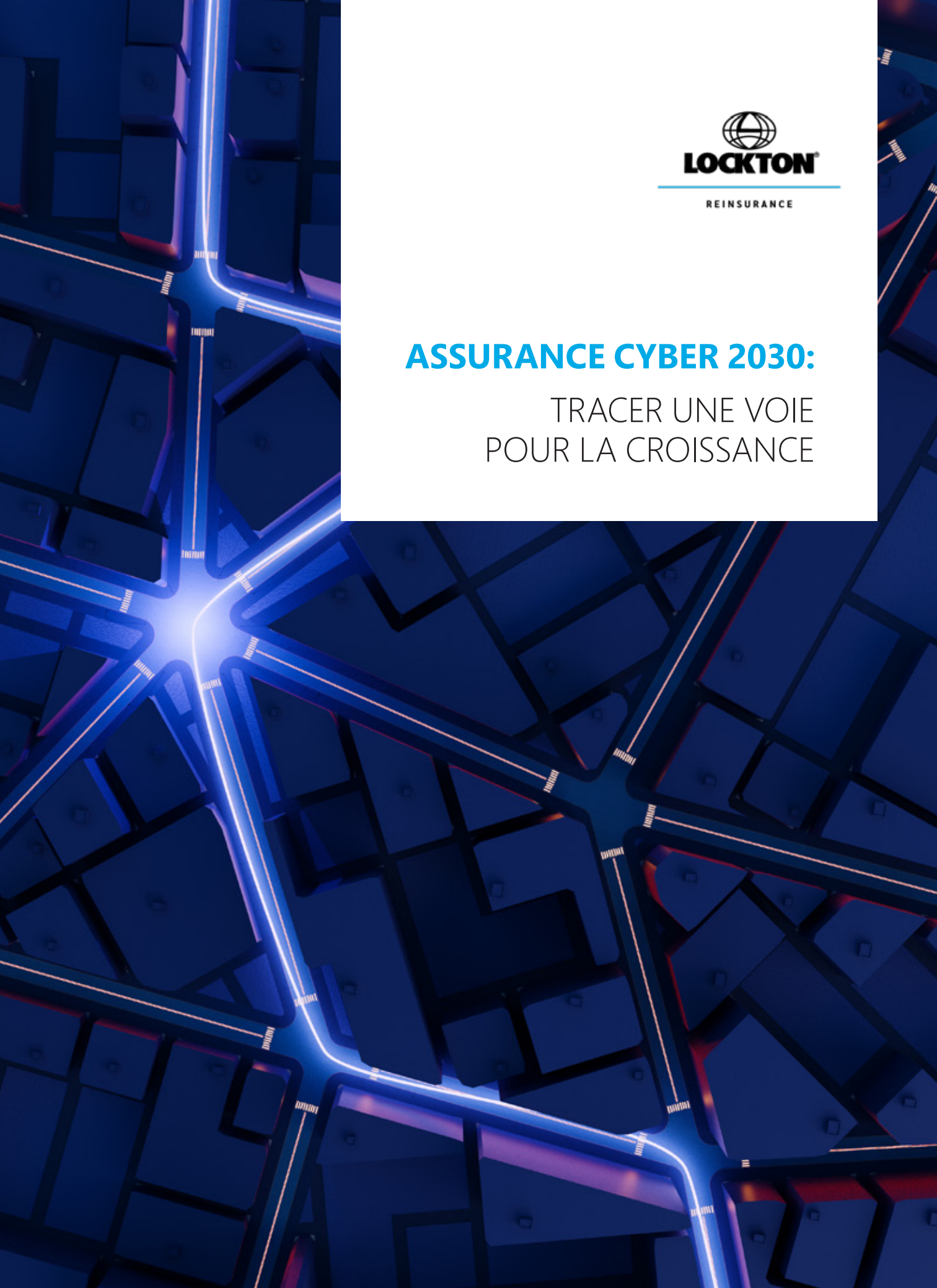


LOCKTON
REINSURANCE

ASSURANCE CYBER 2030:

TRACER UNE VOIE POUR LA CROISSANCE

- **Exposition**
- **Périls**
- Transfert de risques
- Placement

À propos de Lockton Re

Lockton Re, la division mondiale de réassurance de Lockton Companies, aide les entreprises à comprendre, atténuer et tirer parti des risques. Avec plus de 500 collaborateurs répartis dans 23 bureaux à travers le monde, l'entreprise poursuit sa croissance et propulse le secteur de la réassurance vers l'avant grâce à des solutions plus intelligentes qui exploitent les nouvelles technologies, fournies par des équipes habilitées à agir dans l'intérêt des clients.

Les rapports, analyses de marché et perspectives de Lockton Re se concentrent sur les sujets, événements ou évolutions majeurs du marché de la (ré)assurance et du courtage qui impactent nos clients et partenaires. Afin de mieux orienter nos lecteurs, nous classons ce contenu en quatre catégories : Expositions, Périls, Transfert de risques et Placement. Lockton Re se réjouit de travailler au nom de ses clients pour fournir de nouvelles perspectives et des produits innovants conçus pour répondre aux multiples facettes des risques cyber.

Résumé exécutif

Le marché de la cyber-assurance devrait plus que doubler d'ici 2030. Même les estimations les plus prudentes prévoient une croissance soutenue, aux répercussions profondes tant sur le marché de la (ré)assurance cyber que sur l'ensemble du secteur. Toute projection de croissance du marché comporte une incertitude inhérente. C'est pourquoi, plutôt que de nous limiter à des estimations chiffrées, nous allons au-delà des chiffres pour examiner les conditions nécessaires à la réalisation de ces attentes. La croissance nécessaire pour atteindre les prévisions de 2030 n'est pas inévitable. Elle dépendra d'une série d'actions délibérées de la part du secteur. Nous avons rassemblé un large éventail de points de vue issus de différentes parties prenantes du secteur et avons cherché à répondre à des questions telles que : Comment se préparer à un tel marché ? Quelles innovations en matière de produits et de capitaux seront nécessaires pour l'accompagner ?
Nous interrogeons et explorons ces enjeux, tout en proposant des pistes pour favoriser la croissance. Trois axes majeurs ressortent pour soutenir cette croissance :

1. **Amélioration de la qualité des données**
2. **Poursuite des investissements dans la modélisation**
3. **Flexibilité de l'approche produit pour la distribution**

These are examined in more detail in this white paper.

