CESIA

CLUB D'EXPERTS DE LA SÉCURITÉ DE L'INFORMATION EN AFRIQUE

BAROMÈTRE DE LA CYBERSÉCURITÉ EN AFRIQUE

ÉDITION 2022

www.lecesia.com

Sommaire

ÉDITORIAL

Pour la deuxième année consécutive, le CESIA - CLUB D'EXPERTS DE LA SÉCURITÉ DE L'INFORMATION EN AFRIQUE publie son baromètre de la cybersécurité en Afrique. Une étude qui se veut qualitative et réalisée directement auprès de ses membres sur la période de décembre 2021 à janvier 2022.

La crise sanitaire liée au COVID-19 n'a pas eu un impact majeur sur les entreprises en Afrique. D'après l'édition 2021 du baromètre de la cybersécurité en Afrique seuls 10% des entreprises ont déployé le télétravail. Au fort de cette crise sanitaire, les entreprises ont su faire preuve de résilience et poursuivre leurs activités. Cela dit, à la faveur de cette crise, les Directions des Systèmes d'Information (DSI) ont été très fortement sollicitées pour prouver leur rôle stratégique. Les DSI étaient au pas de guerre pour des lancements, des déploiements ou encore l'accélération des projets de transformations digitales afin de garantir la continuité des activités des entreprises.

De son côté, le Responsable de Sécurité des Systèmes d'information (RSSI) était tenu de suivre la cadence de la DSI pour conseiller, prévenir, sécuriser et parfois gérer des incidents numériques dans le meilleur des cas sinon des crises cybers. De l'avis général, le RSSI a gagné auprès de la direction générale cette visibilité et ces lettres de noblesse tant espérées depuis longtemps, même s'il reste encore beaucoup à faire. Chacun a pris conscience que c'est bien grâce à la résilience numérique que la continuité des activités peut avoir lieu. Pour la seule année 2020, les experts de la cybersécurité s'accordent à dire que le nombre de cyberattaques aurait considérablement augmenté, la crise que nous traversons démontre que les investissements réalisés, ces dernières années en matière de sécurité numérique, n'ont pas été vains et ont permis une mise en place très rapide du télétravail dans certains cas.

En conclusion, les entreprises africaines sont mal préparées en matière de cybersécurité : une gouvernance cyber encore perfectible, un manque de formation et de sensibilisation, un manque de budget, un manque de ressources et des compétences dédiées à la cybersécurité, etc. sont autant de points qui ralentissent la mise en place d'un réel programme cyber en entreprise.

A PROPOS DU CESIA

Initié en fin 2019, le CESIA - CLUB D'EXPERTS DE LA SÉCURITÉ DE L'INFORMATION EN AFRIQUE est un espace d'échange et de partage d'expérience réservé aux décideurs et aux professionnels de la sécurité numérique exerçant en Afrique ou avec un intérêt pour le développement du secteur sur le continent.

Cette année, le CESIA compte 170 membres présents dans 18 pays en Afrique avec pour objectifs :

- PROMOUVOIR les métiers liés à la sécurité numérique face aux enjeux stratégiques des entreprises et des États ;
- FAVORISER LES ÉCHANGES entre experts et pouvoirs publics des pays Africains membres du club afin d'accompagner les évolutions réglementaires ;
- PARTICIPER AUX DÉMARCHES nationales et internationales ayant pour objet la promotion de la sécurité de l'information en Afrique ;
- ACCOMPAGNER LES ENTREPRISES ET LES ÉTATS africains dans leurs démarches de sécurité numérique ;
- SENSIBILISER les décideurs et les utilisateurs en Afrique aux enjeux de la sécurité numérique ;
- ACCOMPAGNER LE RSSI en lui proposant tous les outils nécessaires à l'accomplissement de sa mission de facilitateur de la transition numérique.

Contact :

contact@lecesia.com

www.lecesia.com

LES OBJECTIFS DU BAROMÈTRE

- Initié en 2019 avec une publication pilote sur 4 pays en Afrique, le BAROMÈTRE DE LA CYBERSÉCURITÉ EN AFRIQUE est désormais l'enquête annuelle du CESIA. Il se veut être une étude qualitative réalisée directement auprès de ses membres pour connaitre les enjeux de la cybersécurité en Afrique et sa perception au sein des entreprises et des pays membres ;

- Dans un second temps, notre enquête annuelle permet de mettre à jour la perception et la réalité de la cybersécurité en Afrique. Le BAROMÈTRE DE LA CYBERSÉCURITÉ EN AFRIQUE contribue à publier des chiffres dont manque cruellement le continent en matière de cybersécurité. Ces indicateurs sont un outil pour défendre des positions ou étayer une démonstration ;

- Enfin, BAROMÈTRE DE LA CYBERSÉCURITÉ EN AFRIQUE apporte des précisions sur l'impact des projets de transformation numérique au sein des entreprises ou des États en Afrique.

