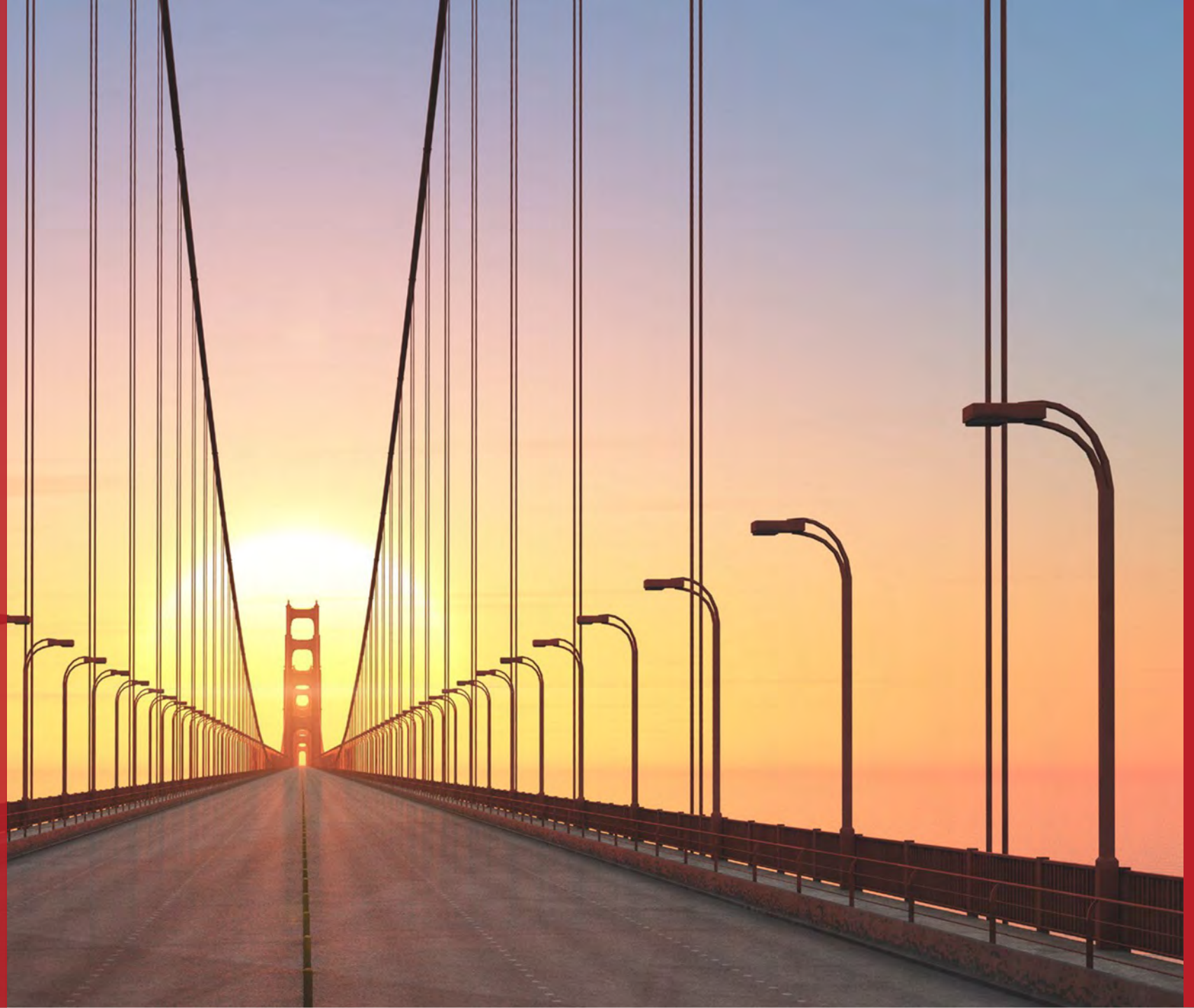
Chedid Re
Afrique
Ensemble, et toujours plus loin.

