Webinaire

Se prémunir des risques cyber: cas des banques, assurances, opérateurs télécoms et fintechs

Mercredi 17 janvier 2024 **13h30 (GMT+1)**

Modératrice

Patricia Pedhom Nono
Associée
PwC

Intervenants

Didier Simba
Président du CESIA
Manager Général DSTrust

Georges Mpoudi Ngole
Managing Director
Cybastion Infrastructure

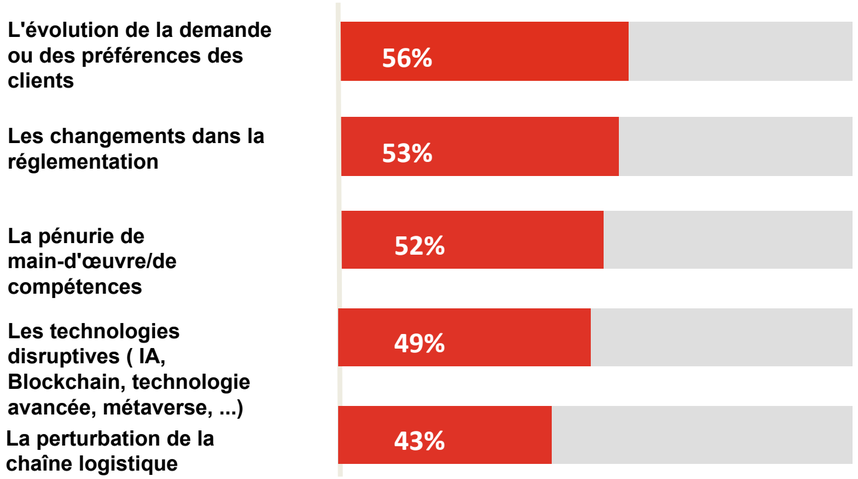
Ghimelle Karaboué
Directrice de la Sécurité des Systèmes d'Information
Groupe AFG

Lionel Beninga
Associé
PwC

Risques cyber, quels sont les enjeux ?

49%

Des dirigeants interrogés perçoivent la **technologie comme un défi majeur**, susceptible de compromettre la rentabilité de leur entreprise.

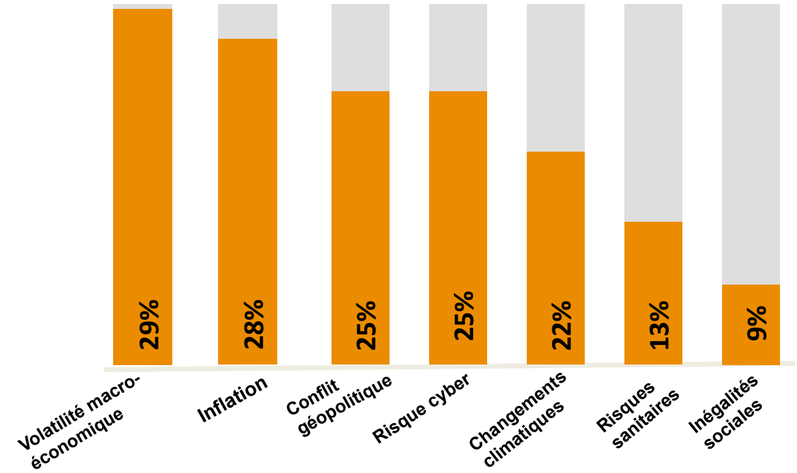


Source: PwC 26th CEO Survey

Selon le *PwC 26th CEO Survey*, la technologie se positionne parmi les cinq tendances majeures qui impacteront le paysage des affaires au cours des dix prochaines années, aux côtés des changements législatifs, de la pénurie de compétences et de l'évolution des besoins des consommateurs.

4ème

Le **risque cyber**, classé quatrième **parmi les cinq menaces tangibles** pouvant compromettre la rentabilité de toute entreprise, pour les cinq prochaines années.