NOTRE MÉTHODOLOGIE

Notre **échantillon représente 170 membres du CESIA** présents dans **19 pays en Afrique**.

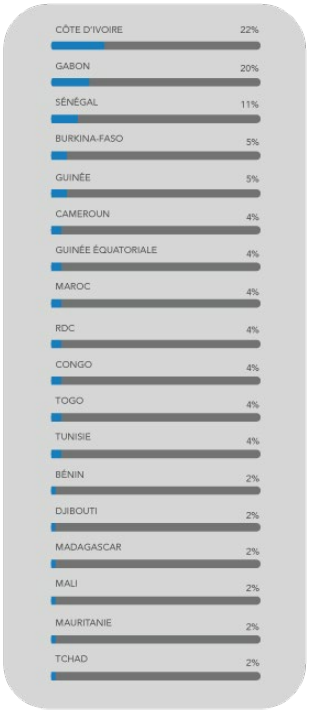
Près de **70% des répondants sont RSSI, 24% sont DSI et 6% sont DSSI.**

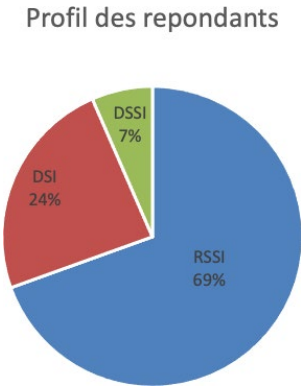
Notre enquête s'est déroulée du **1er décembre 2021 au 31 janvier 2022**.

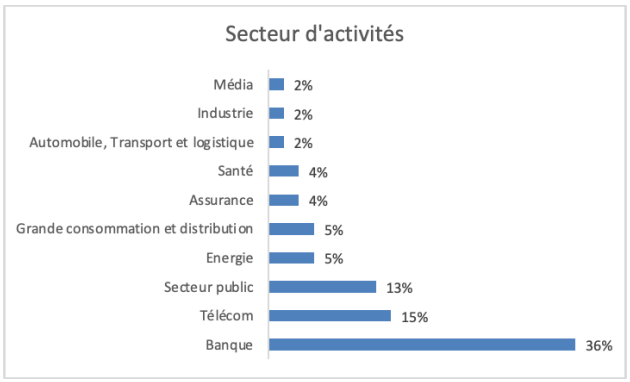
Les membres du CESIA ont été interviewés via un **formulaire en ligne**.

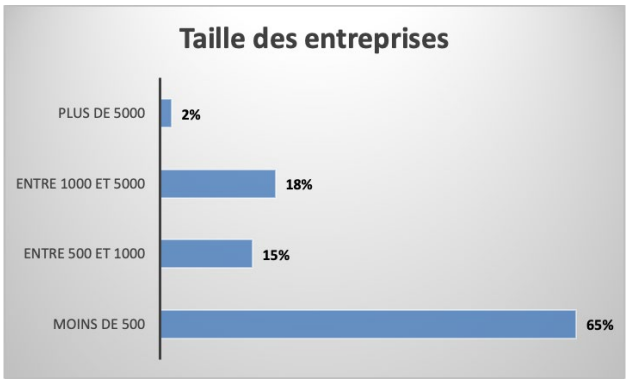
LES RÉPONDANTS

PARTICIPATION PAR PAYS









LE MOT DU PRÉSIDENT

Les nombreux projets de transformation digitale lancés dans plusieurs pays en Afrique couplé à leur accélération due à la crise sanitaire depuis 2020 complexifient de plus en plus les systèmes d'information dans les entreprises. Des entreprises de plus en plus interconnectées, des données dans le cloud ou encore des objets connectés dans l'entreprise, la cybersécurité doit s'imposer partout.

Depuis quelques années, la cybersécurité connait une évolution majeure qui prend en compte d'un côté l'évolution croissante des menaces et de l'autre la transformation des architectures, des solutions numériques et des organisations. À cela s'ajoute la disparité observée à travers les 54 États que contente le continent en matière de maturité en cybersécurité.

Cela dit, les professionnels de la cybersécurité ont besoin de partager des pratiques, des expériences. La compréhension des risques et le partages d'information sur les menaces et les pratiques sont essentiels dans l'exercice de leur fonction : le BAROMÈTRE DE LA CYBERSÉCURITÉ EN AFRIQUE s'impose donc comme un outil efficace pour suivre l'évolution des menaces et des enjeux de cybersécurité pour les entreprises et les États africains. Il constitue un réel atout stratégique pour appréhender le niveau de maturité du continent en la matière.

Cordialement.