LA CYBER ASSURANCE

07/2025

Groupe Chedid Capital



Évolution des priorités en matière de risques – 2025

2014	2018	2022	2023	2024	2025
BI - Supply Chain Disruptions	BI - Supply Chain Disruptions	Cyber	Cyber	Cyber	Cyber
Natural Catastrophes	Cyber	BI - Supply Chain Disruptions	BI - Supply Chain Disruptions	BI - Supply Chain Disruptions	BI - Supply Chain Disruptions
Fire, Explosion	Natural Catastrophes	Natural Catastrophes	Macroeconomic Developments	Natural Catastrophes	Natural Catastrophes
Changes in Regulation and Legislation	Market Developments	Pandemic Outbreak	Energy Crisis	Changes in Regulation and Legislation	Changes in Regulation and Legislation
Market Stagnation or Decline	Changes in Regulation and Legislation	Changes in Regulation and Legislation	Changes in Regulation and Legislation	Macroeconomic Developments	Climate Change
Loss of Reputation and Brand Value	Fire, Explosion	Climate Change	Natural Catastrophes	Fire, Explosion	Fire, Explosion
Intensified Competition	New Technologies	Fire, Explosion	Climate Change	Climate Change	Macroeconomic Developments
Cyber	Loss of Reputation and Brand Value	Market Developments	Shortage of Skilled Workforce	Political Risk and Violence	Market Developments
Theft, fraud corruption	Political Risks and Violence	Shortage of Skilled Workforce	Fire, Explosion	Shortage of Skilled Workforce	Political Risk and Violence
Quality deficiencies / defects	Climate Change	Macroeconomic Developments	Political Risk and Violence	Energy Crisis	New Technologies

Référence: AM Best

Cybersécurité en Afrique : Statistiques et Tendances 2024

Au regard de ses efforts dans le développement du numérique, l'Afrique est un marché en pleine mutation digitale mais doit faire face à la montée en puissance de la cyber criminalité.

>3.5 Mds $

Pertes Annuelles

+14%

Attaques Spyware

Ransomware & BEC

Ransomware & BEC menaces #1 (Interpol African Cyberthreat Report 2024)

Grands Secteurs Touchés

Énergie
Portuaire
Banques
Télécoms

- **Cyber = Risque n° 1 pour les entreprises africaines:** 38 % des répondants au 'Allianz Risk Barometer 2025' placent les incidents cyber en tête, devant l'interruption d'activité et les catastrophes naturelles.
- L'escalade **financière** et **technologique** confirme l'urgence d'investir dans la prévention et l'assurance (chiffres présentés sur la diapositive).
- **Énergie, transport/logistique, import-export, pétrole & gaz, finance et services publics** – aucune industrie n'est épargnée, d'où la nécessité de polices cyber sur-mesure et d'une gestion fine des accumulations par ligne d'activité.

Évolutions Réglementaires

2023

- **Nigeria**: Signature du Nigeria Data Protection Act (NDPA)
- **Algérie: Pleine application de la Loi 18-07** sur la protection des données - Fines 20,000 - 1,000,000 DZD + peines d'emprisonnement ; obligation de localisation des données.

2024

- **Kenya: Premiers pénalités ODPC (KES 5M)** contre des entreprises (Whitepath, Oppo)
- **Arabie Saoudite:** Révision du Cyber-Security Framework (SAMA CSF)

2025

- **Botswana: Data Protection Act 2024 entre en vigueur** - Amendes jusqu'à BWP 50M ou 4% du CA; notification de violation en ≤ 72 h; 45 pays reconnus « adéquats » pour les transferts.