Remerciements

Ce livre blanc n'aurait pas pu voir le jour sans les contributions et les retours de plusieurs acteurs du secteur de l'assurance cyber. Certains ont préféré rester anonymes, et nous leur sommes reconnaissants pour le temps et les perspectives qu'ils nous ont offerts. D'autres ont partagé leurs points de vue et leurs commentaires, parmi lesquels :

YOSHA DELONG,
Responsable de l'engagement mondial, Mosaic Insurance

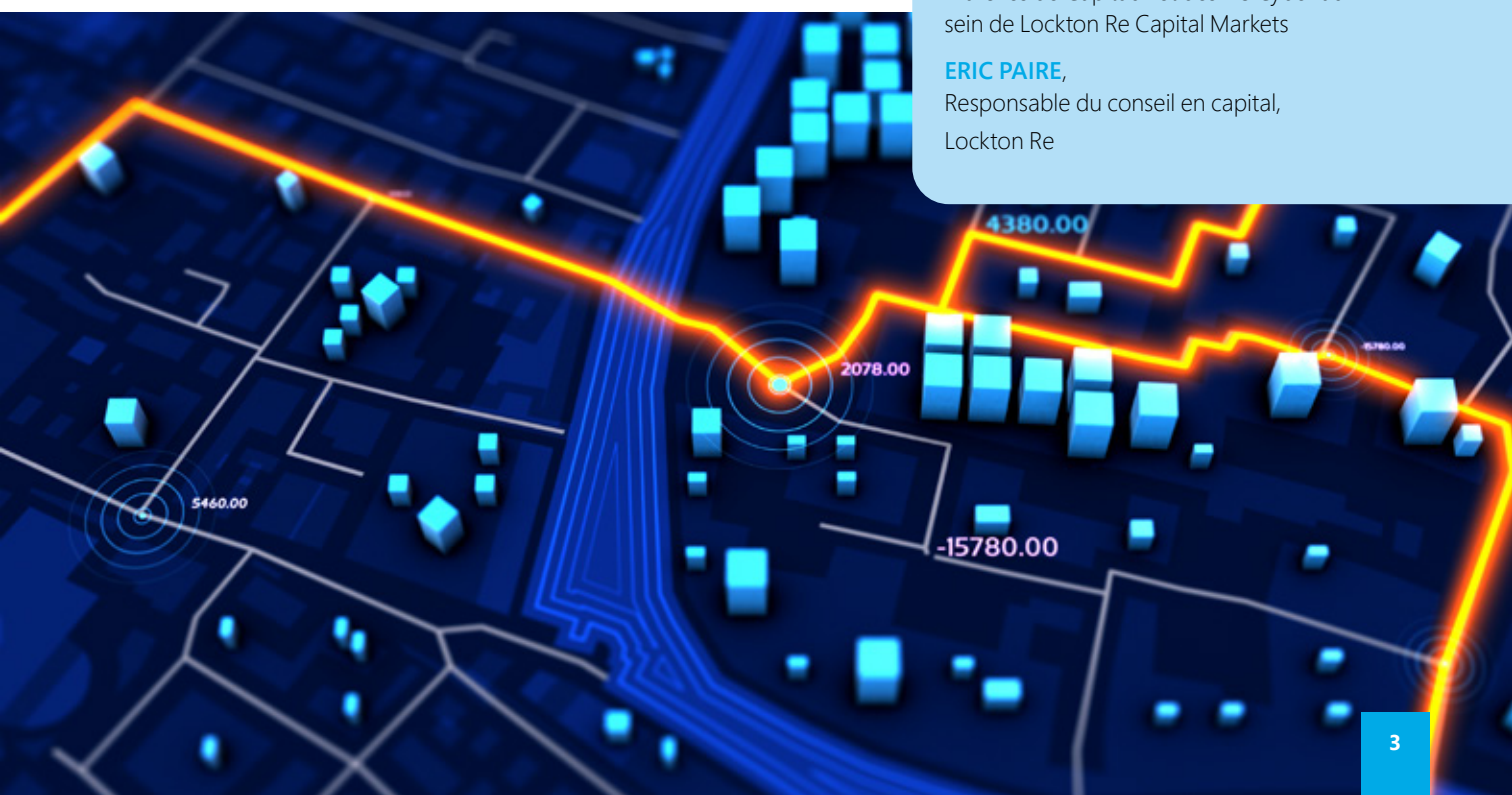
TOM DRAPER,
Directeur général du Royaume-Uni, Coalition

TIM GARDNER,
PDG de Lockton Re

MARK GREISIGER,
Président-directeur général de Netdiligence

THEO NORRIS,
Responsable de la Structuration des Marchés de Capitaux et des ILS Cyber au sein de Lockton Re Capital Markets

ERIC PAIRE,
Responsable du conseil en capital, Lockton Re



Introduction

Le marché de la cybersécurité a été l'une des grandes réussites de l'assurance dommages et responsabilité civile au cours des deux dernières décennies. Cette croissance a été due à l'adoption rapide des technologies, à l'évolution du paysage des risques et aux tactiques sophistiquées des acteurs malveillants, ainsi qu'à une sensibilisation croissante aux menaces. Les estimations du marché pour 2025 varient entre 16 et 20 milliards de dollars,[1-2] tandis que celles pour 2030 se situent entre 30 et 40 milliards de dollars, voire plus.[3]

Le taux de croissance annuel composé (TCAC) moyen du marché de la (ré)assurance cyber entre 2015 et 2025 a régulièrement dépassé 20%. Certaines années, il a même excédé 30%. Ces dernières années, l'hypothèse d'une croissance similaire du marché cyber a rarement été remise en question. Cependant, depuis le pic des taux fin 2021 et début 2022, l'augmentation de la capacité d'assurance, tirée par l'offre, a entraîné un ralentissement du TCAC. Néanmoins, diverses estimations suggèrent toujours des taux de croissance supérieurs à 10% pour le reste de la décennie, impliquant un doublement approximatif des primes mondiales d'ici 2030.

Le consensus reste que la croissance se poursuivra, malgré le léger repli actuel des tarifs. En effet, AM Best a rapporté pour la première fois une baisse du volume absolu des primes aux États-Unis,[4] reflétant une concurrence intense pour les acheteurs actuels d'assurance cyber.

Nous examinons les différentes hypothèses qui sous-tendent la croissance attendue et analysons les dynamiques qui influencent l'expansion continue du marché. Ce rapport n'a pas pour objectif de prédire l'avenir, mais plutôt d'offrir une occasion de faire le point et de passer en revue les tendances actuelles qui génèrent à la fois des opportunités et des défis pour le marché. Ce document met l'accent sur la manière dont ces influences évoluent afin de répondre aux fortes attentes de croissance du marché. Nous avons interrogé divers acteurs du secteur afin de mieux comprendre les thèmes communs, de comparer la situation actuelle avec la vision à long terme du marché et de déterminer les meilleures façons de combler les écarts.[5]

[1] http://munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html
[2] https://www.rootsanalysis.com/cybersecurity-insurance-market
[3] https://www.reinsurancene.ws/beazley-forecasts-cyber-insurance-market-to-grow-to-40bn-by-2030/
[4] https://www3.ambest.com/ambv/sales/bwpurchase.aspx?record_code=354887&AltSrc=22&AltServ=640

Croissance du marché cyber : une évidence ?

Dans le secteur de l'assurance cyber, il est unanimement reconnu que la croissance rapide du marché est une réalité omniprésente. Le marché de l'assurance dommages et responsabilité civile a enregistré un TCAC moyen à un chiffre élevé entre 2015 et 2024. Le marché de la (ré)assurance cyber a, quant à lui, plus que doublé sur la même période.

