faible part du coût total des sinistres pour les Grandes Entreprises (GE) et les Entreprises de Taille Intermédiaire (ETI), où les sinistres XL et XXL prédominent.

La base de données LUCY est principalement composée de sinistres XS et S. Cependant, les grandes entreprises et les entreprises intermédiaires sont plus souvent touchées par des sinistres de taille M et L, tandis que les grandes entreprises comptabilisent la majorité des sinistres XL et XXL.

3.3 Croisement des bases de données VERIS et LUCY

Avec les données LUCY, il est possible de déterminer les proportions des tailles de sinistres pour chaque année. La variable **victim.employee_count** fournit le nombre de salariés dans l'entreprise, ce qui permet de conjecturer sur la taille de l'entreprise. Les différentes valeurs possibles pour **victim.employee_count** sont : 1 to 10, 11 to 100, 101 to 1000, 1001 to 10000, 10001 to 25000, 25001 to 50000, 50001 to 100000, Over 100000, Small, et Large.

Nous classons donc les entreprises selon la segmentation proposée par LUCY :

Taille de l'entreprise	Valeurs prises
Petite Entreprise (PE)	1 to 10, 11 to 100
Moyenne Entreprise (ME)	101 to 1000
Entreprise de taille Intermédiaire (ETI)	1001 to 10000, 10001 to 25000
Grande Entreprise (GE)	25001 to 50000, 50001 to 100000, Over 100000

TABLE 3.9 : Répartition effectuée pour la taille des entreprises de la base VERIS

Problème des *Small* et des *Large*

Cependant, un problème se pose avec les catégories *Small* et *Large* : *Small* correspond à moins de 1000 employés, tandis que *Large* correspond à plus de 1000 employés, ce qui crée une ambiguïté dans la classification.

D'après le site veris :

- Small : Petite organisation, 1000 employés ou moins et donc small peut représenter les valeurs 1 to 10, 11 to 100 ou 101 to 1000 soit des entreprises des petites ou moyennes entreprises
- Large : Grande organisation, plus de 1000 employés, donc des variables 1001 to 10000, 100001 to 25000, 25001 to 50000, 50001 to 100000 ou Over 100000, et peut représenter des ETI ou GE

Ainsi Small peut décrire une petite ou moyenne entreprise et Large une ETI ou GE

Nous allons utiliser la proportion de variables non *Small*, non *Large*, pour répartir ces valeurs.

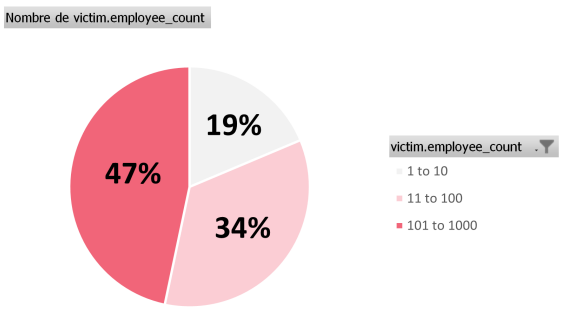

FIGURE 3.12 : Répartition des valeurs de **victim.employee_count** pour un nombre d'employés inférieur à 1000 dans VERIS

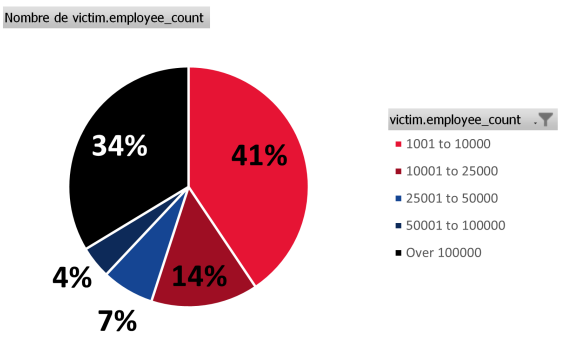

FIGURE 3.13 : Répartition des valeurs de **victim.employee_count** pour un nombre d'employés supérieur à 1000 dans VERIS

Nous attribuons alors les tailles d'entreprises à chaque sinistre de la base VERIS selon *victim.employee_ count*. On obtient le nombre de sinistres par année selon les catégories d'entreprises de la base VERIS

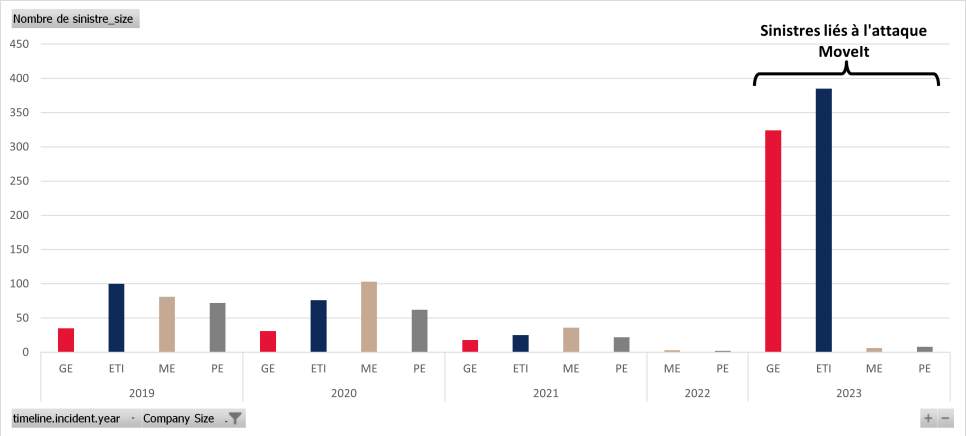

FIGURE 3.14 : Évolution du nombre de sinistre par année selon les catégories d'entreprises de la base VERIS

Les entreprises présentes dans la base VERIS le plus attaquées sont les entreprises intermédiaires (ETI) et moyennes entreprises (ME), vient ensuite les petites entreprises (PE) et finalement les grandes entreprises (GE). Cette répartition est plausible : les grandes entreprises sont moins attaquées comme le souligne le rapport de l'AMRAE

L'année 2022 montre peu de sinistres, ce qui est lié à la vitesse de reporting qui peut être lente (cf. 1.2 et 3.1.3).

L'année 2023 montre cependant un pic extrêmement important de sinistres pour les grandes entreprises (GE) et les entreprises intermédiaires (ETI). Ceci est dû à l'attaque MoveIt qui a été référencée dès son apparition. Pourtant, ces données peuvent contenir des erreurs, car ces sinistres utilisent toutes les valeurs *Small* et *Large* vues précédemment.

Maintenant que les sinistres de la base VERIS incluent la variable *company_ size*, décrivant la taille de l'entreprise attaquée selon les critères des rapports LUCY, nous pouvons créer deux nouvelles variables basées sur les proportions de sinistres observées dans la base LUCY : *loss_ amount*, qui représente la catégorie du sinistre, et *average_ cost*, qui indique les coûts moyens associés.

Par exemple, selon LUCY, 73% des sinistres des grandes entreprises en 2021 sont des sinistres XS et S. Ainsi, dans la base de données créée, 73% des sinistres en 2021 ciblant une grande entreprise seront des sinistres "XS et S".

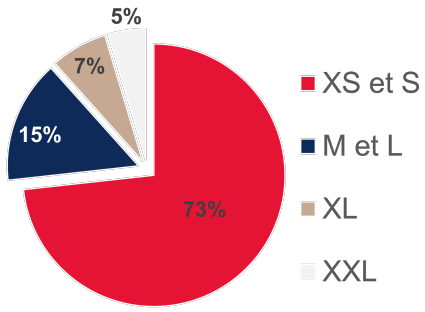

FIGURE 3.15 : Proportion des types de sinistres pour les grandes entreprises en 2021 pour les grandes entreprises selon la base LUCY

Nous pouvons également regarder le coût moyen des sinistres par années et par taille d'entreprise :

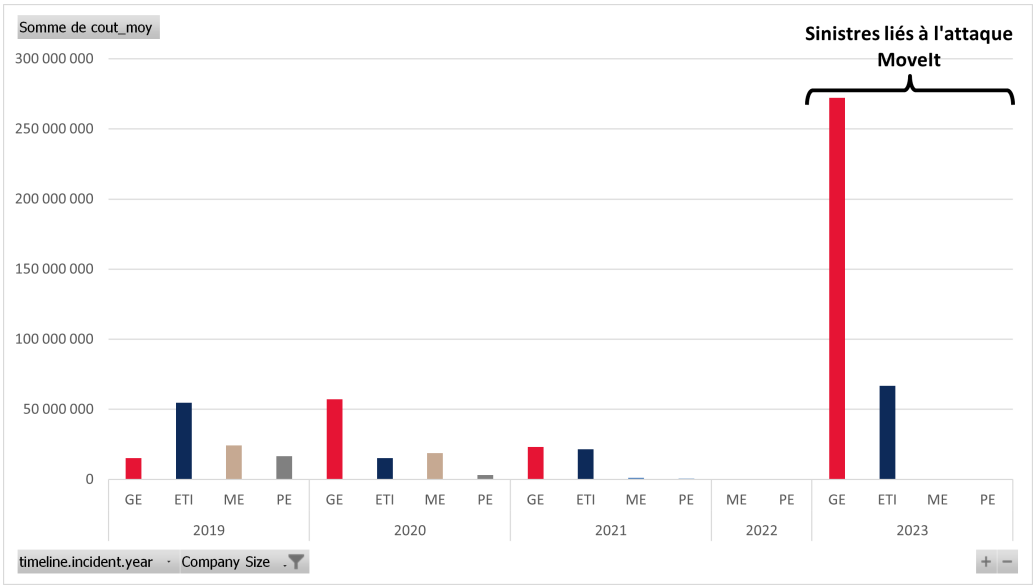

FIGURE 3.16 : Évolution du coût total des sinistres de la base VERIS selon les années et le type d'entreprise

Il existe une disparité entre les années : en 2019, les grandes entreprises ne représentent pas le même poids en termes de sinistres que dans la base LUCY, contrairement aux conclusions de la base VERIS. En revanche, les années 2020 et 2021 montrent une correspondance plus proche entre les deux bases.

L'année 2023 montre un coût total des sinistres très élevé pour les grandes entreprises et entreprises de taille intermédiaire. Cela est dû à leur nombre très élevé (voir figure 3.15) malgré un coût moyen en baisse (voir 1.2).