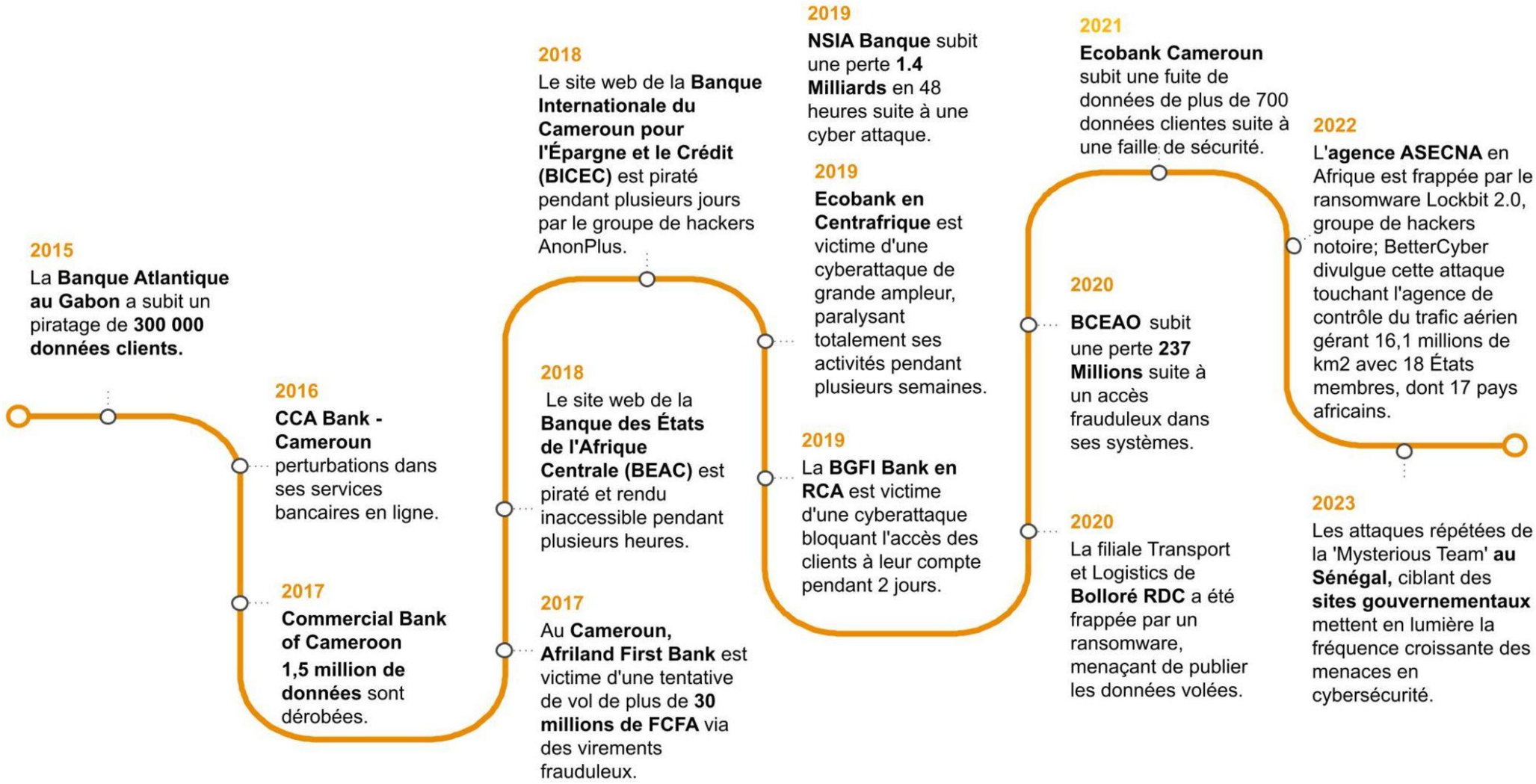


Source: PwC 26th CEO Survey

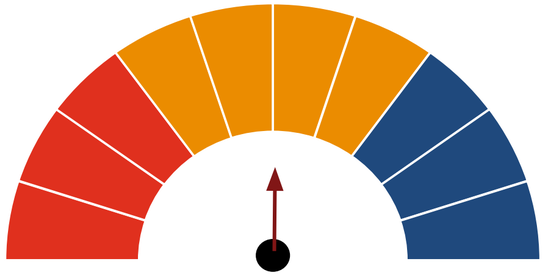
Les dirigeants, conscients des enjeux majeurs liés à l'intégration efficace de la technologie, mettent en lumière un aspect critique de l'ère actuelle : les risques cybernétiques. Selon le *PwC 26th CEO Survey*, ces derniers sont identifiés comme le quatrième risque le plus préoccupant pour les cinq prochaines années,derrière la volatilité macro-économique, l'inflation et les conflits géo-politiques

50%

d'**augmentation constatée** dans le secteur bancaire en **Afrique Centrale** pour les **incidents cybernétiques**, selon un rapport de la COBAC paru en 2020.



Le risque cyber en Afrique francophone subsaharienne ?