> “Le marché de l'assurance dommages et responsabilité civile a enregistré un TCAC moyen à un chiffre élevé entre 2015 et 2024. Le marché de la (ré) assurance cyber a, quant à lui, plus que doublé sur la même période.”

Cette croissance a transformé le marché de la cybersécurité, autrefois relégué au second plan de l'assurance spécialisée, en un élément plus largement reconnu et intégré de l'écosystème plus vaste de la (ré)assurance. Les produits d'assurance cyber sont désormais intégrés dans l'ensemble de la gestion des risques cyber, en particulier au sein des grandes entreprises. On estime qu'environ 80% des grandes entreprises (dépassant 10 milliards USD de chiffre d'affaires annuel) souscrivent une assurance cyber. Sur ce segment du marché, les débats sur le budget consacré à la cybersécurité d'une part et à l'assurance cyber d'autre part sont désormais dépassés.[6]

Pour les entreprises de plus petite taille, la situation est différente. Seules 10% des petites et moyennes entreprises (PME) souscrivent une assurance cyber.[7] De nombreuses raisons freinent la souscription, et nous les examinerons plus en détail. Combler ce déficit de souscription représente l'une des plus grandes opportunités pour le marché dans les années à venir.

[5] https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/global%20insurance%20report%202025/global-insurance-report-2025-the-pursuit-of-growth.pdf

[6] https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/about-cyber-insurance-market.html

[7] Ibid.

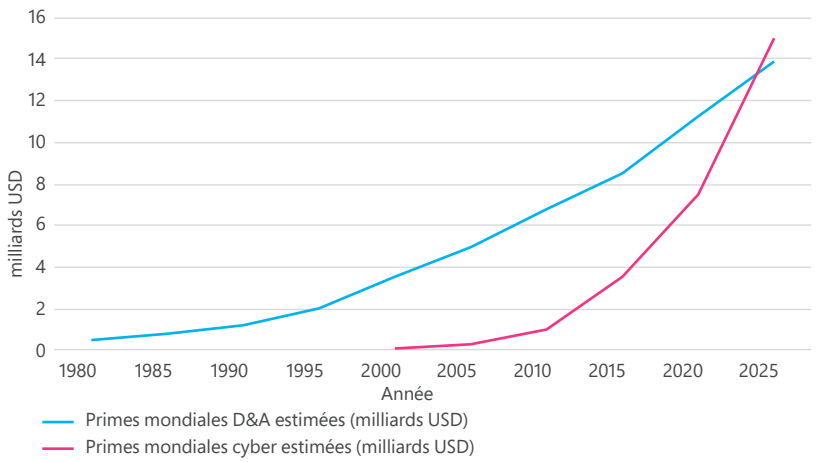
Apprendre de l'expérience

Tim Gardner, PDG de Lockton Re, a comparé la croissance du marché cyber à celle du marché des assurance des Dirigeants (D&O insurance). Les deux marchés ont émergé en réponse aux risques croissants auxquels les entreprises sont confrontées. Le marché D&A a connu une croissance plus régulière, principalement en raison du renforcement de la surveillance réglementaire et d'un environnement juridique de plus en plus exigeant. La croissance du marché cyber, quant à elle, est largement liée à l'évolution du paysage des menaces. L'adoption a été inégale, et la souscription par les PME, tant en D&A qu'en assurance cyber, a été plus lente que pour les grandes entreprises.

Les nouvelles expositions stimulent l'innovation sur le marché, et elles ont créé des opportunités dans les deux contextes. 'Le marché de l'assurance est fortement capitalisé et recherche toujours de nouvelles opportunités à potentiel à long terme. L'assurance cyber en fait partie', déclare Tim Gardner. Lorsqu'un écart significatif existe entre les résultats bruts et nets, cela attire de nouveaux capitaux. Certains redoutent le risque extrême, tandis que d'autres apprécient la volatilité, contribuant ainsi à la formation d'un marché.

Étant donné que l'exposition continuera de croître et d'évoluer, et que le risque systémique influence la stratégie de gestion des risques des assureurs, le principal défi à long terme réside dans le risque de déficit de capital. Il nous incombe, en tant que marché, de renforcer la confiance dans la tarification afin d'attirer un nombre suffisant de nouveaux investisseurs, tant par les voies traditionnelles que par les voies alternatives.

Figure 1: Estimations des primes mondiales d'assurance D&A et de (ré)assurance cyber



Source: Lockton Re

Mettre tous ses œufs dans le même panier?

'Il est sage de se préserver aujourd'hui pour demain, et de ne pas mettre tous ses œufs dans le même panier.'[8] Miguel de Cervantès a parfaitement illustré le concept de diversification dans son roman Don Quichotte, publié en 1605. La diversification n'est pas un concept nouveau dans le domaine financier ; elle est presque aussi ancienne que le secteur de l'assurance et de la finance lui-même. Identifier les actifs ou les risques peu corrélés est fondamental pour la manière dont les (ré)assureurs perçoivent leurs portefeuilles et leurs actifs.

Dans le contexte plus large du marché de la (ré)assurance dommages et responsabilité civile, l'assurance cyber est à juste titre considérée comme un facteur de diversification important. Une part significative des risques assumés par le secteur de l'assurance relève soit de l'assurance dommages (principalement les périls naturels entraînant des expositions à court terme), soit de la responsabilité civile (avec des risques à long terme). L'assurance cyber a évolué en intégrant des aspects d'exposition analogues à l'assurance dommages ainsi que des risques qui ressemblent davantage aux cas de responsabilité civile. Il est important de noter que les risques cyber ne sont pas corrélés avec les autres périls naturels majeurs. Cela signifie qu'en cas d'événement majeur impactant l'assurance dommages (comme un ouragan), les risques cyber ne sont pas affectés de la même manière. De même, les tendances émergentes en matière de responsabilité civile (telles que l'inflation sociale ou les verdicts nucléaires) ont moins de répercussions sur le domaine des risques cyber.

Au sein même de l'assurance cyber, la diversification joue également un rôle important. Les sources courantes de contagion au sein des réseaux, susceptibles d'affecter plusieurs entreprises lors d'un même incident technologique, ont toujours suscité des inquiétudes. À l'émergence du marché cyber, certains assureurs ont intégré des exclusions liées aux 'virus sauvages' dans leurs polices afin de limiter le risque d'accumulation. Cette couverture restreinte limitait la demande, car elle ne répondait pas aux besoins des clients. La concurrence a ensuite élargi la couverture afin d'innover et de répondre à la demande.

Un fait incontournable du marché de l'assurance cyber est qu'il n'y a eu qu'un petit nombre de véritables catastrophes cyber où un incident unique a affecté plusieurs entreprises. Par conséquent, les données permettant de comprendre comment un incident technologique pourrait affecter simultanément plusieurs entreprises sont limitées. De nombreuses recherches ont été menées à ce sujet, mais, inévitablement, un certain degré de conjecture subsiste quant à la manière exacte dont cela pourrait se manifester.