3.4 Synthèse

Nous obtenons une base de données qui se présente comme suit :

Nom	Année	Type	Secteur	Taille	Montant	Types d'attaque
Cameron Univ	2023	ETI	EDU	XS et S	38 461	['malware', 'hacking', 'social']
Tokopedia	2020	ETI	BSR	XS et S	71 194	['hacking']
SCUF Gaming	2020	ME	BSO	XS et S	181 538	['error']

TABLE 3.10 : Trois sinistres de la base de données résultante

Ce chapitre a permis d'obtenir une base plus adaptée au marché français, en intégrant des données spécifiques sur les coûts des sinistres issus des rapports LUCY. Cependant, cette base reste imparfaite. Les proportions des types d'attaques et des secteurs d'entreprises sont toujours basées sur les données américaines issues de la base VERIS. Cela peut introduire des biais en raison des spécificités du marché français. Malgré cela, les coûts des sinistres ont été ajustés pour mieux refléter la réalité du marché français, offrant ainsi une meilleure base de travail pour la modélisation et la tarification des risques cyber en France.

Chapitre 4

Tarification pour l'assurance cyber

Comme nous l'avons vu dans le chapitre I, le marché de l'assurance cyber est encore embryonnaire, et les primes et les couvertures d'assurance restent encore très volatiles. L'objectif de cette partie est de proposer une prime d'assurance cyber à partir de données fournies par l'entreprise.

4.1 Modèle d'optimisation

Considérons une entreprise, ou agent i qui souhaite souscrire une assurance contre les différents risques cyber. L'assureur a accès à un ensemble de données internes pertinentes pour évaluer ce risque. Pour l'assureur, il est crucial de déterminer si assurer l'entreprise i est rentable. En outre, l'offre d'assurance doit être attrayante pour l'entreprise, assurant un équilibre entre couverture et coût. L'assureur peut résoudre ce dilemme à l'aide d'un problème d'optimisation, visant à établir une prime pure et une couverture d'assurance optimale qui soient spécifiquement adaptées aux besoins et au profil de risque de chaque entreprises i. Pour répondre à cette problématique d'optimisation, l'assureur peut étudier les fonctions d'utilité associées aux entreprise i. Dans un premier temps, nous allons donc poser les bases de ce problème d'optimisation et après l'avoir résolu de façon théorique, l'appliquer à des données existantes.

4.1.1 Définition du problème

Cette section présente un modèle d'optimisation du profit pour une compagnie d'assurance qui offre des polices d'assurance cyber. L'objectif est de maximiser le profit de l'assureur, Π_i, tout en s'assurant que l'utilité de l'agent i, ou client, est plus grande avec l'assurance qu'elle ne le serait sans. On considère ici les divers facteurs qui influencent cette utilité et le profit, comme la probabilité d'un incident cyber, la richesse initiale de l'agent, les coûts de protection, les pertes potentielles dues à un incident, la prime d'assurance payée par l'agent, et le dédommagement reçu en cas de sinistre. Le modèle équilibre ces éléments pour définir une structure de prix qui est bénéfique à la fois pour l'assureur et pour l'agent, en se basant sur les fonctions d'utilité conditionnelles avec et sans assurance, et en établissant les contraintes nécessaires pour que l'assurance soit une option attractive pour le client.

On souhaite ainsi maximiser le profit de l'assureur, proposant une assurance cyber pour chaque entreprise i :

$$\Pi_i = (1 - p_i) \cdot \pi_i + p_i \cdot (\pi_i - X_i)$$

On définit la fonction d'utilité conditionnelle de l'agent i **sans** assurance (ou utilité de réserve) :

$$\mathbb{E}\left[U_i(W_i)\right]_r = (1 - p_i) \cdot U_i(W_i^0 - C_i) + p_i \cdot U_i(W_i^0 - L_i - C_i) \tag{1}$$

On définit également la fonction d'utilité conditionnelle de l'agent i **avec** une assurance

$$\mathbb{E}\left[U_i(W_i)\right] = (1 - p_i) \cdot U_i(W_i^0 - C_i - \pi_i) + p_i \cdot U_i(W_i^0 - L_i - C_i - \pi_i + X_i) \tag{2}$$

avec :

$$\begin{cases} p_i & : \text{probabilité d'incident cyber associé à l'agent } i, \\ W_i^0 & : \text{richesse initiale de l'agent } i, \\ C_i & : \text{Coût de l'auto protection cyber de l'agent } i, \\ L_i & : \text{Perte potentielle liée au cyber-incident de l'agent } i, \\ \pi_i & : \text{Prime de la cyber assurance pour l'agent } i, \\ X_i & : \text{Couverture de la protection cyber de l'agent } i, \\ \Pi_i & : \text{Profit de l'assureur vis à vis de l'agent } i. \end{cases}$$

Le problème d'optimisation du profit de l'assureur s'écrit alors :

$$\begin{aligned} &\max \Pi_i \\ &\begin{cases} \quad (2) \geq (1) \\ \pi_i, X_i \geq 0 \end{cases} \end{aligned}$$

4.1.2 Hypothèses sur les variables d'études

Afin de créer un produit d'assurance cyber sur mesure pour les entreprises i, il est impératif d'abord d'établir des hypothèses fondées sur les données internes de ces entreprises. Ces hypothèses nous permettront ensuite, dans la section suivante, d'évaluer et de comparer le niveau de couverture et la prime optimale pour chaque entreprise i.

D'abord, nous examinerons en détail chaque variable, en clarifiant les hypothèses sur lesquelles elles reposent. Ensuite, nous expliquerons la méthode utilisée pour déterminer les valeurs de ces variables pour les trois entreprises choisies comme exemples.

Richesse Initiale W_i^0

Pour comprendre l'enjeu du problème micro-économique, il est essentiel de se pencher sur la richesse initiale, soit W_i^0, car elle constitue le fondement des ressources disponibles pour un agent économique avant toute prise de décision. Cette richesse initiale permet de déterminer la capacité de l'agent à effectuer des investissements, à acquérir des assurances, et à gérer les risques tels que ceux associés aux attaques cyber. Dans le cadre d'une modélisation simplifiée, on peut choisir de représenter cette richesse initiale par le chiffre d'affaires de l'entreprise, car il fournit une mesure accessible et immédiate

de son activité économique. En effet, le chiffre d'affaires, en tant que flux de revenus bruts, peut servir d'indicateur simplifié de la richesse disponible pour engager des dépenses opérationnelles et stratégiques.

Coût de l'auto-protection cyber C_i

Dans le cadre de la microéconomie, le coût de l'auto-protection pour une entreprise, C_i, qui englobe les dépenses en cybersécurité et en mesures préventives pour se prémunir contre les risques opérationnels, est un facteur essentiel dans le problème d'optimisation. Ce coût représente une portion significative des ressources qu'une entreprise alloue pour sauvegarder son intégrité et sa continuité d'activité. Étant donné que le chiffre d'affaires reflète le volume global des transactions économiques de l'entreprise, il peut servir de base pour estimer le coût de l'auto-protection. Utiliser un pourcentage du chiffre d'affaires pour modéliser ce coût offre une méthode simplifiée mais efficace, car elle permet d'adapter les dépenses de sécurité proportionnellement à l'activité économique de l'entreprise. En d'autres termes, plus l'entreprise génère de revenus, plus elle investira absolument, non pas en termes de coûts fixes, mais en fonction de sa taille et de son exposition au risque, dans la protection de ses actifs numériques et opérationnels.

Dans les faits, plusieurs sources, comme l'Agence Natonale de la sécurité des système d'information (ANSSI), Beugin (2022), recommande que les entreprises dépensent en moyenne 4% de leur chiffre d'affaire dans leur branche service technologique incluant la prévention contre le risque cyber.

Probabilité de survenance du risque cyber p_i

La probabilité de survenance d'un risque cyber, notée p_i, est une mesure variable et fortement dépendante de caractéristiques spécifiques à chaque entreprise. Cette probabilité n'est pas uniforme ; elle fluctue selon le secteur d'activité de l'entreprise, qui peut être plus ou moins exposé à des risques de cyber attaques. Par exemple, une entreprise opérant dans le domaine de la technologie ou détenant une grande quantité de données sensibles pourrait être considérée comme ayant une probabilité plus élevée d'être ciblée par des cyber criminels.

La taille de l'entreprise influence également p_i, dans la mesure où les grandes entreprises sont souvent des cibles plus attrayantes en raison de leurs ressources plus abondantes et de leur potentiel de rançon plus élevé. Cependant, les petites entreprises ne sont pas à l'abri ; elles peuvent être perçues comme ayant des défenses moins robustes, augmentant ainsi leur probabilité d'être attaquées.

Le nombre d'employés est un autre facteur pertinent, car un effectif plus important peut signifier une plus grande surface d'attaque due à un nombre plus élevé de points d'accès potentiels, comme les appareils mobiles et les connexions à distance.

Perte potentielle liée au risque cyber L_i

La perte potentielle liée au risque cyber, notée L_i, représente l'impact financier qu'une cyberattaque pourrait avoir sur une entreprise. Cette perte n'est pas une valeur fixe et peut varier considérablement en fonction de plusieurs facteurs intrinsèques à l'entreprise elle-même.

Tout d'abord, **le type d'entreprise** joue un rôle prépondérant dans l'évaluation de L_i. Les entreprises qui opèrent principalement en ligne ou qui dépendent fortement de la technologie informatique

pour leurs opérations quotidiennes peuvent subir des pertes plus importantes en cas d'incident cyber. Par exemple, pour une entreprise de e-commerce, une attaque perturbant les transactions en ligne pourrait entraîner une perte de revenus directe et significative.

La taille de l'entreprise affecte également le calcul de L_i. Les grandes entreprises peuvent avoir plus à perdre en termes de réputation et de revenus, mais elles ont souvent aussi des ressources plus importantes pour la récupération après une attaque. Inversement, même si les pertes absolues peuvent être moindres pour les petites entreprises, l'impact relatif à leur taille peut être dévastateur.

Le domaine d'activité est également un facteur clé. Les secteurs réglementés comme la finance, la santé ou les services aux entreprises, où la protection des données est cruciale, peuvent subir des pertes plus importantes en raison de la violation de données sensibles, pouvant mener à des sanctions réglementaires, des litiges et une perte de confiance des clients.

Le nombre d'employés influence également L_i, non seulement en termes de surface d'attaque potentielle, mais aussi en raison du potentiel de négligence ou d'erreur humaine, qui peut mener à des failles de sécurité.

