La cyber assurance et la gestion des risques cybernétiques: Analyse critique du premier produit lancé en Algérie

Cyber Insurance and Cyber Risk Management: A Critical Analysis of the First Product Launched in Algeria

BOUZIANE Souhila[1♦], LATRECHE Tahar [2]

[1] Laboratoire Reformes Economiques, Développement Stratégies D'intégration En Economie Mondiale, Ecole Supérieure De Commerce d'Alger (Algérie), s_bouziane@esc-alger.dz

ORCID: https://orcid.org/0009-0008-4470-5922

[2] Laboratoire Reformes Economiques, Développement Stratégies D'intégration En Economie Mondiale, Ecole Supérieure De Commerce d'Alger (Algérie), t_latrache@esc-alger.dz

ORCID: https://orcid.org/0009-0003-3439-0940

Reçu le:19/09/2024 **Accepté le:30/12/2024** **Publié le:20/01/2025**

Résumé :

Cet article vise à mettre en évidence le rôle de l'assurance dans la gestion des cyber-risques en analysant les contraintes et les opportunités liées à l'émergence du marché de l'assurance cyber en Algérie, avec un accent particulier sur le premier produit d'assurance cyber en Algérie lancé par la Compagnie Centrale de Réassurance (CCR), qui d'après notre étude analytique se distingue par ses conditions préalables claires, son adaptation au marché local, et ses partenariats internationaux.Toutefois, certaines faiblesses, comme les Critères de sélection de risque qui sont peu personnalisés, la standardisation des tarifs, et la complexité de la gestion des sinistres, nécessitent des améliorations. Des recommandations incluent: la création d'une plateforme de Cyber Self-Assessment pour déterminer la criticité du risque de l'entreprise, une tarification plus personnalisée, et la créattion d'une plateforme de gestion des sinistres en ligne, ont été proposées pour renforcer l'efficacité et l'attractivité du produit.

Mot clés: Cyber-risques, cyber-sécurité, cyber assurance, cyber attaques, Compagnies d'assurances

Abstract:

This study aims to highlight the role of insurance in cyber risk management by analysing constraints and opportunities associated with the emerging of the algerian cyber insurance market, with particular emphasis on the first cyber-insurance product in Algeria launched by the Central Reinsurance Company, which according to our analytical study is distinguished by its clear preconditions, its adaptation to the local market, and its international partnerships. However, some weaknesses, such as the poorly customized Risk Selection Criteria, the standardization of rates, and the complexity of claims management, require improvements.

♦ **Auteur correspandant** .

Ce(tte) œuvre est mise à disposition selon les termes de la Licence Creative Commons Attribution - Pas d'Utilisation Commerciale 4.0 International

Recommendations include: the creation of a Cyber Self Assessment platform to determine the risk criticality, more personalized pricing, and creation of claims management platform, are proposed to enhance product effectiveness and attractiveness.
Keywords: Cyber risk, cyber security, cyber insurance, cyber attacks, insurance companies

1. INTRODUCTION

Les compagnies d'assurance et de réassurance font face aujourd'hui à un environnement en évolution rapide, ce qui entraîne une incertitude croissante. La gestion des risques a toujours été un élément primordial pour les assureurs et a un rôle central dans leur gouvernance. Cependant, la nature du risque est devenue plus complexe, mettant en avant les risques émergents qui se réfèrent à des menaces nouvelles et changeantes, dont l'évaluation est complexe et susceptible d'avoir un impact important sur la société et l'industrie. Leur niveau de danger n'est souvent pas bien compris, rendant leurs implications difficiles à anticiper de manière fiable.

Depuis plusieurs années les risques liés aux cyber-attaques sont en tête de classement des risques émergents selon les études effectuées par les différents professionnels du risk-mangement qui évalue et classe chaque année leurs prévisions de l'émergence des risques. Ces risques suscitent une grande inquiétude pour les états et les oraganisations à travers le monde du fait de leur sévérité et de leur incidence économique sgnificative.

Par conséquent la gestion des risques liés à la cybernétique devient un enjeux majeurs pour les acteurs économiques, qui cherchent à minimiser son impact d'où l'émergence de la cyber assurance comme un outil efficace d'externalisation du risque.

Importance de l'étude: L'importance majeure de cet article réside dans l'impérative nécessité pour les entreprises et les organisations en Algérie de se protéger de manière efficace contre les risques considérables liés à la cybernétique. En effet, avec la recrudescence sans précédent des cyberattaques sophistiquées et des menaces en ligne pernicieuses, il devient impératif d'adopter une politique de cyber assurance robuste afin de préserver la durbilité des activités et de protéger de manière efficace les données sensibles et confidentielles. Ainsi, cette recherche s'attèle à explorer de manière approfondie les multiples implications cruciales de la cyber assurance dans le contexte spécifique de l'Algérie. Grâce à cette étude nous espérons apporter une contribution substantielle à la gestion proactive des risques liés à la cybernétique en Algérie et offrir des solutions innovantes pour faire face à ce défi majeur.

Problématique de l'étude: Nous essayons de donner une réflexion élargie à notre problématique centrale:

Comment les compagnies d'assurance algériennes peuvent-elles optimiser la gestion des risques cybernétiques en concevant des produits de cyber assurance mieux adaptés?

Pour répondre à cette question deux questions secondaires s'imposent:

- Quelles sont les défis et les opportunités auxquelles est confrontée l'émergence de l'assurance cyber en Algérie?
- comment les assureurs Algériens peuvent-ils adapter leurs produits et leurs stratégies pour bénéficier pleinement de ce risque émergent?
- Quelles sont les critères du produit de cyber assurance qui répond le mieux aux besoins des entreprises locales ?

Objectif de l'étude: cette étude vise d'apporter une contribution significative à la compréhension et à l'amélioration du premier produit d'assurance cyber en Algérie. Grâce à une analyse munitieuse des attributs du produit, de son adéquation par rapport aux exigences précises des entreprises algériennes, et en identifiant les éventuelles lacunes, des recommandations pratiques seront formulées pour optimiser l'adoption et la performance de ce produit dans un contexte algérien.

Méthodologie : Pour mener cette étude nous avons adopté dans notre étude la méthode descriptive pour décrire les différents aspects académique du thème et pour décrire le produit d'assurance cyber lancé par la CCR et l'approche analytiques pour examiner et évaluer notre produit.

Nous avons également utilisé divers outils et techniques de recherche pour recueillir et analyser les données comme les entretiens, la révision de documents. Ces outils seront employés de manière diversifiée pour obtenir des perspectives multiples et complètes sur le sujet de l'étude.

Plan du travail: Pour mener à bien cette étude, nous avons jugé pertinent de structurer notre recherche en trois parties distinctes. La première partie sera consacrée à l'exposition des risques cyber, en en analysant les menaces qu'ils représentent pour les entreprises. La seconde partie traitera la gestion de ces risques par l'instauration d'une politique de cyber sécurité solide, en mettant l'accent sur le rôle crucial de la cyber assurance dans cette démarche. Enfin, la troisième partie examinera en détail le premier produit d'assurance cyber lancé par la Compagnie Centrale de Réassurance (CCR), en évaluant ses caractéristiques, ses avantages, ainsi que ses limites.

2. Revue de la littérature

Les recherches antérieures sur le sujet de " **l'importance du cyberassurance dans la gestion des risques liés à la cybernétique"** constituent un élément essentiel pour comprendre les évolutions et les débats actuels sur ce thème. Leur revue offre une vue d'ensemble approfondie des recherches et des conclusions précédentes, contribuant ainsi à orienter l'étude actuelle et à identifier les lacunes dans les connaissances.