Principaux Risques liés aux Cyberattaques

1

Violations de Données / Data Breaches

2

Cyberattaques ciblant les infrastructures critiques et les actifs physiques

3

Augmentation des attaques par logiciels malveillants / rançongiciels - Hausse des attaques de spoofing (usurpation) d' e-mails professionnels

4

Perturbations dues à la défaillance des chaînes d'approvisionnement numériques, des plateformes cloud et des services

Dommages liés aux Cyberattaques

Dommages Directes	Domage Indirectes
Remédiation technique: Restauration des systèmes, purges de logiciels malveillants, renforcement d'urgence des contrôles	**Atteinte à la réputation**: Perte de confiance des clients, érosion de l'image de marque
Interruption d'activité (pertes d'exploitation): Arrêt de la production ou des services en ligne	**Perte de clientèle et de parts de marché**: Départ vers des concurrents perçus comme plus sûrs
Paiement de rançon / extorsion: Règlements en crypto-monnaie ou négociations spécialisées	**Hausse des coûts de financement et des primes d'assurance**: Perception de risque accru par investisseurs et assureurs
Frais d'enquête & de notification: Forensique numérique, information des personnes concernées, call-centers	**Actions juridiques collectives** et recours de tiers (partenaires, fournisseurs)
Amendes et sanctions réglementaires: Non-respect du RGPD, des lois locales sur la protection des données	**Perte d'avantage concurrentiel**: Divulgation de secrets commerciaux ou de propriété intellectuelle
Honoraires de services d'urgence: Conseil juridique, gestion de crise, relations publiques immédiates	**Impact à long terme sur la valeur de l'entreprise**: Baisse durable du cours boursier ou de la valorisation

Protection

Couverture d'Assurance

- Frais de surveillance du crédit
- Frais d'extorsion cyber
- Frais de restauration des données
- Frais d'investigation forensic
- Frais de représentation juridique
- Frais de notification
- Frais de relations publiques
- Frais de remplacement et de réparation du matériel

Bonnes pratiques de sécurité

- Équipe SOC
- Solution EDR (Endpoint Detection & Response)
- Analyse des vulnérabilités
- Protection des données (chiffrement, DLP)
- PCA : Plan de continuité d'activité
- Sensibilisation et formation

Réponse à un Incident de Cybersécurité

- Notification Immediate
- Rappel d'un Incident Manager
- Enquête Initiale du CIMT
- Mobilisation du Panel d'Experts
- Engagement des Parties Prenantes & Gestion de Crise
- Résolution et Clôture

Assurance Cyber 2025

- **Marché stable mais concurrentiel:** AM Best maintient une perspective *Stable* pour l'assurance cyber mondiale en 2025; la détente tarifaire se poursuit, mais la demande et la rentabilité demeurent solides grâce à une meilleure hygiène cyber chez les assurés.

- **Trajectoire de croissance soutenue**: Les primes cyber mondiales ont augmenté de **7% en 2024 pour atteindre env. 15,3 Mds USD** et devraient croître de **> 10 % par an jusqu'en 2030**, portées par les PME et les marchés hors-États-Unis (Europe, Asie).

- **Vent favorable de capital et capacité**: Réassurance et capitaux alternatifs continuent d'affluer; **> 750 M USD** d'obligations « cyber cat » émises en 2024, tandis que le basculement vers des couvertures non proportionnelles accroît la protection contre les sinistres majeurs.

- **L'IA, arme à double tranchant**: Les assureurs exploitent l'IA pour la sélection et la tarification en temps réel, mais les cybercriminels l'utilisent aussi pour industrialiser rançongiciels, BEC et fraudes aux virements, augmentant fréquence et sévérité potentielles.

- **Projecteur sur le systémique & la réglementation**: Des pannes d'envergure (CrowdStrike, CDK) révèlent le risque d'accumulation, tandis que le durcissement des lois sur la protection des données (Cybersecurity Act de l'UE, normes CISA, obligations sectorielles) pousse toujours plus d'entreprises à souscrire ou élargir leur couverture cyber.

MERCI