Il convient donc dans nos exemple de prendre en considération les facteurs ci-dessus pour présenter une valeur de la perte potentielle pour chaque entreprise i

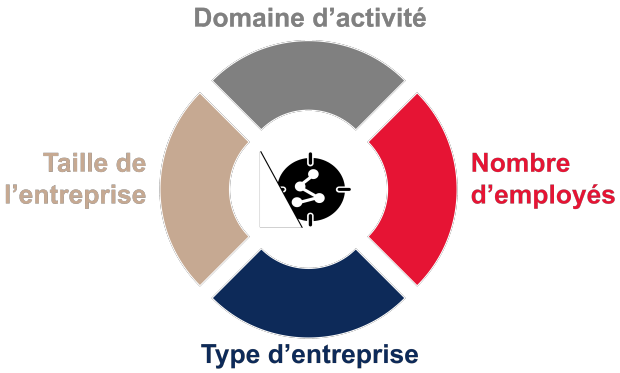

FIGURE 4.1 : Éléments influant le calcul de la perte potentielle

Fontion d'Utilité U_i

La fonction d'utilité U_i en microéconomie représente les préférences d'un agent économique (cf **1.5**), dans ce cas une entreprise, en termes de satisfaction ou de bien-être tiré de différents états de richesse. Elle est fondamentale pour évaluer comment les entreprises prennent des décisions face au risque, comme ceux associés aux attaques cyber.

L'hypothèse d'une fonction d'utilité identique pour chaque entreprise, simplifiée par $U_i = U$, repose sur l'argument que, malgré leurs différences en termes de taille, de secteur, ou de structure, les entreprises ont tendance à réagir de manière similaire face au risque lorsqu'elles sont confrontées à des décisions économiques. Awiszus et al. (2023) soutient que, pour des raisons de modélisation, cette standardisation facilite l'analyse et permet de concentrer l'étude sur les effets des changements dans les variables clés, telles que la richesse initiale, la probabilité de sinistre, et l'ampleur des pertes potentielles. Cette hypothèse est certes utile pour la simplification du modèle, mais elle peut être questionnée dans la mesure où elle suppose une homogénéité qui ne reflète pas toujours la réalité économique. En effet, selon

la taille, le secteur ou encore le degré d'aversion au risque des dirigeants, les entreprises peuvent adopter des stratégies différentes face au risque. Toutefois, dans le cadre de cette étude, cette approximation est justifiée par la nécessité de se concentrer sur les effets des variables clés, tout en maintenant une lisibilité dans l'analyse. Une extension possible consisterait à examiner dans quelle mesure la prise en compte d'une fonction d'utilité différenciée modifierait les conclusions obtenues.

Pour nos premiers calculs de prime, nous allons commencer par utiliser la fonction d'utilité logarithme, $U(x) = ln(x)$, soit une fonction CRRA. Dans le problème d'optimisation micro-économique, la fonction logarithme est couramment utilisée car son utilisation est simple ce qui facilitera nos premiers calculs et constituera une première base solide pour notre problème.

De plus, l'emploi d'une fonction d'utilité logarithmique standardisée pour toutes les entreprises permet de modéliser de manière simplifiée et cohérente l'attitude vis-à-vis du risque, tout en reconnaissant que chaque entreprise cherche à maximiser sa satisfaction ou son utilité face à des décisions sous incertitude.

4.2 Résolution théorique du problème d'optimisation

Dans cette section, nous aborderons la résolution mathématique du problème d'optimisation défini en **2.1**, visant à déterminer les primes π_i et les couvertures X_i optimales pour l'assurance cyber. L'objectif est de trouver une équation délimitant la frontière à partir de laquelle l'offre d'une police d'assurance devient avantageuse pour l'assureur. Cette frontière nous permettra d'identifier les conditions sous lesquelles l'assureur bénéficiera de la proposition d'un produit d'assurance cyber.

4.2.1 Couverture Optimale

On va chercher le contrat optimal (X_i^*, π_i^*) pour un assureur étant averse au risque L'assureur étant averse au risque sa fonction d'utilité est concave, on a donc $U^{'}$ décroissante et $U^{''} < 0$. L'assureur va chercher à maximiser son profit sous **contrainte de participation** de l'agent i.

En reprenant le problème d'optimisation de la partie 4.1, on a :

$$\begin{aligned} &\max \Pi_i \\ &\begin{cases} \quad (2) \geq (1) \\ (\pi_i, X_i) \geq 0 \end{cases} \end{aligned}$$

En réécrivant le profit de l'assureur, on a :

$$\Pi_i(X_i, \pi_i, p_i) = \pi_i - p_i \cdot X_i$$

On écrit le Lagrangien :

$$\mathcal{L}(\lambda, X_i, \pi_i) = \pi_i - p_i \cdot X_i + \lambda \cdot [(2) - (1)]$$

On résout ensuite :

$$\begin{cases} \frac{\partial \mathcal{L}}{\partial \pi_i} = 0 \quad \Leftrightarrow \quad 1 - \lambda \cdot p_i \cdot U^{'}(W_i^0 - C - L_i + X_i - \pi_i) - (1 - p_i) \cdot U^{'}(W_i^0 - C_i - \pi_i) = 0 & (I) \\ \frac{\partial \mathcal{L}}{\partial (X_i)} = 0 \quad \Leftrightarrow \quad -p_i + \lambda \cdot p_i \cdot U^{'}(W_i^0 - C_i - L_i + X_i - \pi_i) = 0 & (II) \\ \frac{\partial \mathcal{L}}{\partial \lambda} = 0 \quad \Leftrightarrow \quad p_i \cdot U(W_i^0 - C_i - L_i + X_i - \pi_i) + (1 - p_i) \cdot U(W_i^0 - C_i - \pi_i) - (1) = 0 & (III) \end{cases}$$

D'une part, avec (I)

$$\lambda = \frac{1}{p_i \cdot U'(W_i^0 - L_i + X_i - C_i - \pi_i) + (1 - p_i) \cdot U'(W_i^0 - C_i - \pi_i)}$$

D'autre part avec (II)

$$\lambda = \frac{1}{U'(W_i^0 - L_i + X_i - C_i - \pi_i)}$$

Ainsi

$$\begin{aligned} & U^{'}(W_i^0 - L_i + X_i - C_i - \pi_i) = p_i \cdot U^{'}(W_i^0 - L_i + X_i - C_i - \pi_i) + (1 - p_i) \cdot U^{'}(W_i^0 - C_i - \pi_i) \\ \Leftrightarrow\ & U^{'}(W_i^0 - L_i + X_i - C_i - \pi_i) = U^{'}(W_i^0 - C_i - \pi_i) \\ \Leftrightarrow\ & X_i^* = L_i \quad \text{(car la fonction } U^{'} \text{est croissante (donc monotone))} \end{aligned}$$

En d'autres termes, la couverture optimale est la couverture complète. Pourtant, ce résultat, bien que conforme aux conclusions émises par Awiszus et al. (2023), n'est dans la pratique pas toujours vérifié. Comme le souligne le tableau des garanties de la partie 1.2, les assureurs proposent systématiquement des franchises dans les contrats d'assurance cyber. Ce constat s'explique principalement par l'onérosité d'une couverture complète, qui impliquerait des primes trop élevées pour les assurés et un risque financier trop important pour les assureurs. Ainsi, la présence de franchises permet non seulement de rendre les contrats plus accessibles aux entreprises en réduisant le coût des primes, mais aussi d'inciter à une meilleure gestion du risque de la part des assurés. Cette approche met en évidence l'écart entre l'optimum théorique et les contraintes économiques et structurelles du marché de l'assurance cyber.

4.2.2 Prime pure optimale

Intéressons-nous maintenant à la prime optimale π_i^*, en reprenant l'équation (III) de la partie précédente, et en y ajoutant la couverture optimale X_i^*, nous avons :

$$\begin{aligned} & p_i \cdot U(W_i^0 + X_i^* - L_i - C_i - \pi_i) + (1 - p_i) \cdot U(W_i^0 - C_i - \pi_i) - (1) = 0 \\ \Leftrightarrow\ & U(W_i^0 - C_i - \pi_i) = (1) \\ \Leftrightarrow\ & \pi_i^* = W_i^0 - C_i - U^{-1}((1)) \\ \Leftrightarrow\ & \pi_i^* = W_i^0 - C_i - U^{-1}((1 - p_i) \cdot U_i(W_i^0 - C_i) + p_i \cdot U_i((W_i^0 - L_i - C_i)) \end{aligned}$$

4.2.3 Ajout de franchises et de chargement au problème d'optimisation

Pour proposer une prime qui soit plus conforme aux primes existantes sur le marché nous pouvons ajouter une franchise, δ_i, et un chargement, λ, dans notre problème d'optimisation.

Cependant la méthode précédente ne nous permet pas de conclure sur une formule de la prime optimale. Pour obtenir une prime, nous pouvons passer par les résultats de Duguet (n.d.) qui propose de calculer une franchises δ_i^* optimale selon les différentes fonctions d'utilités utilisées, puis d'en déduire une prime optimale.

Aisni selon Duguet (n.d.) :

1. **Pour une fonction CRRA**, la couverture optimale s'écrit,

$$a^* = 1 - \frac{1}{W \cdot L} \ln\left(\frac{1+\lambda}{1-(1+\lambda)p}\right)$$

et la franchise optimale s'écrit

$$\delta_i^* = \frac{W_i^0 + (1-(1+\lambda)p_i)L_i}{\frac{1}{k} - (1+\lambda)p_i}$$

avec

$$k = 1 - \left(\frac{1-(1+\lambda)p_i}{(1-p_i)(1+\lambda)}\right)^{\frac{1}{1-\alpha}}$$

Remarque : Dans le cas où $\alpha \to 0$ (donc $U = \ln$),

$$k_{\alpha\to 0} = \frac{\lambda}{(1-p_i)(1+\lambda)}$$

donc,

$$\delta_{i,\alpha\to 0}^* = \frac{\lambda W_i^0}{(1+\lambda)(1-(1+\lambda)p_i)} + \frac{\lambda L_i}{1+\lambda}$$

2. **Pour une fonction CARA**, la couverture optimale s'écrit

$$a^* = 1 - \frac{1}{\alpha \cdot L} \ln\left(\frac{1+\lambda}{1-(1+\lambda)p}\right)$$

la franchise optimale s'écrit :

$$\delta_i^* = \frac{1}{\alpha} \ln\left(1 + \frac{\lambda}{1-(1+\lambda)p_i}\right)$$

Dans notre modèle à risque unique, la prime optimale π_i^*, se calcule alors :

$$\pi_i^* = (1+\lambda)(L_i - \delta_i^* \cdot L_i)p_i$$

4.2.4 Exemple sur trois entreprises $i = 1,\ 2,\ 3$

Nous allons maintenant appliquer les résultats à trois entreprises fictives, notées $i = 1, 2, 3$. Nous commencerons par formuler des hypothèses concernant les variables spécifiques à chacune de ces entreprises. Cet exemple nous permettra de visualiser les résultats obtenus et servira également à illustrer l'étude de sensibilité qui sera menée par la suite.