À travers cette partie, nous tenterons de passer en revue Problématiques traitées par la recherche en la matière, ainsi que les conclusions précédentes et les résultats clés. Cela constituera le fondement de l'analyse de notre recherche et appuiera l'orientation des conclusions à venir et des recommandations nécessaires. Voici une liste, non exhaustive, des études pertinentes:

- L'etude de Sasha Romanosky, Lillian Ablon, Andreas Kuehn et Therese Jones, 2019 intitulée « Content analysis of cyber insurance policies: how do carriers price cyber risk? " : cette étude visait à présenter une analyse thématique des polices d'assurance cyber déposées par les compagnies d'assurance auprès des régulateurs d'assurance des États unies, ainsi que des polices publiées publiquement sur les sites Web des assureurs.

Cette recherche a conclue l'existence d'une forte similarité dans les risques couverts, Les questionnaires de souscription ont révélé un équilibre approprié entre les questions techniques, organisationnelles, et procédurales, mais ont montré des lacunes dans la collecte

d'informations externes, comme les risques liés aux prestataires tiers. En ce qui concerne la tarification, une absence de la sophistication des modèles utilisés a été observée, certains utilisaient des méthodes simples, tandis que d'autres intégraient des paramètres plus complexes.

-Létude de Nir Kshetri, 2020 intitulée " The Evolution of Cyber-Insurance Industry and Market: An Institutional Analysis" cette étude avait pour objectif d'accroitre la compréhension de la Cyber assurance, qui est un domaine de recherche sous-exploité pour aider les organisations à gérer les cyber-risques plus efficacement. Une autre contribution est d'offrir une perspective sur les différents intervenants institutionnels, leurs initiatives et leur progression en ce qui concerne l'assurance cyber.
L'étude a révélé que les institutions progressent de manière à promouvoir le secteur de la cyber assurance, et que de nombreux défis actuels sont également susceptibles d'être surmentés grâce à l'introduction de nouvelles solutions technologiques.
Compte tenu que la majorité des organisations sont sous-assurées ou non assurées, les gouvernements devraient mettre en place des politiques visant à encourager l'adoption généralisée de la cyber assurance et les politiques doivent être clairement articulées de manière à motiver les entreprises à acheter des Cyber assurance.

-L'étude de Viktor Matejka et Juan Angel Huacan Soto, 2021 intitulée "A Framework for the Definition and Analysis of Cyber Insurance Requirements": l'objectif de cette étude était de proposer un cadre formel complet et conceptuel visant à aborder tous les processus et étapes déterminants de l'élaboration des polices d'assurance cyber en se basant sur les aspects importants d'autres modèles déjà présents sur le marché et est approuvé et validé par des experts du domaine de l'assurance cyber.
Cette étude a fini par proposer une méthode flexible et pratique pour le calcul de la prime basée sur un ensemble simple d'étapes qui peuvent être facilement appliquées dans différents contextes.
À travers l'examen des études antérieures, il est clair qu'elles convergent toutes vers un objectif commun : Traiter le théme de la cyber-assurance et sa contribution dans la gestion des risques cybernétiques. Cependant, elles se sont concentrées sur divers aspects comme la fixation des prix des produits d'assurance cyber, les procédures de souscription des contrats de l'assurance cyber et les tendances du secteur de la cyber assurance.
La plupart des recherches antérieures ont employé diverses méthodologies, comme l'étude de cas, les enquêtes auprès des assureurs et les interviews. Cependant, elles diffèrent dans les marchés étudiés.

La particularité de cette étude: réside dans le fait qu'elle est la première étude menée au niveau national en prenant en compte les particularités des entreprises et des compagnies d'assurance algériennes. Cette recherche se distingue aussi par son approche créatrice en formulant des recommandations pratiques et innovantes pour optimiser les produits d'assurance cyber et améliorer leur adéquation avec les besoins spécifiques des entreprises algériennes.

3. Les cyber-risques

Dans un monde de plus en plus numérique, où les entreprises sont fortement basées sur l'utilisation des systèmes informatiques, les risques liés aux cyber-attaques sont devenus une réalité inévitable. De ce fait tous les organismes, qu'ils soient publics ou privés, grands ou petits, sont constamment exposés à des attaques cybernétiques.

3.1. Définition du risque-cyber

Le risque cyber est un risque opérationnel associé à l'exécution d'activités dans le cyberespace, menaçant les actifs informationnels, les ressources TIC (Technologies de l'Information et de la Communication) et les actifs technologiques, et pouvant causer des dommages matériels aux actifs tangibles et intangibles d'une organisation, une interruption des activités ou une atteinte à la réputation. Le terme « risque cyber » inclut également les menaces physiques envers les ressources TIC au sein de l'organisation. (Strupczewski, 2021, p. 6)

La définition proposée met en avant les caractéristiques les plus importantes du risque cyber. Elles sont les suivantes :

- **Le risque cyber se situe dans la classe des risques opérationnels**.
- **Le cyberespace est la source la plus déterminante du risque cyber**, bien que parfois la cause de la matérialisation du risque puisse être physique (par exemple, un incendie dans une salle de serveurs ou des dommages accidentels à un câble réseau).
- Les objets exposés aux pertes causées par le risque cyber incluent : **les actifs informationnels** (par exemple, les données, les logiciels, les systèmes d'exploitation), **les ressources TIC** (par exemple, le matériel informatique, les systèmes de télécommunication, la vidéosurveillance), et **les actifs technologiques** (par exemple, les dispositifs contrôlés électroniquement, les chaînes d'assemblage, les systèmes informatiques industriels, les systèmes de transport, l'approvisionnement énergétique).
- Le risque cyber peut survenir aussi bien dans un **appareil informatique isolé** ou dans des **réseaux informatiques locaux**, que dans des systèmes informatiques vastes, interconnectés et interdépendants, y compris **l'Internet**.
- **L'impact potentiel du risque cyber peut être triple**:

1- **Dommages matériels**, signifiant non seulement des pertes matérielles, mais aussi l'obligation d'indemniser les dommages causés à des tiers en cas de violation de données (responsabilité civile), ainsi que la perte de bénéfices due à un dysfonctionnement du système informatique ;
2- **Perturbation des opérations d'une organisation** (sans perte financière directe) ;
3- **Atteinte à la réputation**, pouvant être associée à une perte de confiance des clients et à d'autres conséquences négatives pour l'entreprise.

