PAYSAGE CYBER SÉCURITAIRE

Tendances mondiales

INTERVALLE
TECHNOLOGIES

Tendances mondiales en matière de cybersécurité

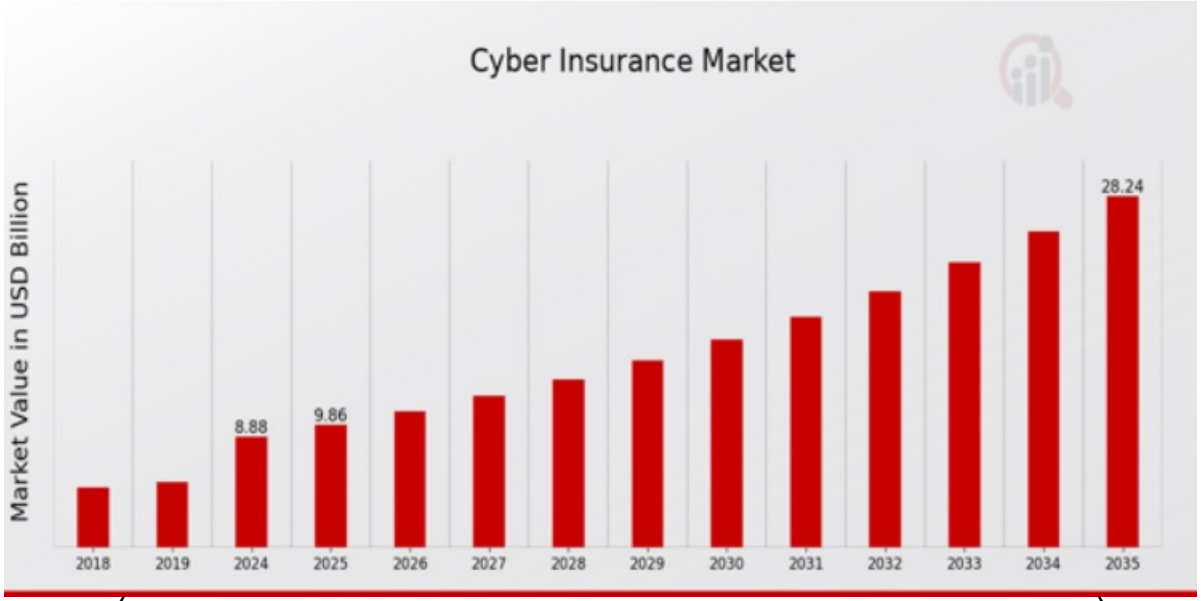
- **10 500 milliards $ /an** à fin 2025, contre 3000 milliards $ il y a dix ans, est le coût total de la cybercriminalité (***Statista***).
- Augmentation des attaques de **4151 %** depuis le lancement du ChatGPT (***SlashNext***)
- **95%** des attaques motivées par un gain financier
- **4.88 million $,** coût moyen d'une violation (***IBM)***
- **60 %** des PME / PMI ne se remettent jamais d'une violation majeure (***US National Cyber Security Alliance***).
- **70 %** des violations ont entraîné des perturbations opérationnelles importantes / très importantes (***IBM***).
- **3,58 millions $** est le coût moyen de récupération d'une attaque de ransomeware (***Sophos***).
- **63%** des demandes de ransomware **> 1 million $**;
- **30%** des demandes de ransomware **> 5 millions $**.