La première entreprise, $i = 1$, spécialisée dans la technologie et le développement de logiciels, emploie 150 personnes et génère un chiffre d'affaires annuel de 20 millions d'euros. Elle est hautement vulnérable aux attaques cyber en raison de la quantité importante de données sensibles qu'elle manipule

et parce qu'elle est activement engagée dans la lutte contre les menaces cyber, ce qui en fait une cible de choix. Il est raisonnable d'estimer à 30% la probabilité qu'elle soit victime d'une attaque cyber au cours de l'année. Consciente de ce risque, elle consacre un budget significatif à sa protection, soit 4% de son chiffre d'affaires, ce qui représente 800 000 euros. Comme son activité économique repose essentiellement sur le traitement de données sensibles via des outils informatiques, toute interruption de service ou perte de données pourrait entraîner de lourdes pertes financières. Ainsi nous faisons l'hypothèse qu'une attaque cyber pourrait entraîner une perte de 1M€.

L'entreprise 2, avec ses 500 employés et un chiffre d'affaires de 100 millions d'euros, se concentre sur la distribution alimentaire durable. Bien qu'elle soit moins exposée aux attaques cyber que les entreprises technologiques, la nature de ses données client et sa dépendance aux systèmes logistiques intelligents augmentent ses risques. Sa probabilité annuelle de subir une cyberattaque est estimée à 15%. Elle investit 2% de son chiffre d'affaires, soit 2 millions d'euros, dans la cybersécurité. Selon Norton, une attaque pourrait lui coûter en moyenne 2 million d'euros, un risque non négligeable qui pourrait affecter gravement ses opérations.

L'entreprise 3, bien que comptant seulement 80 employés et réalisant un chiffre d'affaires de 50 millions d'euros, n'est pas à l'abri des menaces cyber. En tant que concepteur et distributeur de mobilier haut de gamme, la société pourrait subir des dommages significatifs en termes de vol ou de compromission de designs exclusifs et de données clients, même si son activité se concentre majoritairement sur des biens physiques. Avec une probabilité d'incident de 10% et un investissement de 0.5% de son chiffre d'affaires pour la cybersécurité, soit 250 000 euros, l'entreprise 3 doit être consciente que le coût moyen d'une cyberattaque s'élève à 200 000 euros, d'après les données de Norton, ce qui souligne l'importance d'une assurance et d'une protection adéquates contre ces risques.

	Entreprise 1	Entreprise 2	Entreprise 3
Secteur d'activité	Technologie	ONG	Vente de mobilier
Nombre d'employés	150	500	80
Chiffre d'affaire (W_i^0)	20M€	100M€	50M€
Coût de l'autoprotection (C_i)	4%	2%	0,5%
Probabilité d'incident (p_i)	30%	15%	10%
Pertes potentielles (L_i)	1M€	500k€	200k€

TABLE 4.1 : Caractérisation des entreprises $i = 1,\ 2,\ 3$

En calculant, à partir des résultats de **4.2**, nous trouvons que :

	Entreprise 1	**Entreprise 2**	**Entreprise 3**
Couverture optimale L_i^*	1M€	500k€	200k€
Prime optimal π_i^*	305 636€	75 163€	20 036€
Prime minimale π_i^{min}	300 000€	75 000€	20 000€
Profit optimal Π_i^*	5 636€	163€	36€

TABLE 4.2 : Application numérique

La prime minimale π_i^{min}, prime à partir de laquelle l'assurance fait profit, est calculé de la manière suivante :

$$\pi_i^{min} = L_i^* \cdot p_i$$

Et le profit optimal se trouve simplement comme différence entre la prime optimale π_i^* et la prime

minimale π_i^{min},

$$\Pi_i^* = \pi_i^* - \pi_i^{min}$$

Les résultats obtenus démontrent l'importance d'une évaluation personnalisée des risques dans la tarification des assurances cyber. Trois facteurs clés ressortent :

1. La considération de la richesse initiale dans le calcul de la prime optimale.
2. L'influence significative de la probabilité d'incidence p_i sur les primes d'assurance.
3. La marge de profit étroite, soulignant une gestion prudente des risques dans le secteur de l'assurance cyber.

Dans le cadre de la tarification des garanties proposées aux entreprises, il est pertinent d'introduire des franchises optimales afin d'ajuster les niveaux de couverture en fonction des caractéristiques spécifiques de chaque entreprise. L'approche adoptée pour intégrer ces franchises diffère de celle appliquée précédemment. Comme nous l'avons vu en section 4.2.2, cette approche repose sur une démarche structurée en trois étapes : calcul de la franchise optimale permettant de déterminer la part des pertes supportées par l'entreprise, détermination de la couverture optimale ajustée en fonction de la franchise choisie, et déduction de la prime pure optimale tenant compte de la couverture ajustée et du risque résiduel.

La fonction CARA est couramment utilisée en économie pour modéliser l'aversion au risque de manière réaliste, et est, dans notre cas, simple à mettre en place. Nous choisissons $\alpha = 0.5$ (individu prudent) afin de refléter un comportement modéré face au risque, ainsi qu'un chargement de risque de 20% pour tenir compte de l'incertitude et des exigences de rentabilité des assureurs

Le calcul de la couverture optimale indique que $a^* \approx 100\%$, ce qui signifie que la couverture est complète. Ce résultat est conforme à celui obtenu lors de l'évaluation de la prime optimale sans franchise. Il reflète également une tendance observée sur le marché de l'assurance cyber, où une couverture complète est généralement privilégiée par les entreprises pour se prémunir efficacement contre des risques potentiellement catastrophiques.

Entreprise	**Franchise Optimale**
Entreprise 1	54.,39%
Entreprise 2	43,65%
Entreprise 3	40,96%

TABLE 4.3 : Franchises optimales calculées pour chaque entreprise en utilisant la fonction CRRA

L'Entreprise 1 présente la franchise la plus élevée, ce qui reflète un niveau de risque plus important associé à son secteur. Les entreprises technologiques sont particulièrement exposées aux risques cyber et peuvent supporter des pertes plus importantes grâce à des ressources financières conséquentes.

L'Entreprise 2 bénéficie d'une franchise légèrement plus faible, illustrant une exposition plus modérée aux risques cyber malgré une taille plus importante. Cela peut s'expliquer par des pratiques de cybersécurité mieux établies.

L'Entreprise 3 a la franchise la plus basse, suggérant une exposition aux risques plus contenue mais aussi une capacité financière moindre pour absorber des pertes significatives.

Sur la base des franchises déterminées, nous pouvons calculer les primes pures optimales en fonction des pertes potentielles et des probabilités d'incidents de chaque entreprise :

Entreprise	**Prime Optimale**
Entreprise 1	164 196 €
Entreprise 2	50 715 €
Entreprise 3	14 169 €

TABLE 4.4 : Prime optimale mise à jour pour chaque entreprise

Les primes calculées sont bien en dessous des primes pures sans franchise, ce qui est logique car l'assureur est soumis à moins de risque. L'Entreprise 1 se voit attribuer la prime la plus élevée, en raison d'un risque plus élevé de cyberattaques et de pertes potentielles plus importantes. L'Entreprise 2 bénéficie d'une prime modérée, malgré un chiffre d'affaires important, grâce à une franchise bien adaptée et une probabilité d'incident relativement basse. L'Entreprise 3, malgré sa taille plus modeste, affiche une prime bien inférieure, cohérente avec sa capacité de couverture et son exposition au risque plus limitée.

Pour mieux comprendre comment chaque variable du problème affecte le calcul de la prime optimale, nous pouvons faire des tests de sensibilité, en faisant varier un paramètre et en fixant les autres afin de voir comment évolue la prime optimale.

4.3 Tests de sensibilité autour des différentes variables d'étude

L'analyse de sensibilité explore l'impact de différents paramètres sur la prime optimale d'assurance cyber. Cette section se concentre sur trois aspects principaux : l'effet de la fonction d'utilité, l'influence du chiffre d'affaires de l'entreprise et le rôle de la probabilité d'incident cyber.

4.3.1 Influence du Chiffre d'Affaires

L'analyse de sensibilité par rapport au chiffre d'affaires démontre que la prime optimale diminue avec le chiffre d'affaires de l'entreprise. Cependant, la sensibilité de cette augmentation varie en fonction de la probabilité d'incident et du montant des pertes potentielles couvertes. Les graphiques associés à cette analyse illustrent clairement la relation entre le chiffre d'affaires et la prime optimale, mettant en évidence la nécessité d'une évaluation précise du risque et du potentiel de profit pour l'assureur.

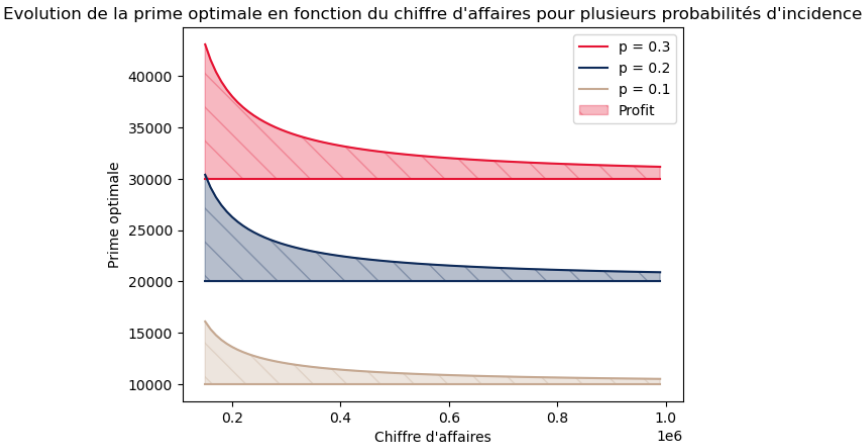

FIGURE 4.2 : Evolution de la prime optimale pour la fonction d'utilité $U(x) = ln(x)$

On observe que plus la richesse initiale est élevée, plus la variation de la prime optimale est faible. Par exemple, la différence entre les primes optimales de deux entreprises ayant respectivement 100 000 € et 1 million d'euros de richesse initiale sera plus importante que celle entre deux entreprises disposant de 1 million et 10 millions d'euros.