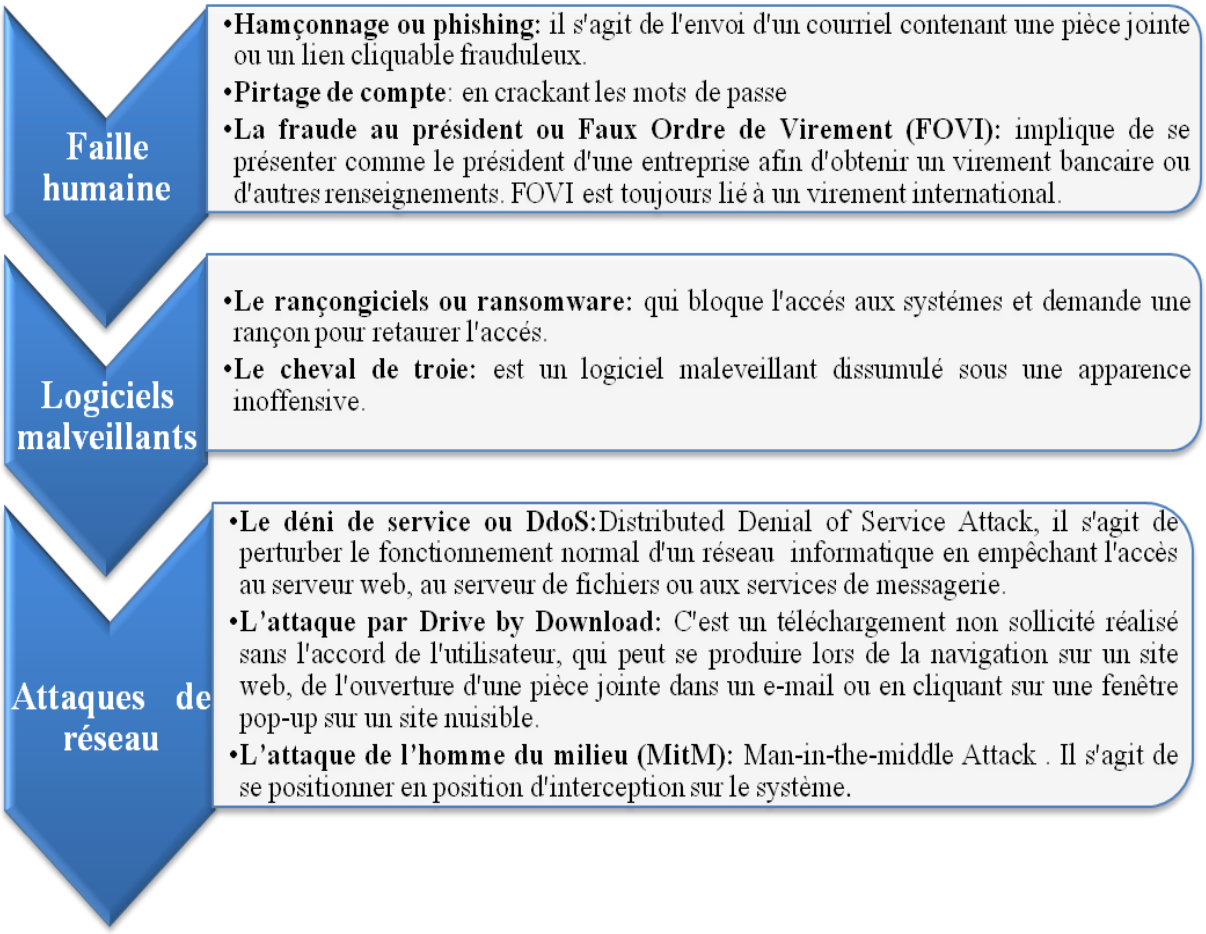
En résumé, le risque cyber se situe dans le cyberespace, mais il impacte non seulement le monde virtuel, mais aussi le monde physique. Ce terme fait référence à une série

d'événements susceptibles de causer des dommages ou d'affecter de manière indésirable les données numériques et les ressources TIC des entreprises, des individus ou des institutions.

3.2. Typologie des cyber-risques fréquents

On peut distinguer trois grandes familles de cyber risque:

Figure N°1: Cyber risques les plus fréquents



Source : élaborée par nos soins à partir du rapport de Tunis-Re, risques émergents 2éme édition P23. (ksouma, 2024, p. 24)

Les entreprises sont confrontées à divers types de menaces et attaques cybernétiques, notamment le phishing ou l'ingénierie sociale visant à obtenir des informations confidentielles ou pour effectuer des transactions frauduleuses. Les ransomwares sont également une menace croissante, en chiffrant les données de l'entreprise pour exiger une rançon en échange pour les décrypter. Les attaques DDoS affectent aussi les entreprises en surchargeant ses serveurs pour perturber les opérations normales d'une entreprise.

En outre, les cybercriminels exploitent souvent les vulnérabilités des systèmes informatiques des organisations pour obtenir un accès aux informations sensibles ou pour perpétrer des actes de fraude.

Dans ce qui suit quelque cyber attaques marquantes durant les huit dernières années:

Figure N°2: Quelques attaques cyber au cours des 8 dernières années

Source: Gavėnaitė-Sirvydienė,2019, Evaluation of cyber insurance ass a risk management tool providing cyber security, Social Transformations in Contemporary Society, p88

Le Ransomware constitue le risque le plus avéré, En 2017, l'industrie de l'assurance a été confrontée à une menace majeure de ransomware Les noms de ces virus malveillants sont connus sous les attaques de malwares Petya, NotPetya et WannaCry. Ces programmes dangereux ont infecté des logiciels informatiques dans plus de 150 pays, touchant divers secteurs d'activités. Il est très difficile de calculer la perte globale finale et exacte causée par ces cyberattaques, mais on estime qu'environ 10 milliards de dollars ont été causés par NotPetya, et le virus WannaCry a entraîné des pertes de 4 milliards de dollars. **(Gavėnaitė-Sirvydienė, 2019, p. 88)**

Les cyberattaques ont engendré une perte de 8.000 milliards de dollars à l'économie mondiale en 2023, et ce chiffre devrait grimper à 9.500 milliards en 2024 pour dépasser les 10.000 milliards de dollars en 2025. Ce montant équivaut presque au PIB de l'Union européenne. Les régions les plus affectées par ces attaques sont les États-Unis (46% des attaques), suivis du Moyen-Orient (Sini, 2024).

4. La gestion des cyber risques

De nos jours, le monde fait face à une exposition croissante aux risques cybernétiques, avec une dépendance croissante aux technologies numériques dans la collecte le stockage et le traitement d'un grand nombre de données clients. En effet la gestion des cyber-risques devient une nécessité incontournable.

4.1. La cyber-sécurité

Les systèmes et les services accessibles via l'espace numérique peuvent être vulnérables et être une cible d'attaques cybernétiques. L'avènement d'Internet a introduit de nouvelles menaces qui peuvent engendrer des risques variés en termes de cybersécurité, lesquels peuvent avoir un impact sur les individus, les entreprises privées et publiques, ainsi que sur les États.

La cybersécurité s'applique à tous les environnements numériques qui sont connectés à Internet, visant à protéger les données et les réseaux de communication. (Ghernaouti, 2022, p. 2)

4.1.1. Définition

La cyber-sécurité désigne:« Les stratégies, politiques, et normes couvrant l'ensemble des activités visant à atténuer les menaces, réduire les vulnérabilités, dissuader les attaques, s'impliquer à l'échelle internationale, intervenir en cas d'incident, consolider la résilience et restaurer les systèmes, ainsi que les politiques pertinentes en matière de sécurité des opérations» (IAIS, 2018, p. 7)

La Résolution 181 de l'UIT (Union internationale des télécommunications), adoptée en 2010 à Guadalajara, a approuvé la définition de la cyber sécurité telle que prévue par la Recommandation UIT-T X.1205

" la cyber-sécurité est l'enemble d'outils, de politiques, de concepts de sécurité, de mesures de protection, de lignes directrices, d'approches de gestion des risques, d'actions, de formations, de meilleures pratiques, d'assurances et de technologies pouvant être utilisées pour protéger l'environnement cybernétique ainsi que les actifs des organisations et des utilisateurs."

Autrement dit la cyber sécurité consiste à instaurer un éventail de méthodes et de dispositifs de sécurité visant à protéger les données depuis leur création et traitement jusqu'à leur transfert, stockage, et destruction.

4.1.2. Objectifs

Les objectifs de cyber sécurité comprennent les suivants : (Saudi Arabian Monetary Authority, 2017)

- **Confidentialité**: Les données sensibles sont accessibles uniquement aux personnes autorisées.
- **Intégrité**: Les actifs d'information sont précis, complets et traités de manière appropriée, garantissant leur protection contre toute modification non autorisée, y compris l'authenticité et la non-répudiation.
- **Disponibilité**: Les actifs d'information sont résilients et disponibles lorsque nécessaire, protégés contre toute interruption non autorisée.

Avec l'augmentation des cyber-attaques et la numérisation croissante, la cyber sécurité est devenue un enjeu crucial pour les entreprises en Algérie, tout comme dans le reste du monde.

4.2. La cyber assurance

Face aux risques croissants des cyber-attaques les compagnies d'assurances cherche à s'adapter en offrant une assurance cyber.

La cyber assurance est un domaine relativement récent dans le domaine de l'assurance dommages. Les différents intervenants du marché n'ont pas encore standardisé les conditions générales des polices cybers.