Didier SIMBA

Fondateur et Président du CESIA

LES MESSAGES CLÉS

- 64% des entreprises disent avoir subi au moins une cyberattaque en 2021.
  Si cet indicateur est considérablement à la baisse en comparaison à l'année dernière (82% des entreprises étaient attaquées en 2020), il n'en demeure pas moins vrai que les conséquences sont considérables sur les activités de l'entreprise : Dans 43% des cas on constate une perturbation de la production pendant une durée significative ou l'impact sur l'image de marque. Pour un peu plus d'une entreprise sur 2, l'impact est négligeable.
  Dans près de 60% des cas, le vecteur d'attaque reste le Phishing, une légère baisse (69% en 2020), mais on constate aussi des tentatives de connexion non autorisées (34% contre 44% en 2020) et cette année, l'exploitation des vulnérabilités rejoint le podium au côté de l'ingénierie sociale dans 28% des cas (contre 29% en 2020).
  Ces légères baisses observées démontrent que les efforts consentis progressivement portent leur fruit même si 1 entreprise sur 3 se dit inquiète ou assez inquiète de faire face à une cyberattaque de grande ampleur, plus d'une entreprise sur deux pensent ne pas être prêtes à gérer une cyber-crise (52% en 2022contre 55% en 2020).

- La cybersécurité est une priorité pour les entreprises.
  Pour 48% des répondants, cela se démontre par un sponsoring du top management dans les projets de sécurité et pour 63% des entreprises, la gestion de la cybersécurité est internalisée. Pour se prémunir d'une crise cyber, les entreprises mettent en place des sauvegardes sécurisées dans 93% des cas. En plus des antivirus et les pares-feux, les entreprises se protègent en sécurisant les accès distants (55%) ou en filtrant les URL (33%).
  Comme l'année dernière, la grande majorité des entreprises ne dispose pas de programme de cyber-résilience (85% contre 71% en 2020).
  Par ailleurs, 89% des entreprises n'ont pas recours aux solutions innovantes issues des Start-up, dans la grande majorité des cas (39%) cela s'explique soit par un manque de connaissances des offres, soit une inquiétude sur la pérennité de l'entreprise ou encore un manque d'opportunité (28%).

- La sensibilisation des salariés est intensifiée.
  Si 61% des entreprises disposent d'un plan annuel de sensibilisation, 80% d'entre elles considèrent que les salariés sont bien sensibilisés aux cyber-risques. Cela dit, seulement 20% des entreprises déclarent que les salariés respectent les recommandations de sécurité numérique sans doute dû à l'absence de procédure

pour tester l'application de ces recommandations (20% des entreprises ne disposent pas de procédure pour tester le respect des recommandations et 48% n'en dispose « pas vraiment »).
Les experts de la cybersécurité, relèvent que les usages numériques des salariés présentent les risques suivants : l'utilisation des Devices personnels (37% contre 46% en 2020) et le Shadow IT monte à la 2e place (22% contre 16% en 2020).

- Pour l'avenir…
  65% des entreprises constatent une pénurie de compétence en Afrique, les entreprises ont besoin des profils de pilotage, organisation et gestion des risques (39%) ou encore de support et gestion des incidents (24%). 54% des entreprises comptent acquérir de nouvelles solutions techniques destinées à la protection contre les cyberattaques.

2022

Cette année, notre focus porte sur l'impact de la crise sanitaire liée au COVID-19.

Comme l'année dernière le télétravail reste un défi pour les professionnels de la sécurité numérique. Moins de 10% des entreprises en Afrique qui ont déployé le télétravail jugent trop risqué de mettre en place un tel dispositif et au nombre des risques, on note :

- Empêcher les fuites de données lorsque les utilisateurs sont livrés à eux-mêmes avec des outils collaboratifs déployés à la va-vite sans avoir pris le temps de les former à ces solutions très riches mais souvent très complexes à utiliser (74% contre 66% en 2020) ;
- Maintenir un niveau de sécurité satisfaisant du poste de travail quand celui-ci est en dehors des locaux et surtout lorsqu'il n'est pas connecté en permanence au réseau de l'entreprise (65% contre 85% en 2020) ;
- Être certain que le salarié en télétravail est bien celui qui est assis devant le PC de l'entreprise quand les sas de contrôle d'accès physique de l'entreprise ne sont plus là (52%).

Dans tous les cas, le budget attribué à la cybersécurité reste stable pour presque 40% des entreprises et pour la majorité a augmenté.

LES ACTIONS PRIORITAIRES À COURT/MOYEN TERME

METTRE EN PLACE ET/OU RENFORCER LES CELLULES DE CRISE

Face à la sophistication des cyberattaques et aux conséquences de plus en plus importantes pour les entreprises, il est plus que jamais indispensable de mettre en place une cellule de crise si ce n'est pas encore le cas. La cellule de crise doit être outillée et préparée via des exercices de gestions de crise cyber spécifique. Les attaques de type ransomware ou rançongiciel sont de plus en plus fréquentes en Afrique la maitrise de son impact nécessite une bonne organisation et préparation de la cellule de crise.