4.3.2 Effet de la Fonction d'Utilité

La comparaison entre les fonctions d'utilité CRRA et CARA met en évidence une différence significative dans le calcul des primes optimales. Comme illustré dans la figure, la valeur de la prime optimale varie en fonction de α, le coefficient représentant l'aversion au risque de l'entreprise. Il est également notable que les variations de la prime optimale sonient plus marquées avec la fonction CRRA, tandis qu'elles restent plus modérées avec la fonction CARA.

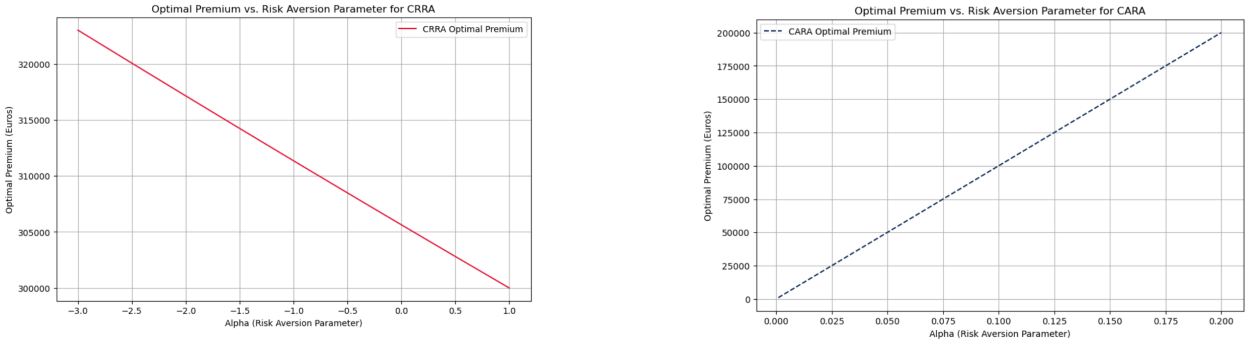

FIGURE 4.3 : Évolution de la prime optimale pour les fonctions d'utilités CRRA et CARA en fonction du coefficient d'aversion au risque α

4.3.3 Rôle de la Probabilité d'Incident

La probabilité d'incident cyber exerce une influence déterminante sur le niveau de la prime optimale. Une probabilité plus élevée conduit à une augmentation de la prime pour compenser le risque accru.

Cette relation est visualisée à travers des courbes de prime optimale (cf. figure 4.2) pour différentes probabilités d'incident, soulignant l'équilibre que l'assureur doit trouver entre le risque et la rentabilité.

Dans le calcul de la franchise optimale, on observe également qu'une augmentation de la probabilité d'occurrence d'un sinistre cyber entraîne une élévation du niveau de franchise.

4.4 Application du modèle à la base de données

Maintenant que la formule de la prime optimale a été trouvée, nous pouvons appliquer la prime à chaque entreprise de notre base de données VERIS croisée avec LUCY pour en conclure une prime moyenne pour chaque type d'entreprise. Nous avons donc besoin d'associer les variables du problème aux variables de la base.

4.4.1 Détermination du coût du sinistre

Pour le coût du sinistre L_i, les rapports LUCY nous ont permis de créer la variable *average_ cost* (cf 3.4). Cette variable sera utilisé pour L_i.

4.4.2 Détermination de la probabilité p_i d'apparition des sinistres cyber

Les rapports LUCY nous indiquent également le nombre d'entreprises assurées, ce qui nous permet de déduire, pour chaque année et pour chaque type d'entreprise la fréquence d'apparition d'un sinistre cyber.

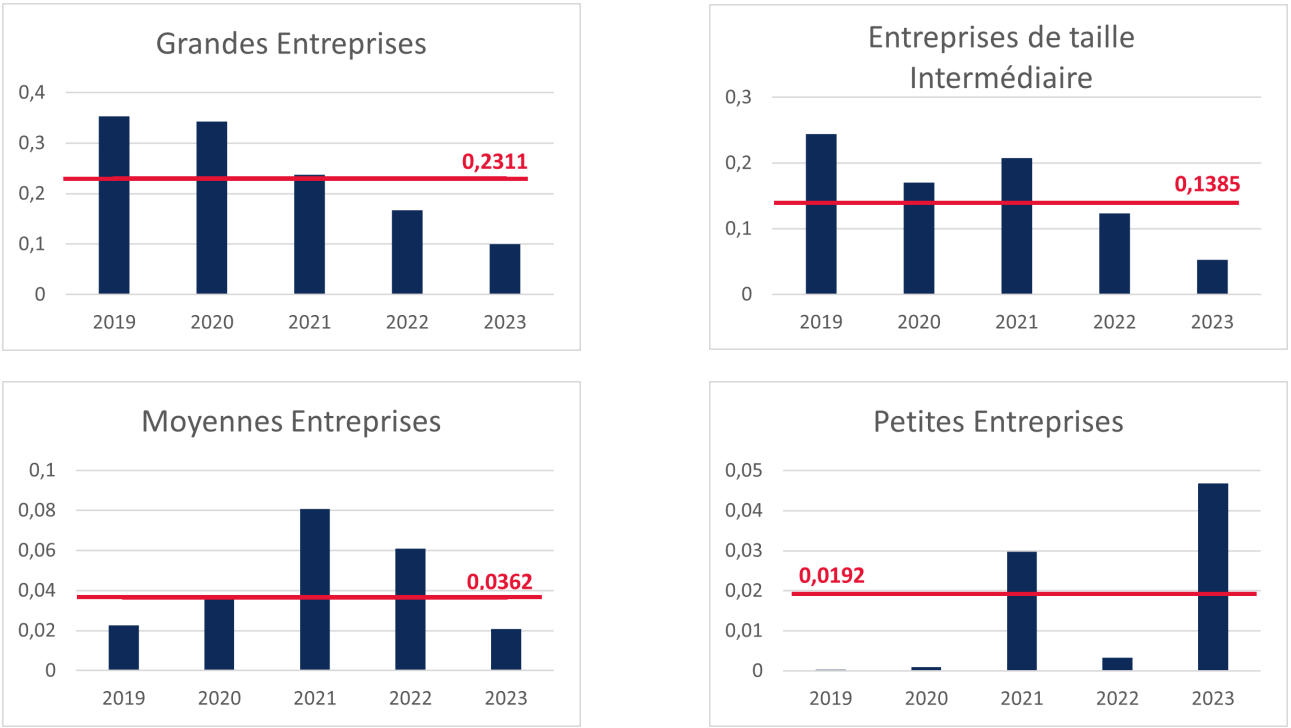

FIGURE 4.4 : Fréquence d'apparition des sinistres en fonction de la taille d'entreprise

Nous cherchons alors la probabilité p_i à implémenter dans notre modèle. La confiance dans les données disponibles reste relativement faible, ce qui limite la fiabilité des analyses basées uniquement sur ces données. En raison de cette incertitude, il est plus prudent d'adopter une approche par scénarios plutôt que de s'appuyer sur un modèle prédictif unique. Cette méthode permet de mieux anticiper les différentes éventualités en tenant compte des diverses incertitudes liées aux données, offrant ainsi une vision plus flexible et robuste des risques potentiels.

L'objectif est de proposer des scénarios probables et de réaliser des études de sensibilité afin de déterminer une probabilité p_i adaptée au modèle.

Les scénarios mis en place pour évaluer la fréquence des attaques

1. **Scénario Baseline (de référence) : fréquence égale à la moyenne historique**

   Ce scénario représente la situation la plus attendue ou typique, basée sur les données historiques. En prenant la moyenne des attaques passées, on crée un point de référence pour ce à quoi on pourrait s'attendre si les conditions restent relativement constantes. Ce scénario est utilisé comme une base pour comparer d'autres scénarios et est utile pour établir un cadre de normalité.

2. **Scénario de Pire Cas historiquement observé : Fréquence égale à la fréquence la plus élevée observée**

   Ce scénario utilise la fréquence maximale observée dans le passé comme un indicateur de ce qui pourrait se produire à nouveau dans un contexte où les risques sont élevés mais comparables à ceux rencontrés historiquement. Il s'agit d'un scénario pessimiste, mais basé sur des faits passés, ce qui le rend crédible.

3. **Scénario d'Escalade : Fréquence égale à 1,5 fois la fréquence maximale observée**

   Ce scénario représente une escalade significative par rapport à ce qui a été observé historiquement. En amplifiant la fréquence maximale passée par un facteur de 1,5, vous anticipez une situation où les conditions de menace pourraient empirer au-delà de ce qui a été vu jusqu'à présent. C'est un scénario prospectif qui anticipe une aggravation potentielle de la situation.

Par exemple, voici les différents scénarios appliqués pour les grandes entreprises

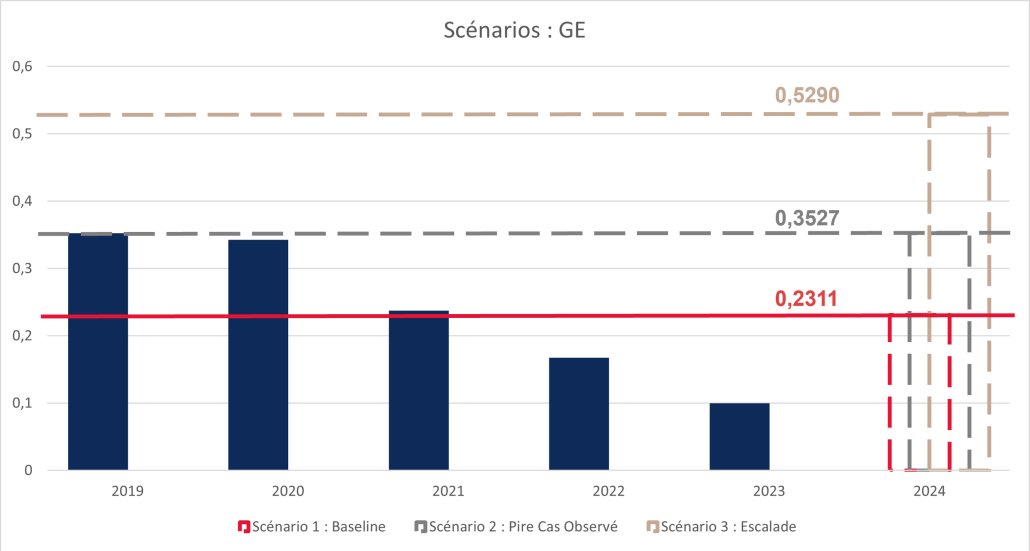

FIGURE 4.5 : Les différents scénarios appliqués aux grandes entreprises

Ces scénarios nous donne alors des $p_{(i,s)}$, des probabilités de survenance de sinistre pour chaque entreprise i, selon le scénario $s = 1, 2, 3$ choisi.