MARCHÉ DE LA CYBER-ASSURANCE

Tendances mondiales

Principales tendance du marché de la cyber-assurance

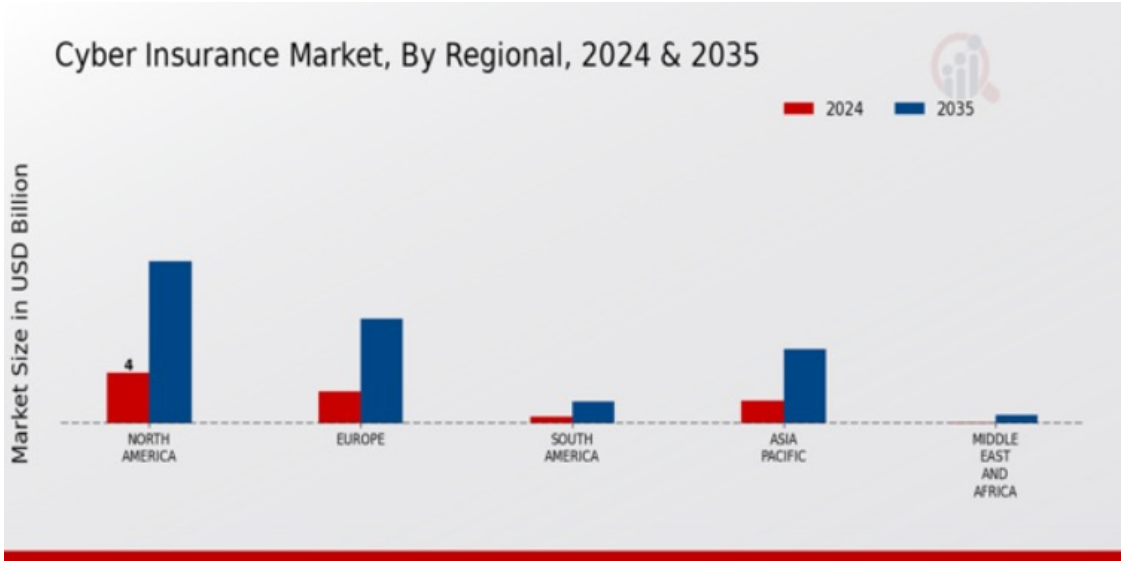
- Augmentation des cybermenaces et des incidents
- Coût moyen des violations de données ~ 4M$
- Exigences réglementaires renforcées
- Adoption de la transformation numérique



(***https://www.marketresearchfuture.com/reports/cyber-insurance-market-8635***)

Principales tendance du marché de la cyber-assurance

	2024	2035
Amérique du Nord	4M$	12,75M$
Europe	2,5M$	8,25 M$
Amérique du Sud	0,5 M$	1,75M$
Asie-Pacifique	1,8M$	5,85M$
Moyen-Orient et de l'Afrique	0,08M$	0,64M$



(*https://www.marketresearchfuture.com/reports/cyber-insurance-market-8635*)

Challenges des cyber-assureurs

- **Manque de normalisation dans la rédaction des polices cyber-assurance :** la diversité dans les couvertures est source de confusion chez les assurés et de malentendus lors de sinistres décourageant les assurés.
- **Paysage des cyber-menaces en constante évolution :** notamment avec l'utilisation des technologies émergentes (Ransomware-as-a-service, Deepfakes, …) forçant les assureurs à mettre à jour les modèles de risque et les conditions de couverture de façon continue pour rester pertinents.
- **Données historiques limitées pour la modélisation actuarielle :** ne permettant pas aux assureurs de quantifier les risques avec précision. D'où des tarifs jugés excessifs et des couvertures
- **Coûts élevés des sinistres et gravité des pertes :** liés aux responsabilités juridiques, efforts de récupération des données, interruptions d'activité, paiements de rançons et atteinte à la réputation dépassant souvent les estimations initiales et pesant sur les assureurs.
- **Agrégation des risques et exposition systémique :** en raison de l'interconnexion des systèmes informatiques et des fournisseurs de services communs, compliquant la gestion du risque d'accumulation pour les assureurs.

DEVELOPPER UN MARCHE PERTINENT DE LA CYBER-ASSURANCE

Cadre juridique

La constitution d'un marché de l'assurance du risque cyber passe par une clarification de son cadre juridique

Initier une coopération entre les décideurs politiques, les experts en cybersécurité et la société civile, pour l'élaboration et la mise en place des politiques et réglementations en s'appuyant sur des pratiques régionales et internationales existantes;

- **Normaliser la terminologie** et clarifier les garanties & exclusions afin d'améliorer la transparence et l'adoption des cyber-assurances
- **Définir les couvertures de la cyber assurance :** par la détermination des risques à couvrir pour obtenir une protection adaptée aux menaces actuelles (couverture dommages directs et responsabilité civile)
- **Fixer les obligation de souscription:** introduire, dans un premier temps, les pratiques de la cyber-assurance comme une initiative volontaire, pour l'exiger dans un deuxième temps pour les Opérateurs d'Importance Vitale (OIV) et les Opérateurs de Services Essentiels (OSE), et ainsi de suite…
- **Encadrer les conditions de prise en charge des sinistres liés aux cyberattaques** : clarifier les obligations des assureurs et des assurés en matière de prévention et de déclaration des risques.
- **Sensibiliser les entreprises sur l'importance de la cyber assurance** et la nécessité de renforcer leur résilience face aux menaces numériques et la nécessité de notification en cas de faille
- **Définir des procédures claires et simplifiées de déclaration** en cas de sinistre.