DÉSIGNER UN RÉFÉRENT DE SÉCURITÉ SI

La désignation d'un référent sécurité ou un Responsable de Sécurité des SI (RSSI) devrait se généraliser à tous les secteurs d'activités. Par ailleurs, 22% des RSSI au CESIA sont encore rattachés à la Direction des SI et le secteur bancaire est celui qui affiche une bonne maturité en matière de sécurité numérique.
Par ailleurs, le référent sécurité ou le RSSI doit impérativement disposer des moyens financiers et organisationnels pour exercer sa fonction. Il doit également être formé.

PROMOUVOIR L'AMÉLIORATION CONTINUE BASÉE SUR LA STRATÉGIE NATIONALE EN VIGUEUR DANS LE PAYS.

Environ 30% des pays membres du CESIA ne disposent pas d'un régulateur ou d'un cadre légal relatif à la cybersécurité dans leur pays.

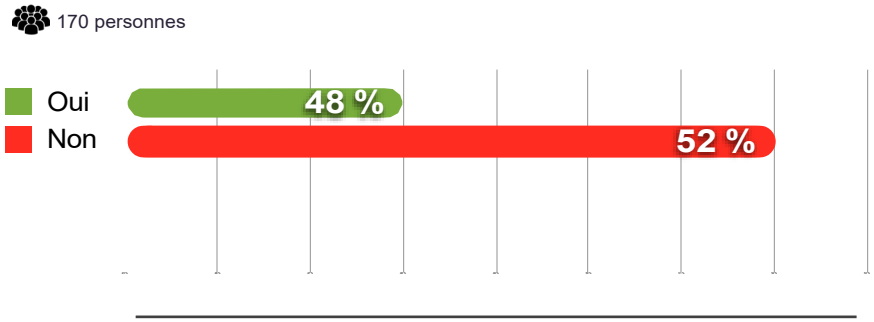
Chaque pays en Afrique doit mettre en place une Agence Nationale de la Sécurité des Systèmes d'information (ANSSI) ou équivalent afin de cadrer et réglementer le fonctionnement des entreprises et des États en matière de sécurité numérique car il en va de la souveraineté nationale.

ANALYSE DES RÉSULTATS

LA CONFIANCE DES ENTREPRISES FACE AUX RISQUES CYBER

Face aux risques cyber, les entreprises se sentent relativement en confiance…

Q8 : Selon vous, votre entreprise est-elle préparée à gérer une cyber-attaque ?

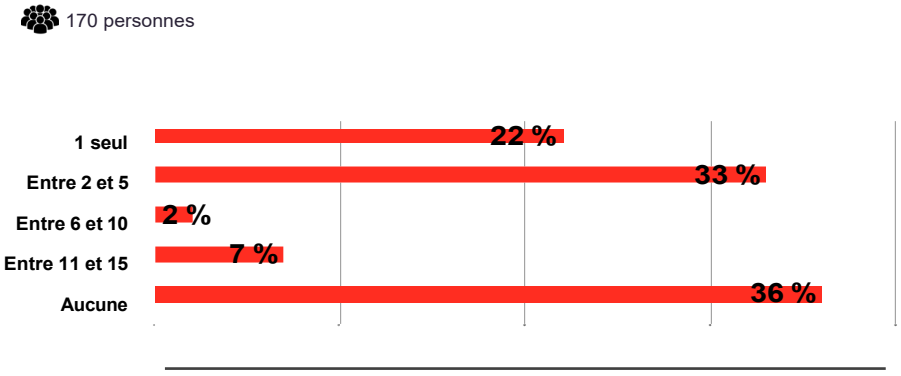


52% *des entreprises en Afrique déclarent ne pas être préparée à gérer une cyber-attaque.*

Définition du CESIA :

« Une cyber-attaque est un événement informatique ayant un impact significatif dans le temps pour l'entreprise sur l'image, les finances, l'organisation, le juridique ou la réglementation. »

Q21 : Combien de cyber-attaques ont été constatées dans votre entreprise au cours des 12 derniers mois ?