PwC *AFSS Cybersecurity Index

- ➔ Vue complète et externe de la posture globale de cybersécurité des entreprises analysées en Afrique Francophone.
- ➔ Indice ajoutant une mesure quantitative au processus d'évaluation de la sécurité des organisations de l'échantillon analysé
- ➔ Basé sur les données publiquement disponibles et recueillies dans le cyberespace sur 12 mois (Dec 22 - Dec 23)

Basique	280 - 700
Intermédiaire	710 - 810
Avancé	820 - 990
Idéal	1000

- ❏ Un score élevé dénote une meilleure posture en matière de sécurité globale.
- ❏ Une entreprise ayant un indice inférieur à 820 est **5 fois** plus susceptible de subir une cyberattaque qu'une entreprise ayant un indice équivalent à 1000.

Ces informations dévoilent l'empreinte numérique distinctive de chacune d'elles. Il est calculé en fonction des paramètres ci-dessous:

- Vos **informations sensibles** sont-elles présentes sur le **Dark Web**?
- Des moyens de communication et des ressources **non sécurisés** sont-ils utilisés par votre **personnel**?
- Existe t-il des antécédents d'incident… **non résolus** ?
- Y a t-il des vulnérabilités **visibles depuis l'extérieur** et potentiellement exploitables ?
- Les **configurations de sécurité** des équipements exposés sur internet sont-elles adéquates?

*AFSS : Afrique Francophone Subsaharienne

PwC AFSS Cybersecurity Index - 2023

4 Secteurs d'activité

Fintech, Telco, Banques, Assurances

+200 Entreprises analysées

Les entreprises sélectionnées figurent parmi les meilleures de leur secteur respectif

8 Pays couvrant 2 régions

Cameroun, Congo, Côte d'Ivoire, Gabon, Guinée équatoriale, République démocratique du Congo, Sénégal, Tchad.

Deux Régions (Afrique Centrale & Afrique de l'Ouest

+12 Mois d'études et de collecte de données

Données collectées de décembre 2022 à décembre 2023

Notes :

- ➔ En raison de la diversité des secteurs d'activité, **la taille de l'échantillon fluctue en fonction de chaque secteur**.
- ➔ Les classements par secteur d'activité sont établis en fonction de **la moyenne de l'indice de sécurité** de l'ensemble des entreprises analysées dans le secteur concerné.
- ➔ **Aucun test d'intrusion n'a été réalisé**. Les données analysées sont toutes accessibles sur le cyberespace.

Et si on présentait les résultats?

Les principaux vecteurs de risque

Par niveau de maturité

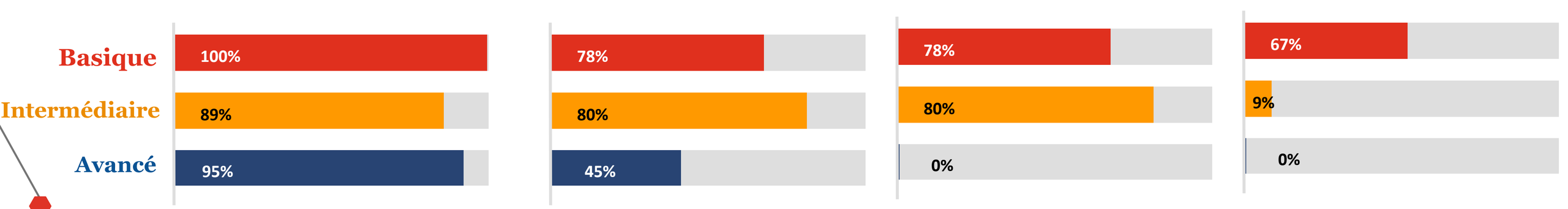
Selon notre étude, les quatre vecteurs principaux de risques exposant les entreprises en Afrique francophone sont :

92% — **Mauvaise hygiène réseau**

68% — **Vulnérabilités Technologiques**

53% — **Exposition aux Logiciels Malveillants**

13% — **Comportements à risque des utilisateurs**



- Plus de **9/10** des entreprises examinées ont une mauvaise hygiène réseau et ceci quelque soit leur niveau de maturité.

- Les entreprises de maturité élevée semblent bien maîtriser les risques d'exposition aux logiciels malveillants et du comportement utilisateur.