> “Un fait incontournable du marché de l'assurance cyber est qu'il n'y a eu qu'un petit nombre de véritables catastrophes cyber.”

Actuellement, les principales sources de contagion potentielles dans l'assurance cyber sont la propagation de logiciels malveillants, l'exploitation de vulnérabilités zero-day et les pannes de la chaîne d'approvisionnement numérique (y compris les services cloud). Bien que ces scénarios couvrent une large gamme de situations spécifiques, ils permettent de fournir un cadre utile pour analyser les différentes manières dont les portefeuilles pourraient être impactés.

Dans le domaine des services cloud, le secteur de l'assurance a approfondi sa compréhension de leur fonctionnement et des conséquences que leurs interruptions peuvent avoir sur les portefeuilles assurés. Amazon Web Services a été lancé en 2006, et au cours des années 2010, l'adoption du cloud computing a connu une accélération spectaculaire. Le marché mondial est passé de 24,6 milliards de dollars en 2010 à 156,4 milliards de dollars en 2020.[9] Aujourd'hui, le cloud est omniprésent, 96% des entreprises l'utilisant sous une forme ou une autre.[10] Ces dernières années, notre compréhension

[8] “Don't Put All Your Eggs in One Basket.” n.d. Grammar-Monster.com https://www.grammar-monster.com/sayings_proverbs/dont_put_all_your_eggs_in_one_basket.htm

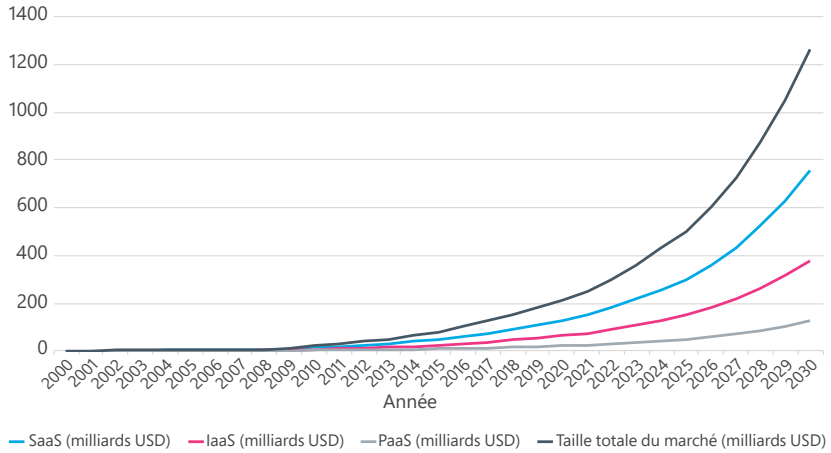
[9] https://www.herrick.com/publications/cyber-liability-insurance-what-to-look-for-when-obtaining-coverage/

de la diversification a beaucoup évolué. Il y a seulement quelques années, l'idée d'un 'cyber-ouragan' impliquait une exposition uniforme et omniprésente à travers les frontières nationales et les technologies communes[11].Nous avons depuis affiné notre compréhension des expositions systémiques cyber, en tenant compte des incidents ayant entraîné des pertes économiques importantes.

Les composants technologiques[12] couramment utilisés par les entreprises ont évolué rapidement, et la dépendance à ces technologies est désormais mieux comprise. Les trois principaux acteurs du marché du cloud computing sont Amazon Web Services, Microsoft Azure et Google Cloud Platform. Ensemble, ils représentaient 63 % de la part mondiale des dépenses en infrastructures cloud en 2024[13].

Les investissements de ces entreprises sont considérables, et les utilisateurs de ces services comprennent mieux comment tirer parti des différentes composantes du cloud computing, tels que l'infrastructure, la plateforme et les logiciels. À mesure que le secteur de la (ré)assurance approfondit sa connaissance du fonctionnement et des interactions de ces différents segments technologiques en réseau, il parvient à une meilleure compréhension des points faibles et des sources potentielles de défaillance. Le cloud computing moderne met de plus en plus l'accent sur la résilience, réduisant ainsi la probabilité que les pannes aient des conséquences critiques.

Figure 2: La création d'un système d'incitation pour valoriser or l'introduction de mesures incitatives pour valoriser



Source: Lockton Re

[10] https://www.statista.com/statistics/500541/worldwide-hosting-and-cloud-computing-market/

[11] https://www.itdeskuk.com/latest-cloud-statistics

[12] http://betterley.com/samples/cpims14_nt.pdf

[13] https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/

Libérer la croissance des PME

Depuis de nombreuses années, il existe une incertitude quant à la manière de développer une offre d'assurance cyber attrayante et accessible aux PME. Les estimations varient selon les territoires, mais malgré la disponibilité de ce produit depuis plusieurs années, moins de 15 % des PME dans la plupart des marchés matures l'ont souscrit. Plusieurs obstacles ont limité l'adoption de l'assurance au sein du secteur des PME. Démontrer la valeur, former les réseaux de distribution, expliquer la couverture et mettre en avant son utilité sont des défis permanents.

Même dans les marchés où les lignes spécialisées sont établies (par exemple aux États-Unis, au Royaume-Uni et dans l'UE), la mise en place d'une couverture cyber affirmative et indépendante demeure un sujet complexe pour les courtiers d'assurance généralistes. Différents modèles de distribution ont rencontré un certain succès, comme la vente directe en ligne ou l'ajout de couvertures cyber par avenant. Ces approches permettent d'introduire l'assurance cyber tout en réduisant les frictions liées à la souscription. De plus, une nouvelle génération de MGA (agents généraux de gestion) spécialisés dans le cyber a spécifiquement ciblé ce segment du marché, en proposant des produits d'assurance simplifiés et plus rentables.

Un de ces MGA est Coalition. Tom Draper, directeur général) pour le Royaume-Uni, revient sur la question du taux de souscription des PME : 'Beaucoup de PME ne considèrent pas le risque cyber comme un défi en matière d'assurance. Il nous appartient de repositionner le débat afin que l'assurance fasse partie intégrante de la solution et trouve un écho auprès de non-acheteurs actuels. 'Malgré des investissements

Diversification : un catalyseur de croissance

La compréhension des corrélations entre les risques du portefeuille d'assurance cyber s'est aujourd'hui considérablement améliorée, en particulier pour évaluer leur impact en cas d'incident cyber majeur. La diversification permet de limiter les pertes potentielles assurées selon quatre axes principaux:

These are:

- **Géographique :** Les déploiements technologiques varient d'un pays à l'autre. De plus, les fuseaux horaires peuvent influencer de manière significative la propagation des incidents cyber.
- **Industriel:** Certaines technologies sont spécifiques à certains secteurs. Elles ont un impact disproportionné sur certains maillons de la chaîne d'approvisionnement, où peu de fournisseurs peuvent dominer un sous-secteur particulier.
- **Selon le chiffre d'affaires :** Les petites entreprises ont tendance à déployer leurs technologies de manière plus uniforme et dépendent davantage des infrastructures cloud publiques. À l'inverse, les grandes entreprises disposent souvent de configurations sur mesure et de réseaux complexes à plusieurs niveaux.
- **Selon l'infrastructure technologique :** Les points communs entre différentes architectures technologiques constituent des sources potentielles de vulnérabilité. Certaines technologies sont utilisées dans de nombreux contextes différents ; comprendre leur déploiement et leur interconnexion est crucial pour évaluer l'impact systémique.