Actuellement, ce secteur de l'assurance dommages se distingue par l'insuffisance de données statistiques, la dimension systémique du risque, et le potentiel d'accumulation des pertes. Il est difficile pour les assureurs de chiffrer leur engagement et de tarifer le produit en raison de ces particularités. En outre, l'aspect global du risque pose un défi en termes de capacité d'assurance et de réassurance.

4.2.1. Définition

« L'assurance cybernétique est une méthode de transfert des risques, qui peut améliorer ou non la cyber-sécurité des entreprises » (KHALILI & NAGHIZADEH, 2017, p. 1)

« La cyber assurance permet aux entreprises de transférer une partie du risque financier associé aux incidents informatiques à une compagnie d'assurance ». (Lawrence, Martin, & Tashfeen, 2003, p. 83)

Autrement dit c'est une assurance qui aide les entreprises à gérer les risques associés aux activités cybercriminelles, comme les cyberattaques et les violations de données. Les menaces en ligne qui compromettent l'infrastructure informatique des organisations engendrent des coûts importants, généralement couverts par les contrats de responsabilité civile standard ou les assurances traditionnelles. La cyber-assurance permet de protéger les organisations contre les couts liés aux cyber-attaques.

4.2.2. Risques couverts

La cyber assurance Couvre l'assuré pour les frais engagés (réparation et dépenses supplémentaires), les pertes d'exploitation et les coûts associés à la gestion de crise, ainsi que les conséquences des réclamations mettant en cause sa responsabilité civile (CCR, 2018, p. 5). Elle peut couvrir un large eventail de risques, notamment:

- La responsabilité civile en cas de violation de données,
- Les coûts de communication aux parties impliquées,
- La restauration des données endommagées ou perdues,
- Les pertes d'exploitation résultant d'une indisponibilité du système,
- Les dépenses liées à la réputation et à la restauration après un incident, ainsi que les demandes de rançon en cas d'extorsion cybernétique ou de vol de données confidentielles.

En outre, la cyber-assurance peut offrir une assistance juridique et des services de surveillance et d'analyse des cyber-menaces pour assister les entreprises à l'identification, la neutralisation et l'attribution des cyber-attaques En adoptant une approche holistique de la gestion des risques en cybersécurité.

Certains cyber-risques sont toutefois considérés comme non couverts en raison du potentiel d'accumulation des risques. Ce risque d'accumulation se manifeste par la défaillance d'une infrastructure affectant une grande communauté de clients, ce qui engendre une forte exposition aux pertes d'exploitation. Par exemple, une attaque ciblant un serveur DNS ou un domaine pourrait provoquer une interruption généralisée des activités, notamment dans le secteur du commerce électronique. (Henda & Naimi, 2020, p. 34)

Les cyber guerres sont aussi des risques souvent exclus et qui peuvent être rachetable. Ce sont des attaques destructrices à but politique qui visent à saboter et à espionner. (Henda & Naimi, 2020, p. 36) tel que la guerre entre la Russie et l'Ukraine

4.2.3. Rôle de la cyber-assurance

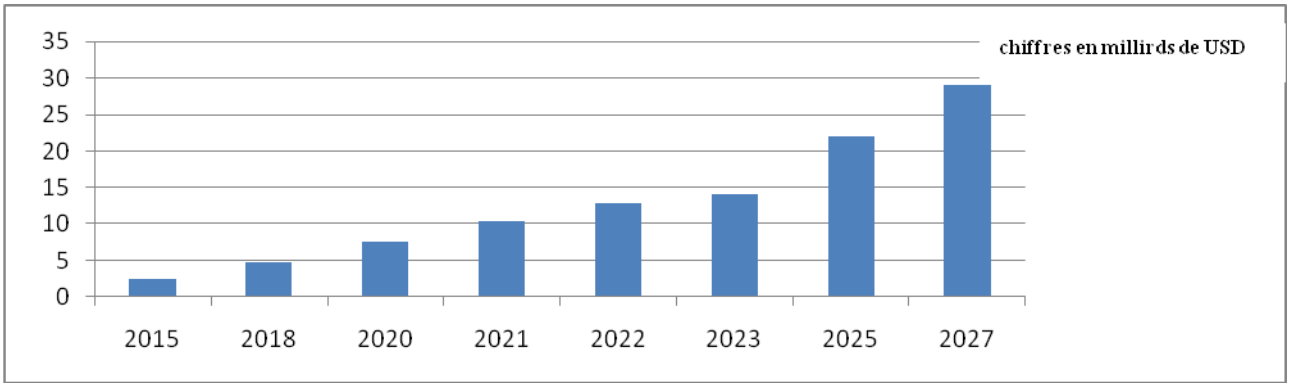
Sur le plan de la gestion des risques, l'utilisation de l'assurance cybernétique peut être essentielle pour renforcer la résistance globale de la sécurité des entreprises contre les cybermenaces. (Hausken, 2020, p. 3). L'assurance cybernétique peut fournir aux entreprises une protection financière contre les pertes potentielles résultant d'incidents informatiques, y

compris les violations de données, les cyberattaques et d'autres activités malveillantes (CREMER, SHEEHAN, & MULINS, 2024, p. 3).
Avec l'assurance cyber, une partie importante de l'exposition cyber d'une entreprise peut être transférée à une compagnie d'assurances en achetant une police d'Assurance cybers. (TALESH, 2018, p. 426).
En outre, l'adoption de l'assurance cybernétique peut encourager les entreprises à améliorer leur position en matière de cybersécurité, car les assureurs exigent souvent que les entreprises respectent des normes de sécurité spécifiques en tant que condition de couverture. (Sullivan, & Nusen 2020).

4.2.4. Le marché mondiale de la cyber assurance

L'industrie mondiale de l'assurance cyber est en plein essor, en 2023, les primes mondiales de l'assurance cyber ont atteint 14 milliards de dollars, affichant un taux d'augmentation de 9.37% par rapport à l'exercice 2022. Le marché projette d'atteindre 29 milliards de dollars d'ici 2027 (Munich Re, 2024).

Graphique N° 1: Evolution des primes cybers: 2015-2027



Source: Munich-Re,2024, Cyber insurance:risks and trends 2024

L'augmentation des primes est dû à:

- L'augmentation des tarifs en réponse à l'accroissement des attaques par ransomware, ce qui a entraîné une hausse des taux de sinistres au cours des années précédentes.
- l'amélioration des couvertures destinées aux petites et moyennes entreprises (PME),
- L'augmentation de la fréquence et la compléxité des cyber-attaques,
- la transition numérique et les avancés technologiques dans toutes les activités,
- Le renforcement des exigences réglementaires en matiére de cyber-sécurité.

Le marché de l'assurance cybernétique a presque triplé au cours des cinq dernières années. Toutefois, à ce jour, seule une fraction des risques ont été assurés. Les grandes entreprises constituent la part de lion des primes; les petites et moyennes entreprises (PME) assument elles-mêmes la majeure partie de leurs risques cyber.
Les assureurs sont confrontés à un défi majeur dans leurs efforts visant à combler l'écart entre les pertes économiques et celles assurées. Compte tenu de la croissance très dynamique des risques dans une économie numérisée, une plus grande pénétration de l'assurance pour les risques cyber est l'objectif premier.

5. La cyber assurance en Algérie

Le marché de l'assurance cyber en Algérie est en phase de développement, mais il suscite un intérêt croissant en raison de l'augmentation des risques liés à la cybernétique. À mesure que les entreprises algériennes se numérisent et que l'économie se digitalise, la nécessité de se protéger contre les cyberattaques devient cruciale.