Les principaux vecteurs de risque

Par secteur d'activité

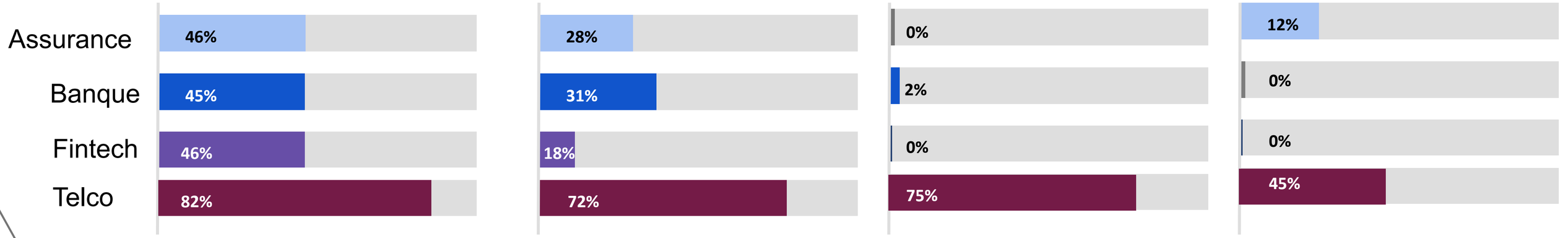
Selon notre étude, les quatre vecteurs principaux de risques exposant les entreprises en Afrique francophone en fonction des secteur d'activités sont :

1 **Mauvaise hygiène réseau**

2 **Vulnérabilités Technologiques**

3 **Exposition aux Logiciels Malveillants**

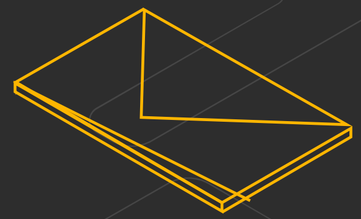
4 **Comportements à risque des utilisateurs**

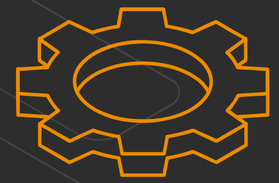


Les quatre facteurs de risque sont largement présents dans toutes les entreprises du secteur des télécommunications. Cependant, les secteurs de l'assurance, de la banque et des fintechs affichent des risques significatifs dus à une mauvaise hygiène de leur réseau. Les vulnérabilités technologiques, qui sont un autre risque à surveiller, se manifestent également à des niveaux relativement élevés dans tous les secteurs d'activité.

34%

seulement des entreprises analysées, tous secteurs confondus ont un Cyber Index de maturité avancé, bien qu’en deçà du niveau idéal





Perspectives par Secteur d'activités

Cybersecurity Index

FINTECH

1

Moyen

6/10 entreprises FINTECH analysées ont un score de maturité *Modéré*

++ La majorité des Fintechs analysées sont des acteurs dans les services financiers de paiement ou de transfert d'argent

ASSURANCE

2

Moyen

5/10 entreprises analysées ont un score de maturité *Modéré*

+70 compagnies d'assurances évaluées sur l'Afrique centrale et l'Afrique de l'ouest (Assurance vie, non vie, prévoyances sociales,...)

BANQUE

3

Moyen

3/10 seulement des banques analysées ont un indice de *maturité Élevée*

++ Niveau de maturité relativement meilleur, par rapport aux banques centrales et commerciales

+100 Banques analysées (banques commerciales, centrales et régionales)

TELCO

4

Faible

8/10 Telcos analysés ont un score de maturité *Faible*

100% des compagnies de télécommunications ont été analysées sur les pays de notre échantillon

Cybersecurity Index Idéal

1000

34% seulement des entreprises analysées ont un score de maturité *Avancé*

0% des entreprises analysées n'a atteint le score idéal.

890 Index le plus élevé sur l'échantillon des entreprises analysées

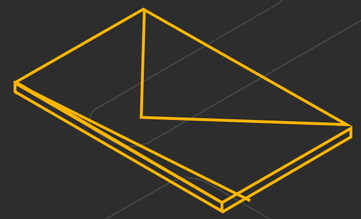
N’hésitez pas à nous contacter pour obtenir le zoom par secteur d’activités