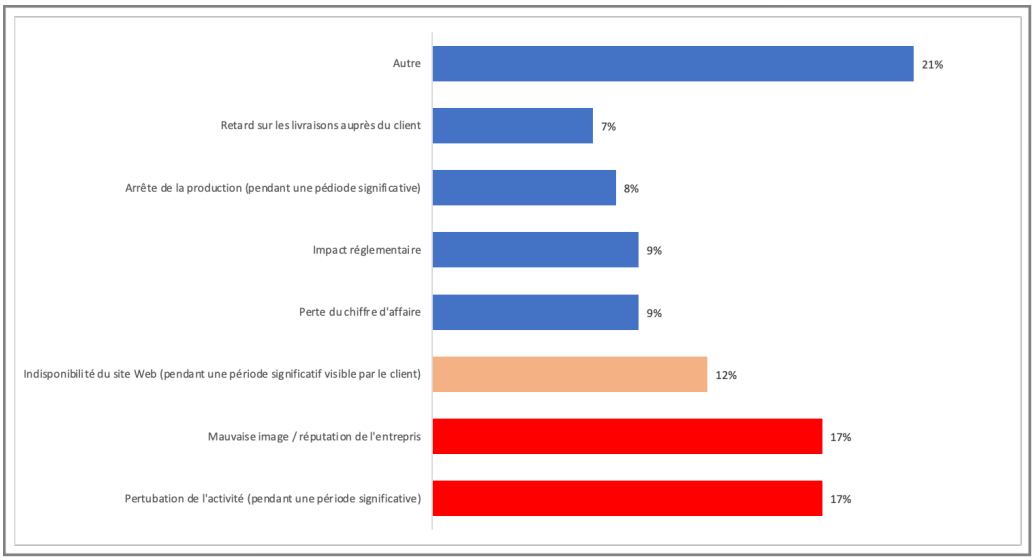


64% *des entreprises africaines déclarent avoir subi au moins une cyber-attaque en 2021 (82% en 2020)*

Cette année ces cyber-attaques ont pour conséquences directes une **perturbation de l'activité pendant une période significative** ou un **impact sur l'image de marque** de l'entreprise…

Q22 : Quel a été l'impact des cyber-attaques sur votre business ?

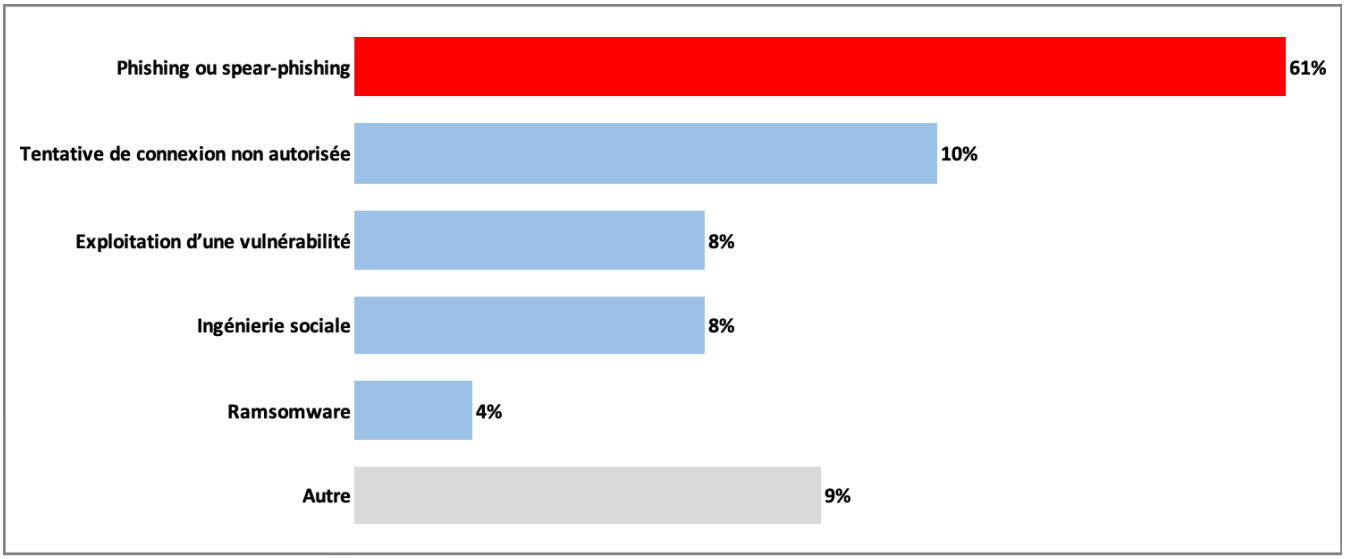
170 personnes



Et cette année, le **Phishing** reste le vecteur d'attaque privilégié des cybercriminels…