5.1. Contraintes et atouts de l'émergence du marché algérien de la cyber assurance

Le marché algérien de la cyber assurance fait face à des des défis et des opportunités qui peuvent influencer son émergence:

Tableau N°1:Contraintes et atouts de l'émergence du marché algérien de la cyber assurance

Les contraintes	Les atouts
- Manque de données et d'expertise locale: L'Algérie, comme beaucoup de pays en développement, manque de données historiques sur les cyber attaques et d'expertise locale en cyber sécurité. Cela complique la tâche d'évaluer avec précision les risques, de fixer les prix des primes et de concevoir des produits d'assurance appropriés. - **Faible sensibilisation et culture de la cyber assurance:** La sensibilisation aux cyber-risques reste faible chez les entreprises algériennes, en particulier les PME. Ce manque de sensibilisation se traduit par une faible demande pour l'assurance cyber et une sous-estimation des risques. **-Cadre juridique et réglementaire en développement:** Le cadre législatif et réglementaire concernant la cybersécurité et la protection des données est encore en développement en Algérie. Ce manque de clarté peut créer des incertitudes pour les assureurs et freiner l'innovation. **- Manque d'infrastructures technologiques robustes:** Le développement rapide de l'économie numérique en Algérie n'a pas toujours été accompagné d'investissements suffisants dans des infrastructures technologiques robustes et sécurisées. Cela augmente la vulnérabilité aux cyber attaques.	**-Marché en croissance exponentielle:** La digitalisation croissante de l'économie algérienne et la multiplication des cyberattaques créent une demande croissante pour l'assurance cyber. Les compagnies d'assurance qui sauront s'adapter rapidement à ce marché émergent bénéficieront d'un avantage concurrentiel. **-Potentiel de diversification des produits:** Les cyber-risques sont complexes et multiformes. Cela donne aux compagnies d'assurance la possibilité de concevoir de nouveaux produits d'assurance pour répondre aux exigences spécifiques des entreprises algériennes. **-Rôle de leader dans la sensibilisation à la cybersécurité:** Les compagnies d'assurance ont la capacité d'influer grandement sur la sensibilisation aux dangers de la cybernétique et la promotion des bonnes pratiques de sécurité en matière de cybernétique chez les entreprises en Algérie. **-Collaboration stratégiques:** La complexité des cyber-risques exige une approche collaborative, où les assureurs peuvent établir des partenariats stratégiques avec des entreprises de cybersécurité, des institutions gouvernementales et des organisations internationales afin de mutualiser les connaissances.

Sources: Elaboré par nos soins

Plusieurs compagnies s'apprêtent à lancer de nouveaux produits d'assurance cyber, dont la CCR (Compagnie Centrale De Réassurance), qui a développé récemment un produit

d'assurance cyber, spécialement conçu pour le marché algérien. Dans ce qui suit nous analyserons les caractéristiques de ce produit.

5.2. Analyse descriptive du premier produit d'assurance cyber destiné au marché algérien: CCR Algérie

La Compagnie Centrale de Réassurance (CCR) est le seul réassureur national détenu à 100% par le ministère des finances qui a pour missions de fournir la réassurance aux assureurs locaux et assister le développement de nouveaux produits.

La CCR a lancé récemment un produit d'assurance cyber à ses assureurs destiné aux Petites Et Moyennes Entreprises (PME) comme premier produit d'assurance cyber adapté au marché algérien et qui asure les cyberattaques ciblant les données, les logiciels et les Systèmes d'information étendu à la responsabilité civile cyber.

- **Marché cible:** PME dont le chiffre d'affaires ne dépasse pas les 4.000.000.000DA avec un effectifs maximum de 250 employés.
  Les PME sont souvent perçues comme des cibles plus faciles pour les cybercriminels en raison de leurs ressources limitées en cyber sécurité ce qui fait de l'assurance cyber un outil essentiel pour leur protection.
- **Partenaires**: qui ont fournit en collaboration avec la CCR les dispositifs de souscription et de fixation des tarifs.

Tableau N°2: partenaires internationaux de la CCR pour la conception du produit de la cyber-Assurance

GALLAGHER	Courtier d'assurance mondial et conseiller de gestion du risque et du capital qui a la plus large équipe dédiée au cyber du marché.
SCOR	Réassureur mondial de premier plan
ENVELOP	une société de souscription d'assurance cyber qui utilise des analyses avancées, l'apprentissage automatique et l'intelligence artificielle pour évaluer et tarifer les risques cyber de manière plus précise
STELLIANT	prestataire de services d'assurance international situé en France, spécialisé dans la gestion des risques, l'expertise en sinistres, et les solutions post-sinistre

Source: élaboré par nos soins à partir des données de la division Re-takaful et risques émergents

- **Conditions préalables à la couverture**

- Maintenir à jour un logiciel antivirus sur tous les appareils de l'assuré
- Veiller à ce que tous les appareils de l'assuré soient protégés par des pare-feux
- Mettre en œuvre des contrôles d'accès pour empêcher tout accès non autorisé
- Sauvegarde mensuelles et stocker ces sauvegardes dans un environnement cloud ou à un emplacement hors site et déconnecté.

- **Risques couverts**

Restauration de données: Les frais de restauration des données comprenant les honoraires, coûts et dépenses que l'assuré engage, avec accord écrit préalable de l'assureur, pour rétablir l'accès à ses données, ou pour récupérer, restaurer, saisir, configurer et/ou remplacer ses données, qui ont été corrompues, effacées, chiffrées, endommagées ou détruites.
Responsabilité Civile: Les dommages que l'assuré est légalement tenu de payer tels que les jugements, sentence ou règlement pécuniaire ainsi que les honoraires, coûts, dépenses engagés dans le cadre de l'enquête, du règlement, de la défense et de l'appel d'une déclaration de sinistre.

- **Exclusions**

Restauration de données: Actes malhonnêtes, électromagnétique, tout paiement en relation avec une tentative d'extorsion, infrastructure, radioactivité, risque physique, dommages matériels, guerre, usure et détérioration.
Responsabilité Civile: Dommages corporels, obligations des administrateurs, actes malhonnêtes, infrastructure, insolvabilité, risque physique, reprise du passé, dommages matériels, partie liée, sanctions, infractions à la loi.

- **Tarification des couvertures :** Les produits de cyberassurance de la CCR sont élaborés à partir de modèles de tarification ajustés en fonction des sinistres cyber observés sur le marché. Les données relatives aux sinistres et les informations sur les polices dans la région MENA (Middle East and North Africa) ont été utilisées dans le cadre de l'analyse pour créer des facteurs de tarification spécifiques pour l'Algérie et les produits cyber de CCR.

Les tarifs proposés sont les plus compétitives possibles. Cela permettra un déploiement réussi de ces couvertures cyber par les clients de CCR auprès de leurs assurés, La CCR a standardisé en effet une grille tarifaire en fonction de la limite de garantie à savoir:

Tableau N°3:Table des tarifs de l'assurance cyber

Limite de garantie DZD	Restauration de données DZD	Responsabilité Civile DZD
500.000	2.370	2.370
1.000.000	2.489	2.939
1.500.000	2.963	3.556
2.500.000	4.463	5.356
5.000.000	8.300	9.960