4.4.3 Détermination de la richesse initiale

La richesse initiale W_i est donnée par le chiffre d'affaire qui peut être déduit de la taille de l'entreprise. En effet, selon les rapports de l'AMRAE :

Taille de l'entreprise	**Chiffre d'affaires annuel (CA)**
Petite entreprise	$<$ 10 millions d'euros
Entreprise de taille moyenne	Entre 10 millions et 50 millions d'euros
Entreprise de taille intermédiaire	Entre 50 millions et 1,5 milliard d'euros
Grande entreprise	$>$ 1,5 milliard d'euros

TABLE 4.5 : Classification des entreprises selon leur chiffre d'affaires annuel selon LUCY

Dans la suite de notre étude, nous utiliserons une valeur moyenne de W_i pour chaque tranche. Ainsi selon la taille de l'entreprise, on a :

Taille de l'entreprise	W_i
Petite Entreprise	5M€
Entreprise de taille moyenne	30M€
Entreprise de taille intermédiaire	775M€
Grande entreprise	1 500M€

TABLE 4.6 : Valeur de la richesse initiale selon la taille de l'entreprise

Remarque : Pour les grandes entreprises, on fixera la valeur de W_i à 1 500 M€, car la tranche est infinie. De plus, selon l'étude de sensibilité effectuée en section 4.2.3, il existe peu de différence en termes d'utilité entre deux entreprises ayant cet ordre de grandeur de richesse initiale.

4.4.4 Modélisation d'une tarification cyber sans franchise sous plusieurs scénarios

En commençant par prendre $U(x) = ln(x)$, fonction CRRA, comme utilité pour les entreprises. On peut étudier les coûts des primes pures moyennes pour chaque type d'entreprise, par année puis faire une moyenne globale de tous les sinistres.

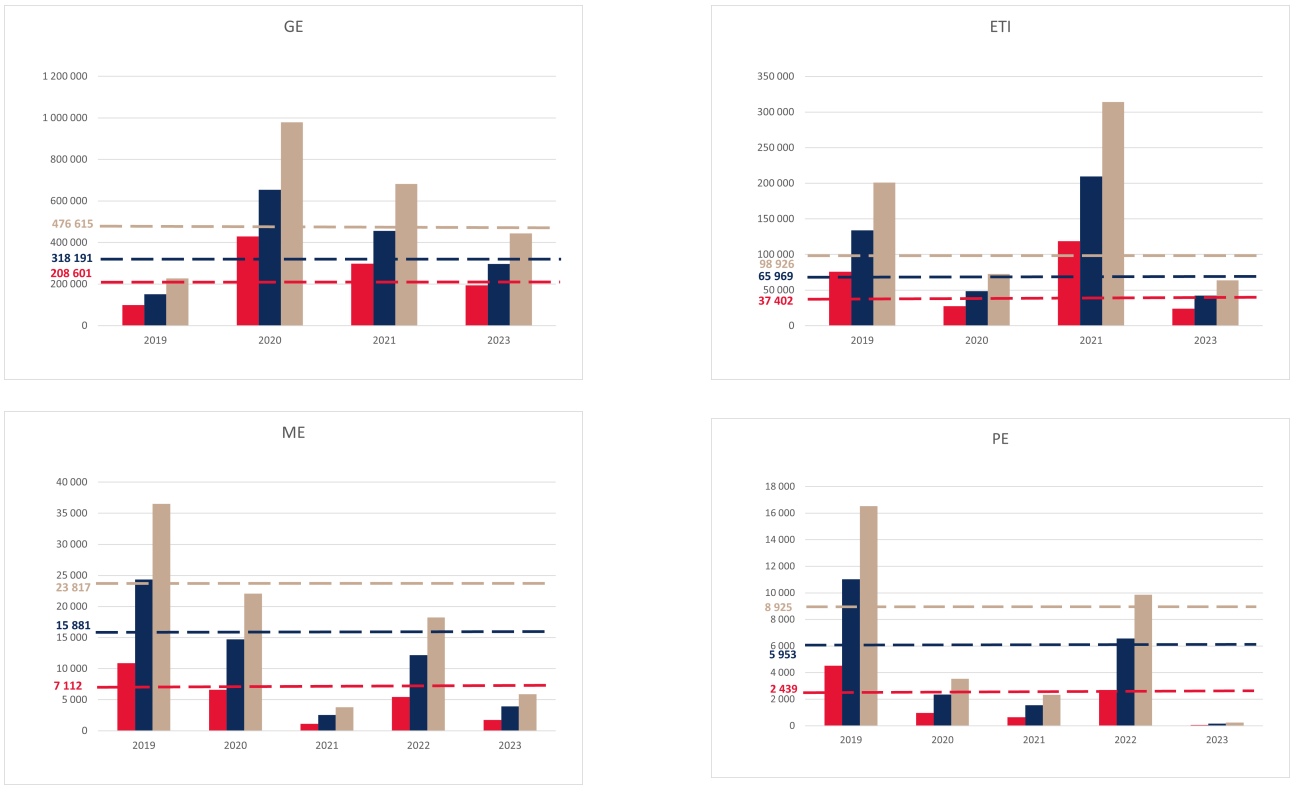

FIGURE 4.6 : Primes pures moyennes de l'assurance cyber pour chaque type d'entreprise par année puis au global pour les différents scénarios et pour $U_i(x) = ln(x)$

- On remarque que les primes que devraient payer les assurés sont très volatiles d'une année à l'autre. Cette volatilité s'explique par la variation du nombre et de la sévérité des sinistres d'année en année, ce qui influence directement le calcul des primes d'assurance.
- Il existe un problème notable pour les années 2022 en ce qui concerne les grandes entreprises et les entreprises de taille intermédiaire. En effet, le faible nombre de sinistres déclarés en 2022, dû à un délai de reporting souvent lent dans la base de données VERIS, ne permet pas d'afficher des valeurs fiables pour cette année. Cette absence de données pourrait fausser l'analyse de tendance et la modélisation des primes pour ces types d'entreprises.
- Pour l'année 2023, nous observons très peu de sinistres déclarés pour les petites entreprises. Cela peut s'expliquer par le fait que l'attaque MoveIt a touché principalement des entreprises de plus grande taille, qui ont été davantage référencées dans la base VERIS. Ce biais dans les données disponibles pourrait influencer la perception du risque pour les petites entreprises.

On peut ainsi conclure que pour des entreprises plus petites, comme des entreprises de taille moyenne, un scénario prudent comme le scénario d'escalade est à recommander. Car celui ci permet de se couvrir contre les variations importantes de sinistralité. Pour une entreprise plus grande,

comme une grande entreprise ou entreprise de taille intermédiaire, un scénario comme celui du pire cas historiquement observé peut être considéré. Pourtant, le scénario de référence comme moyenne historique, ne peut être considéré ici, car une année à forte sinistralité pourrait perturber nettement la santé financière de l'assureur. Il est également à noté que le risque cyber est en constante évolution, et on pourrait s'attendre à une évolution à la hausse de la sinistralité dans les années futures, ce qui élimine le choix du scénario de la moyenne historique.

4.4.5 Modélisation avec une fonction d'utilité CRRA

On va maintenant s'intéresser à la moyenne des primes pour chaque type d'entreprise et chaque scénarios selon différentes valeurs de α pour une fonction CRRA

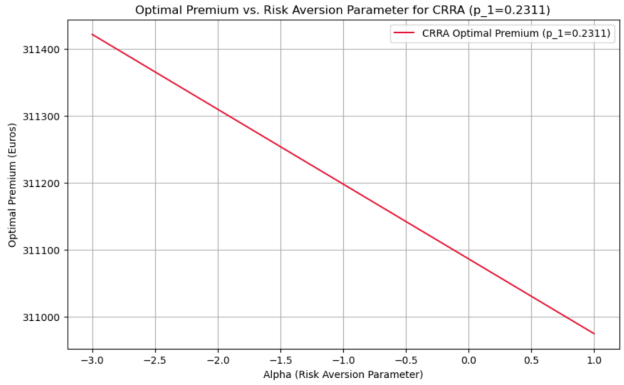

FIGURE 4.7 : Variation de la prime moyenne pour les grandes entreprises selon les valeurs de α pour le scénario 1 **Baseline**

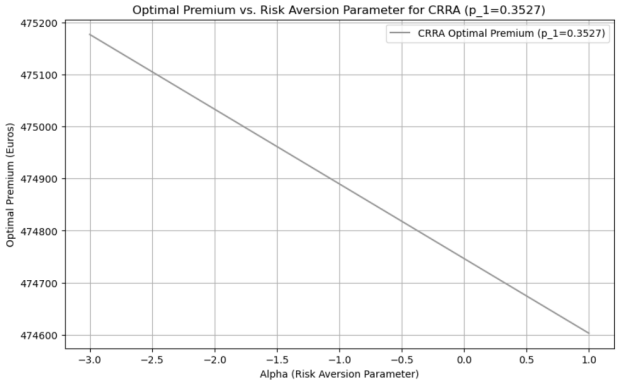

FIGURE 4.8 : Variation de la prime moyenne pour les grandes entreprises selon les valeurs de α pour le scénario 2 **Pire Cas historiquement observé**

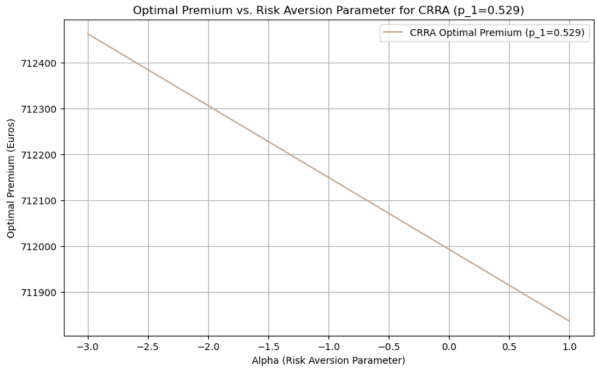

FIGURE 4.9 : Variation de la prime moyenne pour les grandes entreprises selon les valeurs de α pour le scénario 3 **Escalade**

L'analyse des résultats montre que la prime moyenne évolue peu en fonction des valeurs de α. Cette observation est cohérente avec les analyses de sensibilité précédentes qui indiquaient que la variation de la prime est relativement faible lorsque la richesse initiale W_i^0 est importante.