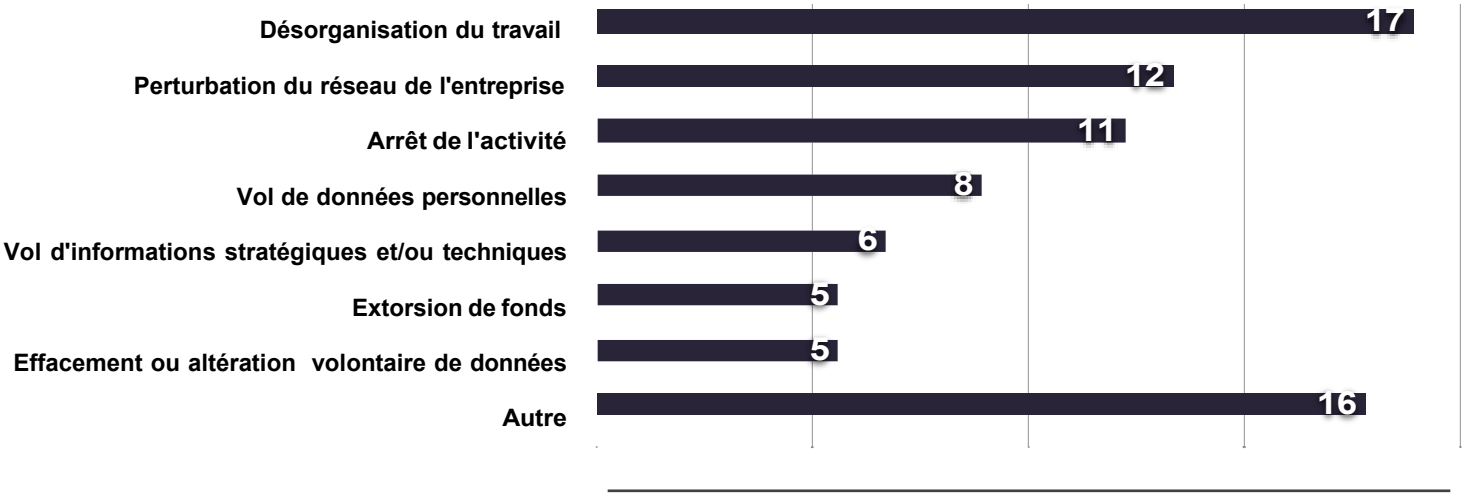
Q23 : Parmi les techniques d'attaques suivantes, lesquelles ont impacté votre entreprise au cours des 12 derniers mois ?

170 personnes



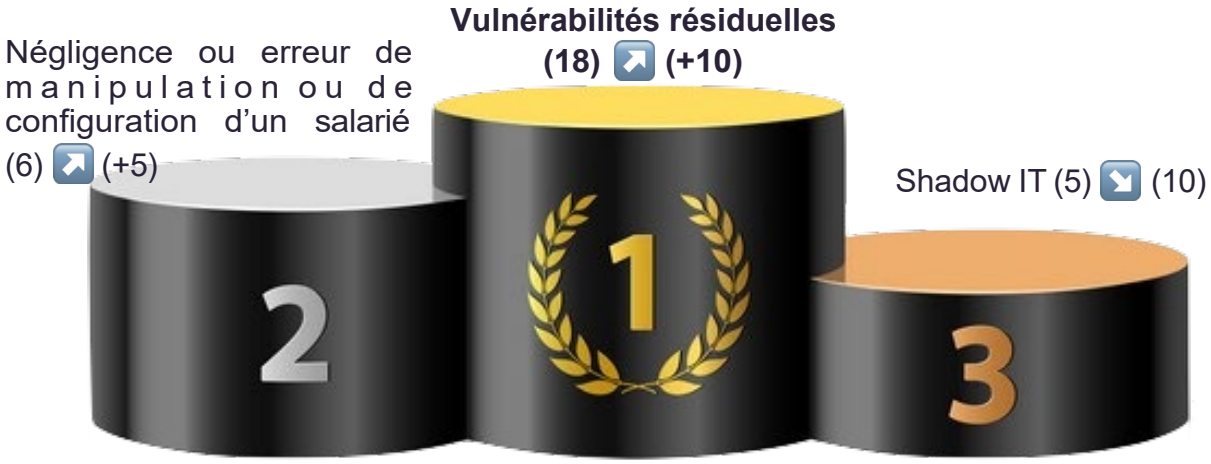
Q24 : Parmi les techniques d'attaques suivantes, lesquelles ont impacté votre entreprise au cours des 12 derniers mois ?

170 personnes



*Cette année, la **désorganisation du travail** passe à la tête des conséquences directe des cyberattaques pour les entreprises.*

Au nombre des vulnérabilités identifiées, cette année les **vulnérabilités résiduelles permanentes** gagnent 10 points par rapport à l'année dernière et s'inscrivent comme étant la vulnérabilité majeure.