Source: Division RE-Takaful et Risques émergents de la CCR

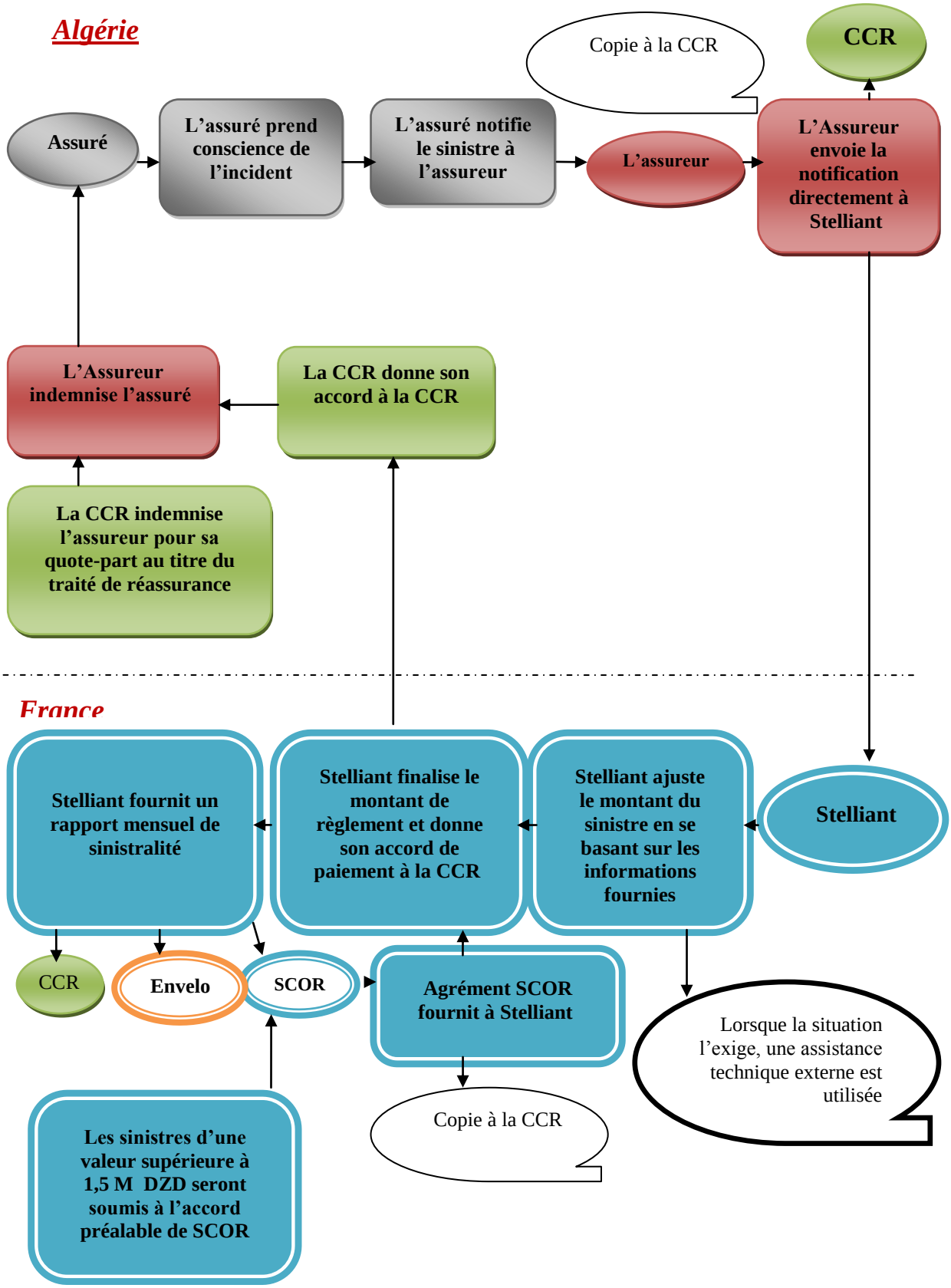
La CCR a introduit un produit simple avec des limites fixes et modestes pour stimuler la demande et éduquer le marché.

- **Gestion des sinistres :** Pour permettre le traitement du dossier sinistre le gestionnaire du sinistre doit réunir toutes les pièces et informations permettant de procéder à l'application du contrat et à l'éventuelle indemnisation de l'assuré et/ou des tierces victimes :

- La déclaration initiale du sinistre
- Les éventuels rapports d'expertise
- Tous les documents nécessaires à L'évaluation et la décision concernant le sinistre
- La détermination des tiers responsables, de leurs assureurs
- La présentation de la réclamation aux tiers responsables
- Les relances par tous moyens disponibles
- La présentation des propositions de règlement pour validation et règlement par le courtier
- La transmission des accords de règlement des recours
- La cloture

La figure suivante montre que la gestion des sinistres cybers passe par plusieurs étapes et implique l'intervention de plusieurs parties nationales et internationales à l'instar du cabinet d'expertise français Stelliant qui procède à l'expertise des dégâts et arrête le montant des dommages après l'accord préalable de la SCOR.:

Figure N°3: processus de gestion des sinistres cybers par la CCR



Source: établi par nos soins à partir des données de la division Re-takaful et risques émergents de la CCR

5.3. Analyse Critique du Produit d'Assurance Cyber de la CCR : Points Forts et Axes d'Amélioration

Le tableau ci-dessous présente une analyse équilibrée du produit d'assurance cyber lancé

Tableau N°4: Points forts et axes d'amélioration

Points forts	Points faibles
-Conditions Préalables Claires : Les conditions préalables à la souscription, comme la mise à jour fréquente des antivirus et la sauvegarde des données, incitent les entreprises à mettre en place les bonnes pratiques en cybersécurité, réduisant ainsi leur exposition aux risques. -**Adaptation au Marché Algérien**: Le produit est spécifiquement conçu pour répondre aux besoins des PME algériennes, avec des limites de couverture ajustées à leur envergure et à leurs capacités financières. De plus, la couverture intègre des éléments essentiels comme la restauration des données et la responsabilité civile. qui sont essentiels pour les PME souvent vulnérables aux cyberattaques. -**Partenariat avec des Experts Internationaux** La collaboration avec des partenaires internationaux tels que Gallagher, SCOR, Envelop et Stelliant renforce la crédibilité et l'efficacité du produit. -**Tarification Compétitive et Standardisée**: La grille tarifaire simple et compétitive rend le produit attractif pour les PME, facilitant son adoption sur le marché. La tarification est basée sur des données spécifiques à la région MENA, assurant une adéquation avec les risques locaux. - **La procédure de gestion des sinistres:** est rigoureusement structurée et implique l'expertise de spécialistes internationaux, ce qui garantit une gestion efficace des réclamations. L'implication de Stelliant pour l'expertise des sinistres garantit une estimation professionnelle des dommages.	**Les critères de sélection de risque uniforme** ne tiennent pas compte de la diversité des profils de risque, ce qui peut entraîner une sous-évaluation des risques pour certaines entreprises avec des vulnérabilités spécifiques ou une surévaluation pour celles disposant de mesures de sécurité plus avancées. En outre, l'imposition de critères stricts pour l'obtention de la couverture peut exclure les PME les plus exposées aux risques cyber, mais manquent des ressources ou des connaissances nécessaires pour mettre en place immédiatement les mesures de sécurité exigées. Cela contredit l'objectif fondamental de l'assurance cyber, de protéger les entreprises les plus vulnérables. **-La standardisation des tarifs**: Bien que bénéfique pour la simplicité, pourrait ne pas refléter les risques de chaque PME et peut entraîner le risque de sélection adverse. **-Limites de Garantie Relativement limitées**: Les limites proposées peuvent être insuffisantes pour certaines PME qui pourraient faire face à des cyberattaques plus graves, nécessitant des couvertures plus étendues. Cela peut limiter l'attrait du produit pour des entreprises avec des besoins de couverture plus importants **-Absence d'Options Personnalisées** :Le produit actuel n'offre pas de flexibilité pour personnaliser les limites de garantie ou ajouter des options supplémentaires, ce qui pourrait limiter son attrait pour des entreprises ayant des besoins particuliers. - **Complexité dans le traitement des sinistres**:La gestion des sinistres implique plusieurs parties prenantes, dont certaines sont internationales, ce qui pourrait compliquer et rallonger le processus de traitement des réclamations.

Source : élaboré par nos soins

Le produit de la CCR est bien adapté aux besoins généraux des PME algériennes, mais nécéssite plusieures axes d'améliorations le rendant plus rentablable pour les assureurs et plus attractif pour les entreprises.