La compréhension des mécanismes de diversification d'un portefeuille est essentielle pour évaluer la manière dont un sinistre pourrait se dérouler. Lorsque les avantages de la diversification sont pleinement exploités, le capital peut être déployé plus efficacement et l'analyse des calculs de pertes maximales probables peut être allégée. En conséquence, un volume plus important de primes peut être souscrit sur la même base de capital si l'approche de la diversification est fiable. Cela permet une amélioration de la croissance du marché au fil du temps.

technologiques importants dans l'assurance, un défi reste un enjeu : il s'agit de rendre le processus de transaction aussi fluide que possible pour les clients. Si les assureurs parviennent à familiariser les décideurs avec le langage du risque cyber, ils pourront garantir la pertinence du marché pour un secteur qui sera moteur de croissance dans les années à venir.

> Si les assureurs parviennent à familiariser les décideurs avec le langage du risque cyber, ils pourront garantir la pertinence du marché pour un secteur qui sera moteur de croissance dans les années à venir.

Pour atteindre la croissance anticipée du marché global, il est essentiel d'accroître le nombre de nouveaux acheteurs. Dans les premières années du marché de l'assurance cyber, les polices se limitaient à un modèle d'indemnisation, offrant peu de valeur ajoutée aux clients. Cette offre a depuis considérablement évolué pour devenir un service beaucoup plus complet, incluant des avantages en matière de gestion des risques, des alertes actives et des services de récupération après sinistre. La priorité donnée à la formation des courtiers et agents, ainsi que la création d'un système d'incitation pour valoriser or l'introduction de mesures incitatives pour valoriser, sont des éléments clés pour développer le marché. Les décideurs en assurance font face à de nombreuses contraintes de temps et de ressources, ce qui rend ces initiatives encore plus cruciales

Nouveaux acheteurs

L'un des premiers catalyseurs de la croissance du marché naissant de la cybersécurité au début des années 2000 a été l'adoption rapide de réglementations relatives à la gestion et à la divulgation des informations personnelles. Cela s'est illustré par la loi californienne sur la protection de la vie privée (California Information Privacy Act) de 2003 (SB1386). Cette loi imposait aux entités victimes d'une violation de données impliquant des informations personnelles de consommateurs californiens d'en notifier les personnes concernées. Elle est ainsi devenue un cadre de référence pour d'autres États américains ainsi que pour d'autres pays dans l'élaboration de lois et de réglementations. En parallèle, des produits et solutions d'assurance cyber ont été conçus pour aider les entreprises à se conformer à ces obligations réglementaires. Des réglementations supplémentaires, par secteur (par exemple dans la santé ou les services financiers) et par Typologie d'entreprises (comme pour les sociétés cotées en bourse), sont venues enrichir cet ensemble de règles imposées aux entreprises, assorties de sanctions en cas de violation.

À mesure que de plus en plus de pays établissent et développent des cadres réglementaires en matière de cybersécurité et de protection des données, les organisations sont de plus en plus incitées à souscrire une assurance cyber. Certaines régions d'Asie ont récemment adopté des lois qui ont stimulé l'intérêt pour ce type d'assurance. La Chine a mis en œuvre sa loi sur la protection des informations personnelles (Personal Information Protection Law) en 2021 et a introduit ses nouvelles règlementations sur la gestion de la sécurité des données réseau (Network Data Security Management

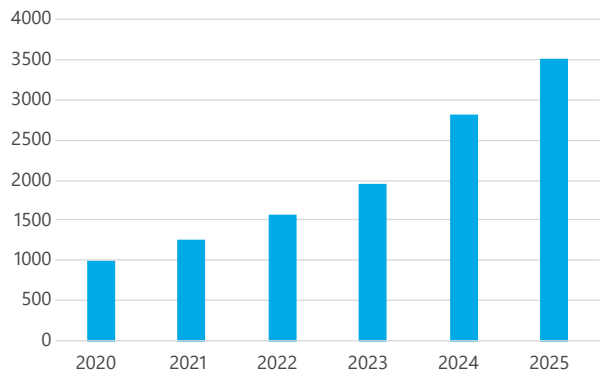
[14] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe

Regulations) en 2025. L'Inde a adopté la loi sur la protection des données personnelles numériques (Digital Personal Data Protection Act) en 2023. De plus, la Corée du Sud a apporté des mis à jour importantes à sa loi sur la protection des informations personnelles (Personal Information Protection Act) en 2024, augmentant la responsabilité en cas de dommages. Ces exemples soulignent l'importance de cette problématique dans ces territoires et l'effet d'entraînement qu'elle peut générer. Au Japon, la loi sur la protection des informations personnelles (Act on Protection of Personal Information) fait actuellement l'objet d'une refonte majeure afin de prévoir des mesures plus complètes pour protéger les données et de revoir le régime des amendes et sanctions. D'autres régions du monde ont également introduit de nouvelles lois relatives aux données personnelles.

La réglementation n'est pas le seul catalyseur. Les impacts des incidents cyber sont également persistants. La Figure 3 ci-dessous illustre la croissance du nombre d'incidents en Amérique latine depuis 2020. La prise de conscience a progressé parallèlement à la reconnaissance du rôle que l'assurance peut jouer dans la protection des entreprises. Il est clair que les incidents seuls ne suffisent pas à stimuler la croissance du marché, mais ils constituent un contexte important pour les discussions autour du transfert de risque.

Un autre sujet, trop peu abordé, est la sous-assurance fréquente, même parmi les grandes entreprises. Il appartient au secteur de l'assurance cyber d'expliquer clairement la quantification du risque cyber de manière compréhensible pour les acheteurs d'assurance, afin de combler le fossé entre cybersécurité et gestion des risques.

Figure 3: La création d'un système d'incitation pour valoriser or l'introduction de mesures incitatives pour valoriser[14]



Source:World Bank

Capital à long terme

Concurrencer sur le marché actuel de l'assurance cyber peut parfois ressembler à un combat de rue, où chaque client se gagne en fonction de la couverture, des tarifs, du service et de tout autre critère jugé important par le client. Cependant, adopter une vision d'ensemble est crucial pour la pérennité à long terme du secteur de l'assurance cyber. Quelques éléments doivent être réunis pour montrer aux investisseurs externes l'attrait du secteur de l'assurance par rapport à d'autres investissements. L'assurance cyber joue un rôle dans ce contexte en améliorant la diversification des portefeuilles des assureurs. Ensuite, l'ajustement continu de l'allocation du capital, en s'appuyant sur une planification réaliste des catastrophes, est nécessaire. Cela permet une utilisation plus efficace du capital et a des répercussions sur la gestion de la solvabilité réglementaire et des obligations en matière de capital. Troisièmement, la compréhension des risques systémiques doit être constamment réévaluée afin de protéger la solvabilité – et la réputation – du secteur.