Quantifier les risques Cyber (CRQ)

Une approche basée sur les risques pour les évaluations des risques cyber

La quantification des risques cyber se base sur la mesure de l'impact financier, les pertes financières ou la probabilité des menaces cyber à travers une évaluation des risques cyber.

1. Rôle des Assurés / Entreprises :

- RSSI et équipes de gestion des risques doivent définir **le profil de risque de l'entreprises** en exploitant les données internes générées par les systèmes de sécurité (tentatives d'intrusion, alertes de sécurité ou des incidents mineurs, …).
- **Traduire ces défis en termes financiers** et les communiquer à la direction pour la convaincre de souscrire à une cyber assurance, et afin que les ressources puissent être allouées avec des résultats défendables et reproductibles.
- Prendre des **mesures proactives** pour minimiser l'exposition :
  - ✓ Investir dans la cybersécurité : contrôles d'accès stricts, gestion des vulnérabilités & Patch management, pentests, ...
  - ✓ Sensibiliser les employés aux risques de phishing et d'attaques par ingénierie sociale
  - ✓ Cryptage des données sensibles pour les protéger en cas de violation et à réduire les coûts potentiels d'une fuite de données.

Quantifier les risques Cyber (CRQ)

2. Rôle des Assureurs :

- **Modélisation précise des risques réalisée** par des experts en modélisation actuarielle et cyber threat intelligence, pour éviter une mauvaise tarification des polices.
- Création de **bases de données sinistres mutualisées** (cyber insurance pools)
- Utilisation des nouvelles technologies, tels que **l'IA & Machine learning** pour une évaluation plus dynamique et personnalisée du profil pour des offres assurantielles mieux calibrées et pour suivre le rythme de l'évolution des menaces.
- Ajuster la **tarification en fonction de l'exposition réelle**, garantissant ainsi la rentabilité tout en maintenant des tarifs compétitifs.
- **S'appuyer sur des professionnels de la cybersécurité / courtiers:**
  - ✓ Pour l'évaluation du profil de risque de l'assuré (questionnaire, audit, scoring…), la traduction du risque technique en risque assurable, et la constitution du dossier de souscription.
  - ✓ Accompagnement post-souscription : Formation, Audit & monitoring proactif, Scans de vulnérabilités, Réponse aux incidents, déclaration, Coordination avec les experts techniques (forensics, juridique, communication de crise), ….

Developper des garanties Cyber

- Evaluer la maturité en cybersécurité de l'assuré (Questionnaire, Audit préalable)
- Expliciter les clauses de couverture et d'exclusion des risques cyber (Garanties de base et garanties optionnelles)
- Définir les conditions d'éligibilité à une suscription (Existence d'un RSSI, Politique de sécurité, politique de sauvegarde, contrôle d'accès MFA, Plan de réponse aux incidents, plan de continuité d'activité, …).
- Renforcer l'information des assurés sur la couverture ou l'absence de garantie du risque cyber.
- Offrir des bonus/malus ou des remises pour les clients proactifs.
- Proposer un pack d'accompagnement cyber intégré à l'offre pour créer une vraie valeur ajoutée pour le client : hotline 24/7, cellule de gestion de crise (technique, juridique, communication), outils de sensibilisation pour les collaborateurs, monitoring externe (dark web, fuites, vulnérabilités)
- Prévoir des procédures de déclaration, d'analyse et de règlement standardisées.

Developper des garanties Cyber

Garantie principale	Garanties optionnelles	Exclusion typique
• Frais d'enquête et de remédiation (Forensic, communication). • Responsabilité civile en cas de fuite de données. • Interruption d'activité liée à un incident cyber. • Cyberextorsion (ransomware). • Frais juridiques et réglementaires. • Frais liés à la restauration des systèmes et données.	• Accompagnement en prévention (audit, formation, tests d'intrusion). • Accompagnement post-incident (Assistance dans la réponse aux incidents)	• Acte de guerre • Faute intentionnelle • Non respect des obligations minimales de sécurité

INTERVALLE TECHNOLOGIES