DES ENTREPRISES EN AFRIQUE QUI SE PROTÈGENT

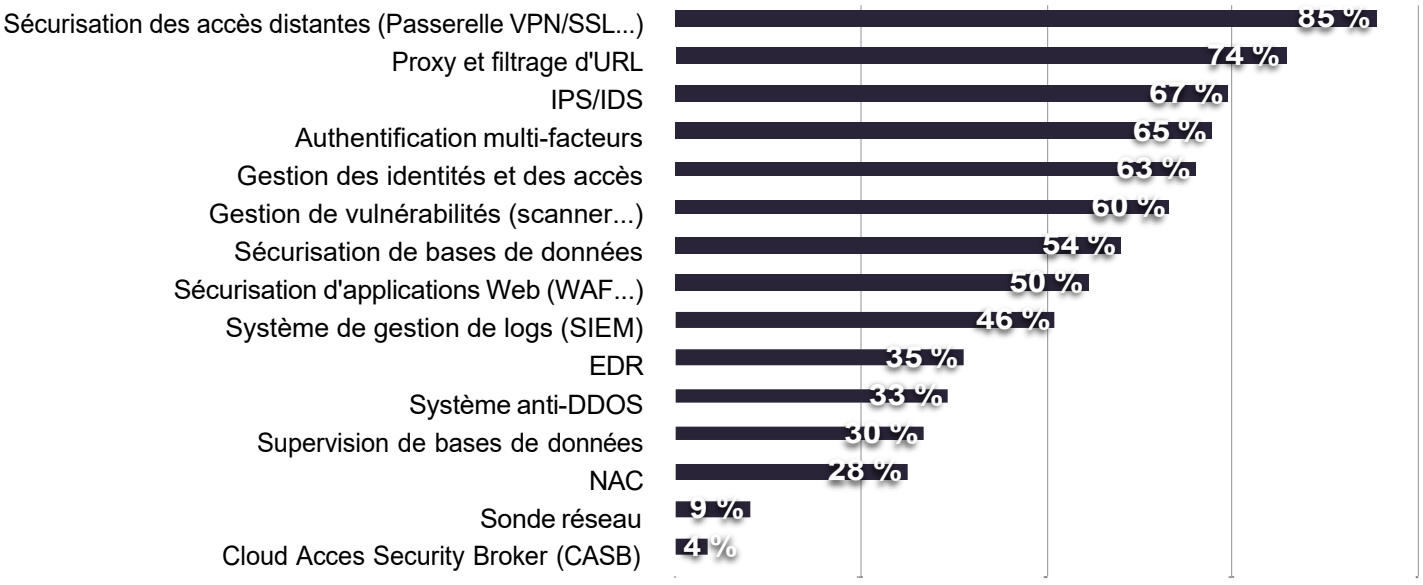
Q9 : Si vous disposez d'une stratégie de gestion de crise cyber, merci de nous indiquer quels sont les éléments que vous avez pris en compte parmi les éléments ci-dessous ?

170 personnes

1 entreprise sur 3 *environ se protège en mettant en place des sauvegardes sécurisées pour faire face à une cyberattaque.*

Q10 : Parmi les solutions de protections suivantes (liste non exhaustive), quelles sont celles qui ont été mises en place dans votre entreprise, en plus des antivirus et pare-feu ?

170 personnes

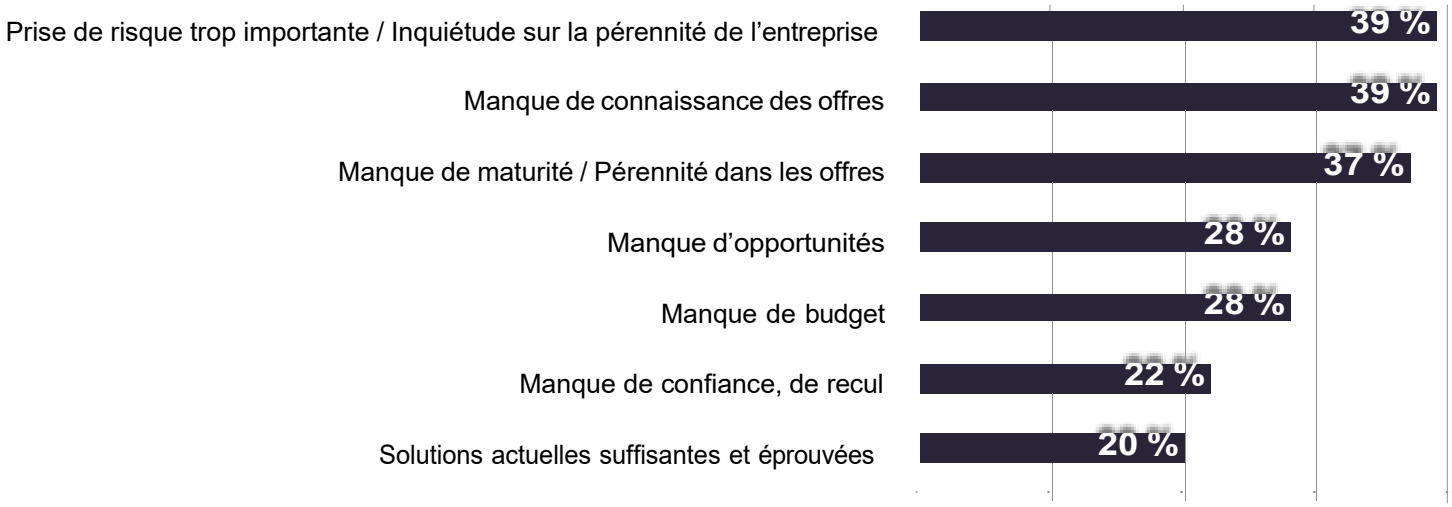


Dans ***85%*** *des cas, les professionnels de la sécurité se protègent en sécurisant les accès à distance.*

Comme l'année dernière, les entreprises n'ont toujours pas recours à des offres innovantes issues des start-up dans 90% des cas.