À mesure que les investisseurs considèrent l'assurance comme une source potentielle d'investissement, le risque d'assurance offre une classe d'actifs non corrélée par rapport aux autres actions. Les risques physiques couverts par la plupart des assurances représentent une exposition différenciée au risque, indépendante des marchés boursiers. Le risque cyber permet aux investisseurs d'accéder à des périls différents des catastrophes naturelles, et certains investisseurs participent déjà à des programmes cyber dans le cadre de Protections globales auprès des Lloyd's. Comme l'a souligné Eric Paire, responsable de Lockton Re Capital Advisory: 'Les investisseurs ne peuvent pas être experts en tout. Ils s'appuient sur les marchés de la (ré)assurance pour développer et affiner des stratégies diversifiées afin de soutenir leurs objectifs d'investissement.'

L'émission de titres financiers (Insurance-Linked Securities – ILS) offrent un mécanisme efficace permettant aux investisseurs non traditionnels d'accéder au risque d'assurance, le risque cyber faisant désormais partie de leur stratégie d'investissement. Depuis l'émission initiale de l'obligation catastrophe cyber en 2023, plus de vingt investisseurs ont déployé du capital. Ce marché, qui représente aujourd'hui près d'un milliard de dollars de couverture répartis sur onze tranches, est devenu un pilier de

la stratégie d'achat de couvertures catastrophes de plusieurs grands assureurs cyber. Une forte activité a marqué l'année 2024, suivie d'un ralentissement des transactions en 2025. Cette situation s'explique principalement par la rentabilité de la capacité de réassurance traditionnelle et par une réduction des cessions moyennes de réassurance, en réponse à la baisse des taux sous-jacents. Si les Cyber Cat Bond restent en progression pour les nouvelles émissions, l'évolution s'est faite par étapes.

Aucune discussion sur les ILS ne serait complète sans une compréhension fine de la modélisation des catastrophes cyber. Les modèles traditionnels de catastrophes naturelles s'appuient sur des décennies de données actuarielles sur les pertes et les incidents liés aux catastrophes naturelles, tandis que la modélisation des catastrophes cyber doit composer avec un nombre limité de précédents historiques. Ce défi génère une incertitude inhérente, ce qui peut conduire les investisseurs en ILS à intégrer une rémunération additionnelle dans leur marge, afin de compenser ce risque, en plus de celle déjà prévue pour risques de catastrophe. Bien que les modèles évoluent rapidement, davantage de capital est conservé pour tenir compte de cette incertitude. Une conséquence à court terme est que le capital disponible pourrait être insuffisant pour répondre aux mesures de risque extrême exigées par les (ré)assureurs. Tant qu'un incident cyber majeur ne mettra pas ces modèles à l'épreuve, l'incertitude perçue quant à la manière dont les couvertures et obligations réagiront aux événements persistera.

Lockton Re adopte une vision à long terme. La plupart des acteurs du marché s'accordent à dire que le capital traditionnel est simplement incapable de suivre le rythme de croissance du cyber. Les marchés de capitaux deviendront un élément crucial et constant du marché de la réassurance cyber, et les structures continueront d'évoluer. On observe déjà des émissions répétées d'obligations, ainsi que de premières transactions sur le marché secondaire, à mesure que les investisseurs cherchent à s'exposer au risque cyber. Selon Theo Norris, responsable du Cyber ILS chez Lockton Re Capital Markets : 'Les cédantes testent leurs définitions d'événements et calibrent leur perception du risque en coulisses, afin de se préparer à l'expansion des protections contre les catastrophes cyber, en passant de couvertures par événement à des couvertures Cat Bond.'

L'œuf ou la poule?

Une caractéristique intrigante du cybermarché actuel est que, pour attirer des investisseurs en capital, il faut démontrer une trajectoire de croissance claire pour le marché. Parallèlement, pour permettre cette croissance, il est nécessaire de disposer d'une source de capital durable. La relation entre la croissance du marché et le capital nécessaire pour la soutenir est symbiotique, non linéaire, mais essentielle à la réussite globale du marché. C'est la question millénaire du 'qui de l'œuf ou de la poule vient en premier ?'. Une manière de résoudre ce paradoxe réside dans l'évolution constante à la fois de la réponse du marché face aux menaces et de l'adaptation des modèles de catastrophe cyber, qui amélioreront les paramètres d'évaluation des opportunités de croissance et des besoins en capital au fil du temps.

Il existe un compromis dans l'utilisation du modèle entre d'une part la stabilité du modèle qui soutient le cycle de planification du capital à long terme, et d'autre part, la nécessité de mettre à jour et de maintenir une vision contemporaine du risque, tenant compte d'adversaires actifs et d'un paysage des menaces en évolution rapide.

Tous les modèles ont des limites. Plus le secteur gère et opère efficacement dans le respect de ces paramètres, plus les modèles utilisés pour soutenir les capitaux de tiers peuvent être valorisés. Les modèles efficaces intègrent une combinaison d'analyse de scénarios, de renseignements sur les menaces, de cartographie des dépendances technologiques et d'analyse comportementale afin de fournir des estimations probabilistes des pertes sur l'ensemble des portefeuilles. À mesure que les cadres réglementaires et les profils d'exposition deviennent plus sophistiqués, ces modèles (qui permettent aux (ré)

assureurs d'évaluer plus précisément les expositions globales) doivent eux aussi évoluer pour permettre d'identifier les vulnérabilités systémiques et de tarifer les risques avec une confiance accrue. L'investissement continu et l'application des enseignements tirés de ces modèles seront essentiels, à mesure que les risques cyber s'entrelacent de plus en plus avec les systèmes économiques mondiaux et les infrastructures numériques.

La croissance des dépendances technologiques représente un défi de taille pour les (ré)assureurs cyber ainsi que pour les modélisateurs de catastrophes cyber. Les organisations modernes s'appuient sur un vaste ensemble de services numériques interconnectés, de plateformes cloud, de fournisseurs tiers et d'infrastructures critiques, chacun introduisant des points de vulnérabilité spécifiques. Les réseaux présentent des personnalisations importantes (surtout chez les grandes entreprises), ce qui limite sans toutefois éliminer le risque potentiel. Une seule défaillance ou compromission – que ce soit dans les chaînes logicielles, les services informatiques externalisés ou les environnements réseau partagés – peut se répercuter sur plusieurs entités, accroissant l'ampleur des pertes et compliquant les évaluations de risque.

Alors que les écosystèmes numériques gagnent en complexité et en portée mondiale, il devient essentiel de cartographier ces dépendances et de comprendre leur impact systémique potentiel. Yosha DeLong, responsable de l'engagement mondial chez Mosaic Insurance, déclare : 'Les défaillances dans la chaîne d'approvisionnement constituent une source de préoccupation pour les assureurs et créent un risque de volatilité dans la manière dont les pertes se manifestent.'