En comparant un individu presque neutre au risque ($\alpha = 1$) à un individu très averse au risque ($\alpha < -3$), nous constatons que la différence de prime est d'environ 600€, ce qui représente une variation de l'ordre de 0,5% à 2% pour chaque scénario étudié.

Ainsi, nous pouvons conclure que la variation du coefficient α n'a pas d'impact significatif sur le calcul de la prime moyenne. Par conséquent, il est possible de considérer soit le pire cas, où l'entreprise est presque neutre vis-à-vis du risque, soit un cas où l'entreprise est très averse au risque, sans que cela n'affecte sensiblement les résultats obtenus.

4.4.6 Ajout de franchise à la tarification cyber

Ajoutons maintenant, dans notre garantie, les franchises calculées à partir des formules en 4.2.3. Nous choisissons la fonction CARA car plus facile à implémenter avec $\alpha = 0.5$ et $\lambda = 20\%$. Nous obtenons, pour les différents scénarios, les franchises suivantes :

Scénario	**Baseline**	**Maximum Historique**	**Escalade**
Grande Entreprise	440 280	536 423	789 964
Entreprise de Taille Intermédiaire	115 910	134 330	164 574
Moyenne Entreprise	74 392	78 386	82 393
Petite Entreprise	46 436	47 920	49 254

TABLE 4.7 : Franchises optimales moyennes selon la taille de l'entreprise et le scénario choisi

On remarque que la valeur des franchises augmente avec un scénario plus prudent. De même, plus la taille de l'entreprise est importante, plus la franchise est élevée. Ces franchises, nous permettent ensuite de calculer des primes pures optimales selon ces engagements :

Scénario	**Baseline**	**Maximum Historique**	**Escalade**
Grande Entreprise	127 786	154 285	72 387
Entreprise de Taille Intermédiaire	25 532	39 645	46 168
Moyenne Entreprise	5 272	11 389	16 500
Petite Entreprise	1 800	4 312	6 355

TABLE 4.8 : Prime Pure Moyenne optimale par entreprises assurées et par scénarios

De la même manière qu'avec les franchises précédemment calculées, plus la taille de l'entreprise augmentent ou plus le scénario est prudent, plus la prime pure optimale est importante. Cependant, on remarque que pour les grandes entreprises et pour le scénario d'escalade, la prime pure optimale diminue. Ceci est due à la franchise importante, qui tend à faire baisser la prime pure optimale. En effet, comme une très grande franchise a été calculée (790 K€), ceci a une effet inverse sur la prime optimale : ce n'est plus la fréquence d'apparition du risque cyber qui dicte la croissance mais la haute franchise qui pousse à la baisse de la prime.

Nous observons également que les primes pures optimales observées sont inférieures à celles calculées en absence de franchises. Ce qui est logique : une franchise importante est un frein dans l'acceptation de la garantie par l'assuré, ce qui baisse la prime maximale qu'il serait prêt à placer. (cf 4.2.4)

4.5 Synthèse

Dans ces parties nous avons donc vu un modèle de tarification du risque cyber proposant une prime optimale sous franchise. Pour analyser nos résultats, nous pouvons établir un ratio Sinistre sur Primes (S/P) à partir de notre base de données. Voici ce que l'on obtient selon les différents scénarios.

Scénario	**Baseline**	**Maximum Historique**	**Escalade**
Grande Entreprise	127,47%	99,98%	181,91%
Entreprise de Taille Intermédiaire	110,58%	68,98%	56,07%
Moyenne Entreprise	89,12%	40,22%	27,04%
Petite Entreprise	132,48%	35,96%	24,07%

TABLE 4.9 : ratios S/P de la base de données

Nous pouvons observer une disparité dans les ratios S/P, les ratios S/P ont tendance à être plus élevés si la taille de l'entreprise est importante. Ceci s'explique car la marge de profit est moindre lorsque la richesse initiale (ou chiffre d'affaire dans notre modélisation) est élevée (voir 4.3.1). Nous remarquons aussi que le ratio S/P pour les grandes entreprises et pour le scénario d'escalade est particulièrement élevée, ceci étant due à la baisse de la prime optimale malgré la franchise élevée. Nous pouvons conclure que :

- Le scénario d'escalade, bien que plus prudent, n'est pas adapté pour les grandes entreprises, le scénario du maximum observé serait plus adapté.
- Le scénario Baseline est trop risqué et présente sur les différents type d'entreprises (sauf moyennes entreprises) des ratios S/P supérieurs à 100% et est donc à exclure.
- Plus l'entreprise est grande, plus la variation de ses ratios S/P selon les scénario est faible.

Il est important de noter que la prime calculée correspond à une prime pure. En réalité, une marge commerciale est ajoutée, ce qui entraîne une augmentation des primes et une diminution des ratios S/P. Par ailleurs, la prime calculée constitue, en théorie, le montant maximal qu'il est prêt à payer pour s'assurer. Toutefois, en pratique, l'assuré ne possédant pas une connaissance précise de son risque, il peut accepter une prime plus élevée.

Nous pouvons alors comparer avec les résultats présentés dans le rapport LUCY 2024 de l'AMRAE :

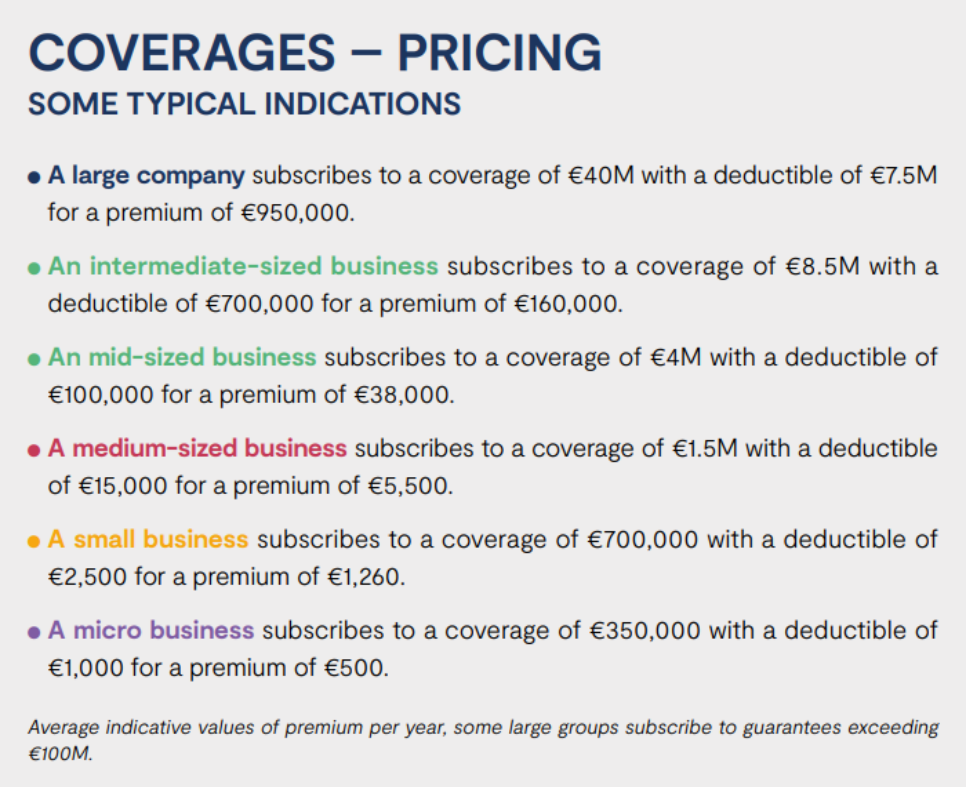

FIGURE 4.10 : Tableau récapitulatif du rapport LUCY 2024 de l'AMRAE

Plusieurs points sont à noter, tout d'abord les franchises et primes calculées sont en-dessous des franchises et primes présentées par l'AMRAE, ceci s'explique par plusieurs raisons : ces données présentées sont issues de l'année 2024 et non sur l'ensemble des données de l'étude, de 2019 à 2024. De plus, il est à noter que le ratio S/P de l'AMRAE sur l'année 2024 est de 12% et donc que les primes ont été fixées bien plus hautes que les sinistres survenus. Enfin, l'année 2024 sépare les entreprises de taille intermédiaire en deux, ce qui n'a pas été fait dans l'étude pour garder l'intégrité de la notation, de même pour les micro-entreprises. Pourtant, on peut voir que pour les entreprises de plus petite taille, moyennes et petites entreprise, le primes calculées raccordent avec celles du rapport.

Conclusion

Cette étude a mis en évidence que la tarification de l'assurance cyber est un domaine complexe, principalement en raison du manque de données disponibles, de leur difficulté d'accès et de leur qualité souvent moindre. Ces limitations résultent de plusieurs facteurs, notamment la difficulté de définir précisément le risque cyber, la réticence des entreprises à signaler les incidents et les évolutions constantes de la législation. Ces obstacles rendent le marché de l'assurance cyber particulièrement difficile à structurer et à stabiliser.

Les modèles micro-économiques se sont révélés être des outils efficaces pour estimer les primes d'assurance dans un contexte où les données sont limitées. En prenant en compte les comportements des entreprises et les risques auxquels elles sont exposées, ces modèles permettent de proposer des primes adaptées aux spécificités du marché tout en assurant la viabilité des assureurs. Grâce à ces approches, il est possible d'optimiser les décisions de tarification en tenant compte de l'incertitude et des différentes stratégies de protection adoptées par les entreprises.

L'étude a également montré que l'amélioration de la qualité des données passe par le croisement des différentes bases existantes. L'utilisation conjointe des bases VERIS et LUCY permet d'obtenir une vision plus complète du risque cyber, en compensant les lacunes de chaque source individuelle. Ce processus de consolidation des données offre des perspectives intéressantes pour affiner les modèles de tarification et proposer des solutions plus précises et adaptées au marché français.

En appliquant ces méthodes, nous avons pu constater que les primes optimales obtenues permettent de stabiliser les ratios sinistres/primes en fonction de la taille des entreprises. La différenciation des primes en fonction du niveau de risque et de la capacité financière des entreprises est essentielle pour garantir un équilibre entre accessibilité des assurances et rentabilité du secteur.