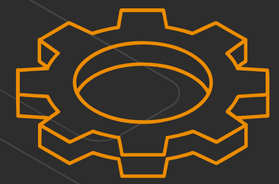
FINTECH

ASSURANCE

BANQUES

TELCO





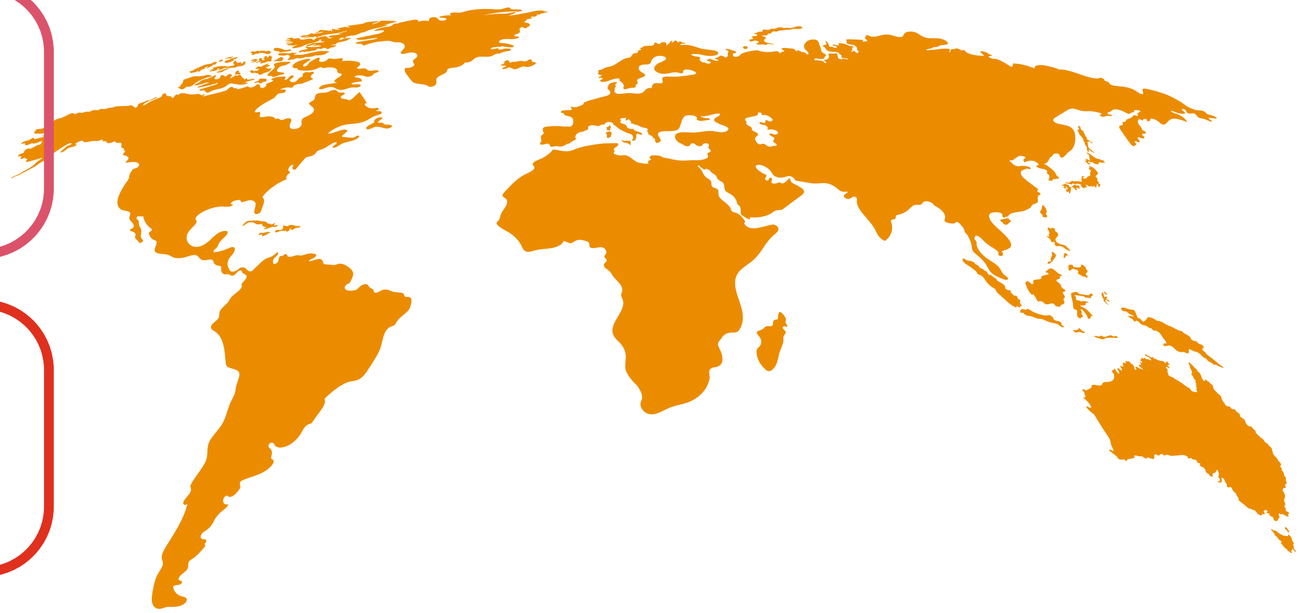
Pour résumer…

Faible - Moyen	Niveau de maturité général **variant de faible à moyen** sur l'échantillon analysé: le **secteur telco** étant **le plus exposé** suivi du **secteur bancaire**
34%	**Seulement** des entreprises analysées ont un niveau de **maturité élevé** y compris le secteur bancaire
67%	Entreprises ayant **un niveau de maturité basique** présentent un **risque "humain"** non négligeable, notamment en raison des ***comportements et usages risqués*** *de leur* ***personnel*** *sur le cyber espace*
9/10	Entreprises analysées ont comme principal **facteur de risque** leur **"hygiène réseau"**, notamment en raison *des configurations des actifs exposés sur internet*

Comment se différencie le top 5% ?

D’après le ***PwC 2024 Global Digital Trust Insights***, le top 5% des entreprises **les plus matures en termes de cybersécurité** sont positionnées pour accroître leur productivité et accélérer leur croissance, devançant la concurrence en se lançant dans les **nouvelles technologies** avec la certitude d'être **bien protégées**.
Les quatres pratiques clés qui les différencient des autres sont:

- Implémentation d'initiatives cyber-transformantes
- Adoption de technologies appropriées
- Mise à jour continue des plans de gestion de risques
- Maturité des pratiques de cyber résilience



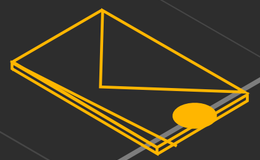
Pour aller plus loin…

Envie de connaître votre PwC Cybersecurity Index ?

Besoin d’en savoir plus sur vos failles de sécurité que nous avons déjà identifiées ?

Nécessité de réaliser un audit de sécurité et/ou de repenser votre stratégie “cyber-résilience”

N’hésitez pas à contacter nos experts cybersécurité !



Nos experts

Patricia Pedhom Nono

- PwC Afrique Francophone Subsaharienne
- Partner
- +237 690 70 75 22
- Patricia.Pedhom.Nono@pwc.com

Lionel Beninga

- PwC Afrique Francophone Subsaharienne
- Partner
- +241 11 76 23 71
- lionel.beninga@pwc.com

Mathis Bakary

- PwC Afrique Francophone Subsaharienne
- Senior Manager Cybersécurité
- +225 27 22 5 58400
- mathis.b.bakary@pwc.com

Lydie Ngo Nogol

- PwC Afrique Francophone Subsaharienne
- CISO
- +237 6 94 22 62 85
- lydie.ngo.nogol@pwc.com

Ghislain Nkoudjou

- PwC Afrique Francophone Subsaharienne
- Manager Cybersécurité
- +237 6 76 05 33 08
- ghislain.nkoudjou@pwc.com

Merci.

www.afrique.pwc.com