Des modèles efficaces de catastrophes cyber doivent non seulement identifier les risques de directs, mais également

> La croissance des dépendances technologiques représente un défi de taille pour les (ré)assureurs cyber ainsi que pour les modélisateurs de catastrophes cyber.

tenir compte des risques indirects liés aux interdépendances technologiques, permettant aux (ré)assureurs d'évaluer plus précisément les expositions globales et de comprendre comment, par exemple, les pertes d'exploitation pourraient se manifester à travers un portefeuille.

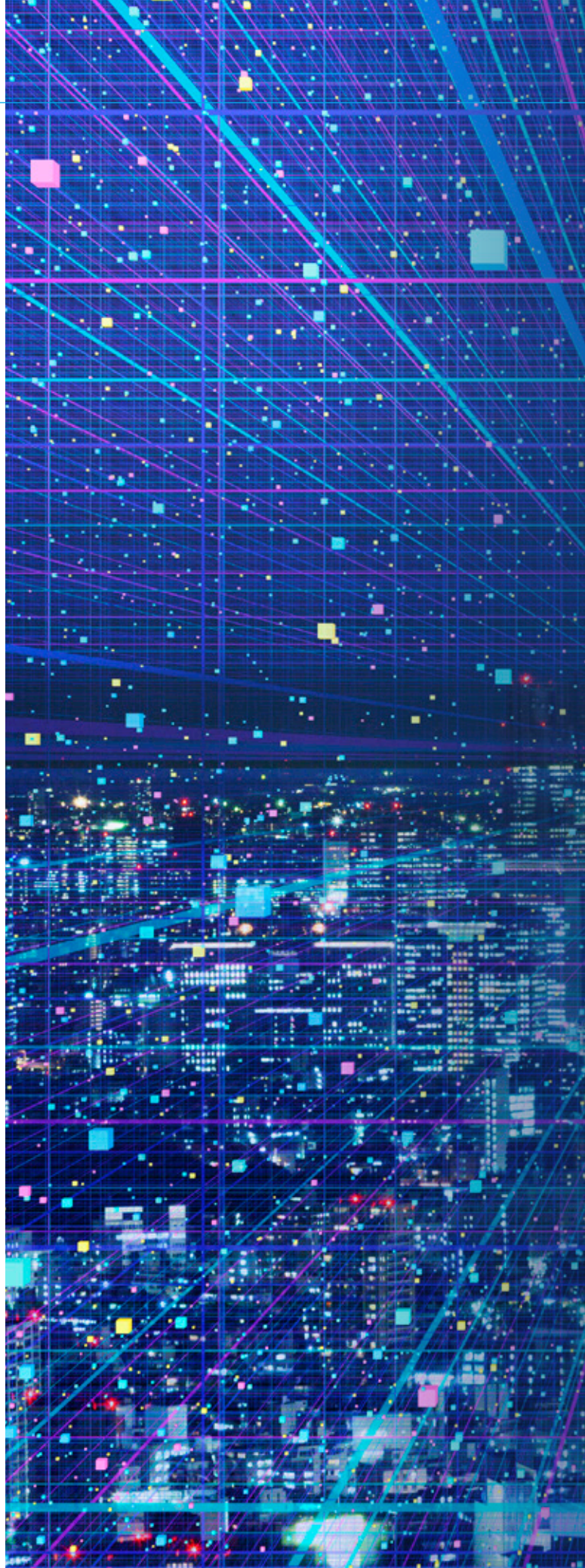
De petits ajustements dans les modèles cyber peuvent considérablement amplifier les variations des résultats modélisés. Par exemple, la méthode de calcul des marges bénéficiaires pour les pertes liées à l'interruption d'activité a un impact important sur les pertes modélisées. De même, la manière dont les différents types de mesures de sécurité sont représentés dans un portefeuille et au niveau de chaque entreprise peut influencer fortement les pertes potentielles. Une autre priorité, obstruée par les systèmes existants malgré les efforts importants déployés par certains acteurs du secteur, est l'amélioration de la qualité des données. Lorsque cette qualité est améliorée (notamment lors de la souscription), elle réduit l'incertitude liée au risque sous-jacent, permettant ainsi un déploiement plus efficace du capital. Cela va de l'information firmographique sur l'entreprise assurée (comme la saisie correcte de l'URL du site web) aux informations relatives aux polices (comme les sous-limites de couverture). Certains outils de traitement des données permettent d'automatiser ces processus, mais ils ne sont pas encore largement utilisés ni pleinement fiables.

Évolution du produit

La gamme de produits d'assurance cyber directe est restée relativement stable pendant plus d'une décennie. Les couvertures ont été ajustées et mises à jour pour refléter les nouvelles technologies et expositions, mais la structure fondamentale d'une offre large, englobant risques subis par l'assuré et envers ses tiers (y compris les pertes d'exploitation), a été au cœur du succès du marché jusqu'à présent. Pour soutenir les attentes de croissance du marché, il est peut-être temps de repenser en profondeur la structure des produits. Cela pourrait inclure des structures de produits plus économiques, offrant une couverture uniquement pour ce que l'entreprise perçoit comme son exposition maximale – par exemple, ne couvrir que certains types de dommages subis par l'assuré résultant des attaques les plus sophistiquées, avec une réduction correspondante des primes. Lockton Re a déjà discuté des avantages de la séparation des risques de subis par l'assurés et envers ses tiers, et il existe encore un potentiel pour rationaliser la distribution de cette manière[15].

D'autres opportunités pour développer les produits d'assurance cyber incluent l'intégration de produits d'assurance avec d'autres solutions de cybersécurité. De nombreuses initiatives ont été menées dans ce domaine, notamment l'offre d'assurance associée à l'adoption de services cloud. Par ailleurs, l'assurance a parfois été combinée avec des logiciels de sécurité. À ce jour, peu d'exemples montrent que cette approche a permis une adoption réussie. Compte tenu des multiples catégories d'assurance impliquant une offre d'assurance associée à d'autres solutions de gestion ou de distribution des risques, une attention accrue est nécessaire pour soutenir une proposition de valeur plus large.

[15] https://global.lockton.com/re/en/news-insights/the-all-risk-cyber-arc-challenge-an-assessment-to-simplify-cyber-reinsurance



Conclusion

Plusieurs obstacles freinent les attentes de croissance du marché de l'assurance cyber d'ici la fin de la décennie. On observe une convergence de défis techniques, opérationnels et liés aux données, tandis qu'un excédent de capacité à court terme crée des conditions qui pourraient rendre les projections du marché exagérées. Les (ré)assureurs sont confrontés à une incertitude inévitable et persistante en raison de la complexité et de la rapidité de l'évolution des infrastructures numériques et acteurs malveillants. La modélisation du risque cyber en est encore à ses balbutiements, compliquée par des données incomplètes ou peu fiables, souvent issues de systèmes hérités ou d'informations de souscription insuffisantes. Par conséquent, il est difficile de tarifer correctement les risques et d'allouer efficacement le capital. Ces problèmes sont amplifiés par la nature statique de la plupart des offres de produits actuelles, qui peinent à s'adapter à l'évolution des besoins des clients et aux contours nuancés des menaces cyber émergentes.