5.4. Recommandations et orientations pour améliorer le produit

Dans ce qui suit nous donnons quelques recommandations pour l'amélioration du produit d'assurance de la CCR

5.4.1. Sélection des risques à travers une plateforme de Cyber Self Assesment et la cartographie des parties prenantes

Pour optimiser la sélection des risques en adéquation avec le profil de risque des entreprises, nous suggérons à la CCR de créer en collaboration avec ses partenaires internationaux une plateforme de CyberSelf Assesment, une plateforme interactive qui permet aux PME d'évaluer elles-mêmes leur niveau de risque cyber (MAHBOULI, 2022, p. 45), fournissant ainsi à la CCR des données précises et à jour permettant de cartographier les parties prenantes (MATEJKA, 2021, p. 85) pour une tarification et une couverture plus adaptées.

La plateforme propose un questionnaire structuré couvrant plusieurs domaines critiques de la cybersécurité : (ROMANSKY, ABLON, & KUEHAN., 2019).

Organisation : Questions sur l'indistrie, et la situation financière de l'entreprise

Contrôle des Accès : Questions liées à l'authentification multifactorielle et aux politiques de gestion des identités

Mises à Jour Logicielles : Gestion et cadence des mises à jour des systèmes et logiciels.

Sécurité des Données : Mesures de sauvegarde des informations, et protection des données sensibles.

Formation et Sensibilisation : Mise en place de programmes de formation destinés aux employés en matière de cyber sécurité.

Historique des Incidents : Répartition des incidents antérieurs et réponses aux cyber attaques.

Les plans d'intervention en cas d'incident: Préparation à la reprise des activités en cas de sinistre majeur.

A travers ce questionnaire la CCR procède à cartographier chaque risque cyber à couvrir des parties prenantes (les entreprises) ,en s'appuyant sur la méthode des matrices d'évaluation de la criticité du risque. (Merad, 2004) (ACHOURI, 2009, p.17) en procédant comme suit :

1-**Déterminer la criticité brute du risque:** En analysant la fréquence et l'impact de chaque type de risque qu'elle envisage de couvrir (tel que la violation des données, le phishig…ect) sur la partie prenante selon le tableau suivant:

Tableau N°5 : Fréquence et impact du risque sur la partie prenante

Code	Fréquence	Impact
1	Jamais produit et improbable	Modéré
2	Jamais produit dans le passé mais reste probable	Significatif
3	Peu fréquent: Déjà produit une fois depuis 2 à 3 ans	Important
4	Fréquent: Déjà produit une fois dans l'année écoulée	Très important

Source : élaboré par nos soins en collaboration de la division Re-takaful et risques émergents

Pour déterminer ensuite le niveau de la criticité brute du risque qui est le résultat de la cotation du risque sur les deux échelles précédentes. L'association de ces deux paramètres permet de dégager l'évaluation du risque brut, tel qu'il est mentionné sur la matrice suivante:

Tableau N°6 : Matrice de Criticité brute du risque cyber de la partie prenante

Fréquence	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
	Impact				

Source : élaboré par nos soins en collaboration de la division Re-takaful et risques émergents

La criticité brute du risque=la fréquence du risque*l'impact du risque

2- Évaluer le niveau des mesures d'atténuation : Stratégies ou dispositifs mis en œuvre pour réduire ou gérer le risque (tel que: l'automatisation des processus, mise à jour rapide des systémes…). en se basant sur le tableau suivant :

Tableau N°7 : Niveau de la cyber sécurité de la partie prenante

Code	Mesures de mitigation
1	Avancées
2	Modérées
3	Faibles
4	Initiales ou inexistantes

Source : élaboré par nos soins en collaboration de la division Re-takaful et risques émergents

3- Déterminer la criticité nette du risque : l'évaluation de criticité nette du risque tient compte le degré de maturité en matiére cyber sécurité de l'entreprise

Criticité nette du risque=criticité brute-Mesures de mitigation

Tableau N°8: Echelle de criticité nette du risque cyber de la partie prenante

Echelle de la criticité		Description de la criticité
1-3	Faible	L'entreprise est bien protégée et pourrait bénéficier d'une prime réduite
4-7	Modéré	Une couverture standard est recommandée, avec des ajustements selon les risques spécifiques.
8-11	Elevé	Des mesures supplémentaires de cybersécurité sont conseillées avant d'offrir une couverture complète.
9-12	Critique	L'entreprise pourrait être refusée ou se voir offrir une couverture limitée avec des primes élevées.

Source : Elaboré par nos soins en collaboration de la division Re-takaful et risques émergents

Après l'évaluation, les entreprises cartographié reçoivent un rapport personnalisé qui détaille leur niveau de risque et fournit des recommandations spécifiques pour améliorer leur cybersécurité.

Par ailleurs La création d'une plateforme de Cyber Self Assessment représente une avancée significative pour la CCR dans l'amélioration de la sélection des risques. Ce système permet d'une part l'identication plus précise du profil de risque, et d'autre part d'optimiser la tarification et la couverture proposées en fonction des données recueillies. Grâce à une évaluation rigoureuse et à l'utilisation de matrices de criticité, la CCR peut adapter ses offres en fonction du niveau de maturité en cybersécurité de chaque entreprise, renforçant ainsi la pertinence et l'efficacité de ses produits d'assurance cyber.

5.4.2. Une tarification plus équitable

Nous proposons dans ce qui suit un modèle simplifié et flexible qui peut être utilisé comme base pour estimer une prime d'assurance; en l'absence de donnée historique (MATAEJKA, 2021, p. 45) nous avons essayé d'introduire plusieurs facteurs, tels que la taille de l'entreprise, le secteur d'activité, les mesures de sécurité en place, et l'historique des incidents:

Prime d'assurance Cyber= [(prime de base) X (Facteurs modificateurs) X (charge supplémentaires)]+ marge de sécurité

1- Détermination de la prime de base

La prime de base est déterminée en fonction du chiffre d'affaire de l'entreprise et le niveau de criticité net du risque déterminé plus haut en appliquant des coefficients déterminés par les actuaires de la CCR pour chaque critère selon son impact.

2- Application des facteurs modificateurs

Les facteurs modificateurs représentent également des éléments importants qui affectent directement la méthode de calcul des primes. En fait, la prime d'un client peut être ajustée par plusieurs modificateurs qui varient entre ***0,75 et 1.25*** (MAETIJKA, 2021, p.75) selon son impact sur le risque global. Pour notre cas nous avons choisi trois facteurs les plus significatifs à l'instar de: **Secteur d'activité, Volume de données sensibles, Interconnexion**

avec tiers. Une fois les coefficients déterminés pour chaque facteur, ils sont multipliés ensemble puis appliqués à la prime de base.
par exemple: une entreprise du secteur financier avec un volume de données sensible faible et une interconnexion avec des tiers on applique sur la prime de base un taux des facteurs modificateurs de **1,25x0,75 x 1,25=1,17.**

3- Application des charges supplémentaires
Les charges supplémentaires peuvent être ajoutées en fonction des garanties et des services additionnels souhaités par l'entreprise :

- **Couverture étendue (ex. Ransomware)** : +10% à +30% de la prime.
- **Services de réponse aux incidents** : +5% à +15% de la prime.
- **Couverture internationale** : +10% à +20% de la prime.