Cette étude a ainsi permis de proposer une nouvelle méthode de tarification cyber considérant la difficulté d'accès aux données dans un contexte assurantiel en constante évolution. La méthode développée intègre une garantie d'assurance prenant également en compte une couverture et une franchise optimale, permettant ainsi d'offrir aux entreprises une solution plus adaptée à leurs besoins et à leur tolérance au risque.

En perspective, la réassurance pourrait jouer un rôle clé dans l'amélioration de la tarification de l'assurance cyber. En partageant les risques avec des réassureurs, les assureurs primaires pourraient proposer des primes plus faibles, rendant l'assurance cyber plus attractive pour les entreprises de toutes tailles. De plus, la réassurance offre une capacité de couverture supplémentaire et une meilleure résilience face aux événements de grande ampleur, réduisant ainsi l'impact financier des sinistres majeurs.

Enfin, cette étude souligne la nécessité d'une coopération accrue entre les assureurs, les entreprises et les législateurs pour améliorer la collecte et l'exploitation des données, favoriser une meilleure prévention des risques et assurer la pérennité du marché de l'assurance cyber.

Bibliographie

AMRAE (2020 - 2024), 'Lumière sur la cyber assurance', https://www.amrae.fr/bibliotheque-de-amrae?combine=rapport%20lucy&ref_id=4022&ref_type=publication&items=4022&sort_by=created&sort_order=DESC&page=0.

Awiszus, K., Knispel, T., Penner, I., Svindland, G., Voß, A. & Weber, S. (2023), 'Modeling and pricing cyber insurance : Idiosyncratic, systematic, and systemic risks', *European Actuarial Journal* .

Banque de France (n.d.), 'Surveillance du risque cyber', https://www.banque-france.fr/fr/stabilite-financiere/cadre-institutionnel/systemes-paiement-infrastructures-marche/surveillance-risque-cyber.

Bastard, T. (2021), 'Modélisation du risque cyber de perte de données à caractère personnel, modèle de tarification, inclusion dans le bgs et proposition de scénarios de stress pour l'orsa', *Institut des Actuaire* .

Beugin, V. H. (2022), 'Quel budget les entreprises doivent-elles consacrer à la cybersécurité ?', *L'Usine Nouvelle* .

CESIN (2023), 'Baromètre de la cybersécurité des entreprises', https://cesin.fr/articles-slug/?slug=1432-8%C3%A8me+%C3%A9dition+du+barom%C3%A8tre+annuel+du+CESIN.

Deblock, F. (2022), 'Le marché de la cyber assurance en quête de maturité', *INCYBER News* .

Delelis, A. (2023-2024), 'Assurance cyber, un marché encore embryonnaire | risque cyber – de quoi parle-t-on ? lexique | assurance cyber, un cadre législatif encore incomplet | les données disponibles, défi majeur dans la gestion des risques cyber | assurance cyber, une modélisation actuarielle en plein essor', *Seabird* .

Duguet, E. (n.d.), 'Microéconomie de l'incertitude'.

Eling, M. & Schimt, J. T. (2012), 'Is there market discipline in the european insurance industry ? an analysis of the german insurance market', *The Geneva Risk and Insurance Review* .

Erling, M. & Loperfido, N. (2017), 'Data breaches : Goodness of fit, pricing, and risk measurement', *Econ Papers* .

Gouvernement Français (2023), 'Risques', https://www.gouvernement.fr/risques.

Jokung-Nguéna, O. (2001), 'Micro-économie de l'incertain'.

Marotta, A., Nanni, S., Orlando, A. & Yautsiukhin, A. (2017), 'Cyber-insurance survey', *Computer Science Review* .

North Bridge Assurance (n.d.), 'Qu'est-ce qu'un cyberrisque ?', https://www.northbridgeassurance.ca/blog/qu-est-ce-qu-un-cyberrisque/.

Annexe A

Variables et figures de l'étude

A.1 Tableau explicatif des différentes variables

TABLE A.1 : Description des Variables

Nom de la Variable	**Notation**
Probabilité d'incidence d'une attaque cyber associée à l'agent i	p_i
Richesse de l'agent i après la période d'assurance	W_i
Richesse initiale de l'agent i	W_i^0
Fonction d'utilité de l'agent i	U_i
Coût de l'autoprotection de l'agent i	C_i
Prime pure d'assurance de l'agent i	π_i
Prime pure minimale de l'agent i	π_i^{min}
Prime pure optimale de l'agent i	π_i^*
Profit de l'assureur sur l'agent i	Π_i
Profit optimal de l'assureur sur l'agent i	Π_i^*
Niveau d'autoprotection de l'agent i	x_i
Utilité espérée de l'agent i	$\mathbb{E}[U_i(W_i)]$
Couverture de la garantie cyber liée à l'agent i	X_i
Loterie (voir 2.4.1)	$\tilde{x}$
Option risquée d'une loterie	$\tilde{W_f} = W_i^0 + \tilde{x}$
Coefficient d'aversion absolu au risque de l'agent i	α_i
Coefficient d'aversion relative au risque de l'agent i	$\rho_i = 1 - \alpha_i$

A.2 Tableau des figures de l'étude

Table A.2 : Liste des tableaux et figures (Chapitre 1 et 2)

Numéro	Titre
Figure 1.1	Les différentes menaces cyber
Figure 1.2	Différentes attaques cyber survenues ces dernières années
Figure 1.3	Points clés du rapport de l'AMRAE
Figure 1.4	Évolution des ratios S/P du marché de l'assurance cyber
Figure 1.5	Évolution des ratios S/P du marché de l'assurance cyber pour les grandes entreprises de 2019 à 2023
Figure 1.6	Souscription d'une cyber assurance
Figure 1.7	Utilisation effective de la cyber assurance
Figure 1.8	Taux de dépôt de plainte après attaque
Figure 1.9	Taux d'identification post-attaque
Figure 1.10	Tableau présentant plusieurs garanties existantes sur le marché français
Table 1.1	Tableau de garanties risque cyber de la compagnie d'assurance Helvetia, disponible en ligne
Figure 1.11	Les différents points de la loi DORA
Figure 1.12	Garanties cyber et autorités de contrôle
Figure 2.1	Une fonction d'utilité et fonction d'utilité marginale associée
Figure 2.2	Arbre du risque de l'agent i sans assurance
Figure 2.3	Les différents types de marchés
Figure 2.4	Arbre représentant le risque de l'agent i avec assurance
Figure 2.5	Arbre représentant le gain de l'assureur assurant l'agent i
Figure 2.6	Les courbes des fonctions d'utilités CARA et CRRA pour différentes valeurs de alpha

Table A.3 : Liste des tableaux et figures (Chapitre 3)

Numéro	**Titre**
Table 3.2	Description variable *Type of breach*
Figure 3.1	Proportion des types d'attaques de la base PRC
Table 3.3	Description variable Type of organization
Figure 3.2	Proportion des types d'organismes attaqués de la base PRC
Figure 3.3	Proportion des pays des sinistres de la base VERIS
Figure 3.4	Répartition des sinistres VERIS par continent
Figure 3.5	Proportion des types d'attaques de la base VERIS
Table 3.5	Code NAICS pour les différents types d'organisations étudiés
Figure 3.6	Proportion des types d'organismes attaqués de la base VERIS
Figure 3.7	Comparaison de la temporalité des sinistres dans les deux bases de données
Figure 3.8	Comparaison des différentes base selon Bastard (2021)
Table 3.6	Les différentes catégories de sinistres
Table 3.7	Les différentes variables du rapport LUCY
Table 3.8	Exemple pour les Grandes Entreprises en 2019
Figure 3.9	Répartition des sinistres de la base LUCY selon l'année et le type d'entreprise
Figure 3.10	Répartition du nombre des différentes tailles de sinistres selon le type d'entreprise
Figure 3.11	Répartition du coût des différentes tailles de sinistres selon le type d'entreprise
Table 3.9	Répartition effectuée pour la taille des entreprises de la base VERIS
Figure 3.12	Répartition des valeurs de *victim employee count* pour un nombre d'employés inférieur à 1000 dans VERIS
Figure 3.13	Répartition des valeurs de *victim employee count* pour un nombre d'employés supérieur à 1000 dans VERIS
Figure 3.14	Évolution du nombre de sinistre par année selon les catégories d'entreprises de la base VERIS
Figure 3.15	Proportion des types de sinistres pour les grandes entreprises en 2021 pour les grandes entreprises selon la base LUCY
Figure 3.16	Évolution du coût total des sinistres de la base VERIS selon les années et le type d'entreprise
Table 3.10	Trois sinistres de la base de données résultante

TABLE A.4 : Liste des tableaux et figures (Chapitre 4)

Numéro	**Titre**
Figure 4.1	Éléments influant le calcul de la perte potentielle
Table 4.1	Caractérisation des entreprises i = 1, 2, 3
Table 4.2	Application numérique
Table 4.3	Franchises optimales calculées pour chaque entreprise en utilisant la fonction CRRA
Table 4.4	Prime optimale mise à jour pour chaque entreprise
Figure 4.2	Évolution de la prime optimale pour la fonction d'utilité $U(x) = ln(x)$
Figure 4.3	Évolution de la prime optimale pour les fonctions d'utilités CRRA et CARA en fonction du coefficient d'aversion au risque α
Figure 4.4	Fréquence d'apparition des sinistres en fonction de la taille d'entreprise
Figure 4.5	Les différents scénarios appliqués aux grandes entreprises
Table 4.5	Classification des entreprises selon leur chiffre d'affaires annuel selon LUCY
Table 4.6	Valeur de la richesse initiale selon la taille de l'entreprise
Figure 4.6	Primes pures moyennes de l'assurance cyber pour chaque type d'entreprise par année puis au global pour les différents scénarios et pour $U_i(x) = ln(x)$
Figure 4.7	Variation de la prime moyenne pour les grandes entreprises selon les valeurs de α pour le scénario 1 Baseline
Figure 4.8	Variation de la prime moyenne pour les grandes entreprises selon les valeurs de α pour le scénario 2 Pire Cas historiquement observé
Figure 4.9	Variation de la prime moyenne pour les grandes entreprises selon les valeurs de α pour le scénario 3 Escalade
Table 4.7	Franchises optimales moyennes selon la taille de l'entreprise et le scénario choisi
Table 4.8	Prime Pure Moyenne optimale par entreprises assurées et par scénarios
Table 4.9	ratios S/P de la base de données
Figure 4.10	Tableau récapitulatif du rapport LUCY 2024 de l'AMRAE