La bonne nouvelle est que l'innovation suit rarement une trajectoire linéaire et, bien qu'elle puisse être chaotique et engendrer des conséquences imprévues, l'enthousiasme pour les opportunités offertes par le marché ne manque pas. Nous pouvons tirer des leçons de l'expérience d'autres secteurs, et avec l'impact croissant de l'amélioration rapide de la puissance de calcul, de nombreuses raisons nous incitent à rester optimistes quant à la solidité à long terme du secteur de l'assurance cyber.

Mark Greisiger, président-directeur général de Netdiligence et acteur chevronné du marché, exprime un sentiment positif. Il déclare : 'Les assureurs recrutent des souscripteurs techniques, et le tri des comptes ainsi que l'efficacité des processus s'améliorent, ce qui constitue un indicateur précurseur favorable. L'investissement dans les services de gestion des risques se poursuit pour soutenir les clients, ce qui démontre la valeur perçue par ces derniers. De plus, l'assurance cyber devient de plus en plus souvent une obligation contractuelle, stimulant ainsi la souscription.'

> “Nous pouvons tirer des leçons de l'expérience d'autres secteurs, et avec l'impact croissant de l'amélioration rapide de la puissance de calcul, de nombreuses raisons nous incitent à rester optimistes.”

Les trois axes principaux à aborder pour atteindre la croissance attendue du marché sont:

1. **L'amélioration des outils et de la qualité des données pour mieux comprendre le risque des portefeuilles**
2. **La poursuite des investissements dans des modèles plus granulaires pour atténuer le risque systémique**
3. **Des produits flexibles et ciblés pour améliorer la distribution**

Le marché de l'assurance cyber se trouve à un carrefour dynamique, façonné par l'évolution des cadres réglementaires, l'augmentation de la fréquence des incidents et la complexité croissante des dépendances technologiques. En favorisant une meilleure adéquation entre les exigences réglementaires, les attentes des investisseurs et les réalités technologiques, le secteur peut non seulement relever les défis actuels, mais également ouvrir de nouvelles voies de croissance et de résilience à l'ère numérique.

Authors and Contacts

AUTHORS

Contacts

Londres

Oliver Brew ACII
Responsable du Centre d'Excellence

+44 (0)7384 248 268
oliver.brew@lockton.com

New York

Brian Lewis
Responsable Cyber, Amérique du Nord

+1 646 279-1940
brian.lewis@lockton.com

CONTACTS

London

Matthew Silley FIA
Responsable du courtage international en cybersécurité

+44 (0)7391 387 699
matthew.silley@lockton.com

Jemima Hopper ACII
Courtière

+44 (0)7855901856
jemima.hopper@lockton.com

New York

Jaimie Hunter
Courtière principale

+1 718 288 5337
jaimie.hunter@lockton.com

Chris Wafer
Courtier principal

+1 646 993 5029
cwafer@lockton.com

Caitlin Barnett
Courtière

+1 929 675 9132
caitlin.barnett@lockton.com

MEDIA CONTACTS

London

Isabella Gaster
Lockton Re Directrice Marketing monde

+44 (0)7795 400981
isabella.gaster@lockton.com

New York

Elizabeth Miller Kroh
Lockton Re Responsable Marketing, Amérique du Nord

+1 (445) 248 2228
elizabeth.kroh@lockton.com

Sources

1. "Cyber Insurance: Risks and Trends 2025 | Munich Re," Munich Re, updated March 4, 2025, https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html

2. Ronit Sharma, Nesa Kashyap, 2024. "Cybersecurity Insurance Market Size, Share, Trends, & Insights Report, 2035." Rootsanalysis.com. Roots Analysis. January 20, 2024. https://www.rootsanalysis.com/cybersecurity-insurance-market

3. Beth Musselwhite. 2024. "Beazley Forecasts Cyber Insurance Market to Grow to $40bn by 2030 - Reinsurance News." ReinsuranceNews. October 2, 2024. https://www.reinsurancene.ws/beazley-forecasts-cyber-insurance-market-to-grow-to-40bn-by-2030/

4. Market Segment Report: US Cyber: Pricing Cuts Bring First Ever Reduction in Direct Premiums Written (AM Best, 2025), https://www3.ambest.com/ambv/sales/bwpurchase.aspx?record_code=354887&AltSrc=22&AltServ=640 (paywall)

5. Alex Kimura et al., Insurance Practice Global Insurance Report 2025: The Pursuit of Growth (McKinsey & Co., 2024), https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/global%20insurance%20report%202025/global-insurance-report-2025-the-pursuit-of-growth.pdf

6. "Reality Check on the Future of the Cyber Insurance Market," Swiss Re, updated November 18, 2024, https://www.swissre.com/riskknowledge/advancing-societal-benefits-digitalisation/aboutcyber-insurance-market.html

7. ibid

8. "Don't Put All Your Eggs in One Basket." n.d. Grammar-Monster.com https://www.grammar-monster.com/sayings_proverbs/dont_put_all_your_eggs_in_one_basket.htm

9. Ronald J. Levine, Alan R. Lyons, Barry Werbin, "Cyber Liability Insurance: What to Look for When Obtaining Coverage." 2014. Herrick, Feinstein LLP. October 2014. https://www.herrick.com/publications/cyber-liability-insurance-what-to-look-for-when-obtaining-coverage/

10. "Hosting and cloud computing market size worldwide 2010-2020" n.d. Statista. https://www.statista.com/statistics/500541/worldwide-hosting-and-cloud-computing-market/

11. "Latest 2025 Cloud Solutions Statistics | IT Desk," IT Desk, updated July 10, 2025, https://www.itdeskuk.com/latest-cloud-statistics

12. Richard Betterley, "Maybe next Year" Turns into "I Need It Now" (The Betterley Report, 2014), http://betterley.com/ samples/cpims14_nt.pdf

13. Felix Richter, The Big Three Stay Ahead in Ever-Growing Cloud Market (Statista, 2025), https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloudinfrastructure- service-providers/

14. "From Fiction to Reality: How Latin America Became the World's Most Critical Cyber Battleground," World Bank Blogs, November 28 2024, https://blogs.worldbank.org/en/latinamerica/seguridadcibernetica-en-america-latina-y-el-caribe

15. "The All Risk Cyber (ARC) Challenge – an Assessment to Simplify Cyber Reinsurance | Lockton." 2023. Lockton. 2023. https://global.lockton.com/re/en/news-insights/the-all-risk-cyber-arc-challenge-an-assessment-to-simplify-cyber-reinsurance

LOCKTON®

REINSURANCE

www.locktonre.com

261 Fifth Avenue, New York • NY 10016

The St. Botolph Building, 138 Houndsditch • London EC3A 7AG

#0810_08.25