4- Appliquer une marge de sécurité : La marge de sécurité est ajoutée à la prime pour couvrir les incertitudes et les risques additionnels non quantifiables. Cela inclut les fluctuations inattendues des sinistres, les erreurs dans les estimations actuarielles, ou les changements soudains dans l'environnement de risque (par exemple, une nouvelle menace cybernétique). La marge de sécurité est une composante essentielle pour garantir que la prime collectée par l'assureur est suffisante pour couvrir les sinistres inattendus et protéger la solvabilité de l'assureur. Elle doit être ajustée régulièrement en fonction des nouvelles informations et évolutions du profil de risque.
Cette méthode de tarification permet d'effectuer des ajustements en temps opportun en réponse aux évolutions du profil de risque d'une entreprise, comme la mise en place de nouvelles techniques ou l'instauration de nouveaux dispositifs de sécurité. Elle permet également à la CCR de négocier des conditions personnalisées ou des ajustements tarifaires en fonction des spécificités de chaque client

5.4.3. L'allégement des procédures de gestion des sinistres

Pour faciliter la procédure de gestion des sinistres nous suggérons à la CCR de:

1- créer une **Plateforme de Gestion en Ligne** pour déclarer et assurer le suivi des sinistres en temps réel, avec des mises à jour automatiques et des notifications sur l'état des réclamations.
2- Simplifier la documentation pour accélérer le traitement des sinistres, avec la possibilité de téléverser les rapports directement via l'application.
3- Avoir un service de gestion des sinistres impliquant plusieurs juridictions, adapté pour les PME opérant à l'international ou ayant des partenaires étrangers.

5.4.4. Elargir le champ d'application du produit

1- Considérer l'inclusion des start-ups et des micro-entreprises, qui sont également vulnérables aux cyber attaques, en offrant des produits adaptés à leur taille et à leurs besoins spécifiques.
2- Ajouter des couvertures supplémentaires pour des risques émergents comme les ransomwares, l'interruption d'activité en raison de cyberattaques,

3- Personnalisation des garanties ainsi que de leurs limites, en foction des besoins particuliers des entreprises.

6. Conclusion

À l'instar de nombreux pays, l'Algérie connaît une digitalisation rapide de son économie et de sa société. Si cette transformation numérique ouvre de nouvelles perspectives, elle s'accompagne également d'une augmentation des cyber-risques. La gestion de ces risques est cruciale pour sécuriser les données sensibles des clients, garantir la continuité des activités, et maintenir la réputation des entreprises.

Pour renforcer leur impact sur la résilience des entreprises locales, il est crucial que les assureurs algériens adoptent une approche proactive. Cela implique d'étblir des partenariats stratégiques, d'investir dans la formation en cybersécurité, et concevoir des produits d'assurance spécifiquement adaptés aux besoins du marché algérien. Les assureurs algériens possédent le potentiel de jouer un rôle majeur dans la sécurisation de l'écosystème économique contre les cyber attaques. Cependant, leur rôle dans la gestion des cyber-risques des entreprises locales reste largement sous-exploité.

L'émergence du marché de la cyber assurance en Algérie est confrontée à plusieurs défis, notamment le manque de données historiques, l'insuffisance de l'expertise locale, l'absence du cadre juridique ainsi que la faible sensibilisation et culture en matière de cyber sécurité.

Malgré ces défis, la Compagnie Centrale de Réassurance CCR a pris une initiative pionnière en lançant le premier produit d'assurance cyber en Algérie. Ce produit présente plusieurs atouts qui le positionnent favorablement sur le marché national. Parmi ses points forts, on trouve des conditions préalables claires qui encouragent les bonnes pratiques en cybersécurité, un partenariat stratégique avec des experts internationaux qui renforce la crédibilité du produit, ainsi qu'une tarification compétitive. Cependant, des axes d'amélioration sont nécessaires pour accroître l'efficacité et l'attractivité du produit en particulier les critères de sélection des risques, la tarification, et la complexité dans la gestion des sinistres.

Des recommandations ont été formulées pour améliorer le produit et accroitre son efficacité notamment: La mise en place d'une plateforme de Cyber Self Assessment pour un portefeuille équilibré assurant à long terme la viabilité du produit, une tarification plus équitable qui tient compte du profil de risque de l'entreprise, et l'allégement des processus de gestion des sinistres en mettant en place une plateforme de gestion en ligne. En intégrant ces améliorations, la CCR pourrait non seulement renforcer la pertinence de son produit sur le marché, mais aussi jouer un rôle clé dans la résilience face aux cyber risques.

Le marché de la cyber assurance en Algérie est encore naissant, mais il offre des perspectives de croissance significatives. En créant des produits d'assurance adaptés aux besoins locaux et en renforçant la collaboration entre les parties prenantes, l'Algérie pourrait devenir un exemple en matière de gestion des risques cybernétiques dans la région. L'évolution rapide des technologies numériques et l'augmentation des menaces cybernétiques rendent indispensable l'anticipation et l'adaptation continues des produits d'assurance pour protéger efficacement les entreprises algériennes contre ces nouveaux risques.

7. Réfférences Bibliographiques

1. ACHOURI, N. (2009). apport de la logique floué á l'analyse de criticité des risques industriels. 17-20. Université El-Hadj Lakhdar - Batna: mémmoire de magistère.
2. Compagnie Centrale de Réassurance. (2018). cyber risques. *ALGEREASS , 2018* (1ER TRIMESRE), 1-5.
3. CREMER, F., SHEEHAN, B., & MULINS, M. (2024). On the insurability of cyber warfare: An investigation into the German. *computers and security , Vol 142* (103886), 1-14.
4. GAVĖNAITĖ-Sirvydienė, J. (2019). Evaluation of cyber insurance as a riskmanagement tool providing cyber security. *Social Transformations in Contemporary Society , 7*, 84-93.
5. GHERNAOUTI, S. (2022). *cybersécurité:Analyser les risques et mettre en oeuvre les solutions* (Vol. 7éme édition). France: DUNOD.
6. HAMOUDA, W. O. (2024, juillet 04). Cybersécurité dans le secteur des assurances et réassurances. *Horizons* .
7. HAUSKEN, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things , 11* (100204), 1-9.
8. HENDA, S., & Naimi, A. (2020). risques émergents. *TUNIS RE , 1ére édition*, 27-44.
9. International Associationof insurance superv, IAIS. (2018). *Application paper on supervision of insurer cybersecurity.* https://www.iaisweb.org/uploads/2022/01/181108-Application-Paper-on-Supervision-of-Insurer-Cybersecurity.
10. KHALILI, M. M., & NAGHIZADEH, P. (2017). Designing Cyber Insurance Policies in the Presence of Security. *NetEcon Cambridge, MA USA* (7), 1-6.
11. ksouma, I.(2024). Les cyber risques, risques émergents. *2éme édition*, Tunis Re 21-39.
12. Lawrence, A. G., Martin, P. L., & Tashfeen, S. (2003). 'A Framework for Using Insurance for Cyber-Risk Management. *Communications of the ACM , 46* (3), 81-85.
13. MAHBOULI, T. (2022). Des solutions innovantes et adaptées pour faire face aux risques émergents. *Revue de l'assurance , 39*, 41-45.
14. MATAEJKA, V. (2021). A Framework for the Definition and Analysis of Cyber Insurance requirment. *university of zurich* .
15. Merad, M. M. (2004, mars). Analyse de l'état de l'art sur les grilles de criticité.*rapport INERISDRA638 https://www.ineris.fr/sites/ineris.fr/files/contribution/Documents* .
16. Munich Re. (2024). *cyber insurance:risks and trends 2024.* https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.
17. ROMANSKY, S., ABLON, L., & KUEHEN, A. (2019). content analysis of cyber insurance policies, How do carriers write policies and price cyber risk? *journal of cyber security , 5* (2), 1-40.
18. Saudi Arabian Monetary Authority. (2017). *Cyber Security Framework.* https://www.sama.gov.sa/en-US/RulesInstructions/CyberSecurity.
19. Sini, N. (2024, mars 2). Cybersécurité : De grands enjeux pour les entreprises et les assureurs. *Horizons* .
20. Sullivan, J., & Nusen, R. C. (2020). Cyber Security Incentives and the Role of Cyber Insurance. (R. U. Studies, Ed.) *EMERGING INSIGHTS* , 1-20.

21. Strupczewski, S (2021). Data defining cyber risk. *Safety science, Elsevier 135*, 1-10.
22. TALESH, A. (2018). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses. *Law and social inquiry , 43* (2), 417-440.