Q12 : Pour quelles raisons ne sollicitez-vous pas de start-up ?

170 personnes



Dans 39% des cas, les professionnels de la sécurité jugent le ***risque important en recourant aux solutions de start up ou un manque de connaissance des offres.***

80%

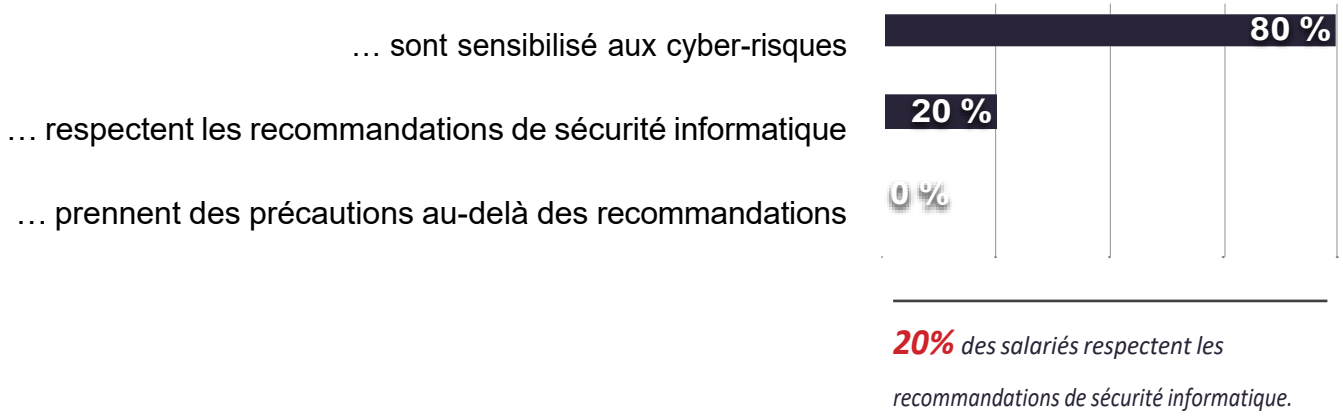
des entreprises n'ont pas souscrit à une cyber assurance.

LA 1ERE LIGNE DE DÉFENSE : LA MOBILISATION DES SALARIÉS

2 Salariés sur 10 respectent les recommandations de sécurité numérique en entreprise et parmi les usages à risque, dans près de **40% des cas, le BYOD** (Bring Your Own Device - en français : « Apportez Votre Équipement personnel de Communication »).

Q28 : Parlons de sensibilisation, à votre avis, les salariés de votre entreprise …

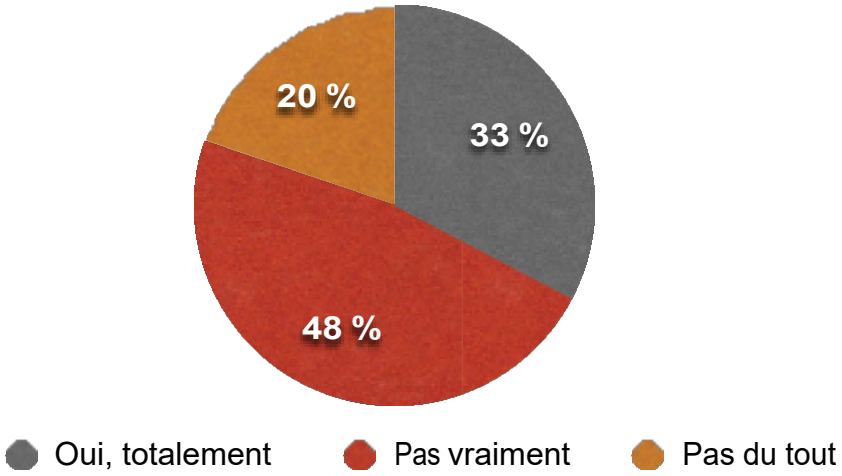
170 personnes



20% *des salariés respectent les recommandations de sécurité informatique.*

Q29 : Avez-vous mis en place des procédures pour tester l'application des recommandations par les salariés dans les situations concrètes comme des audits, campagnes de faux phishing, contrôles internes, etc. ?

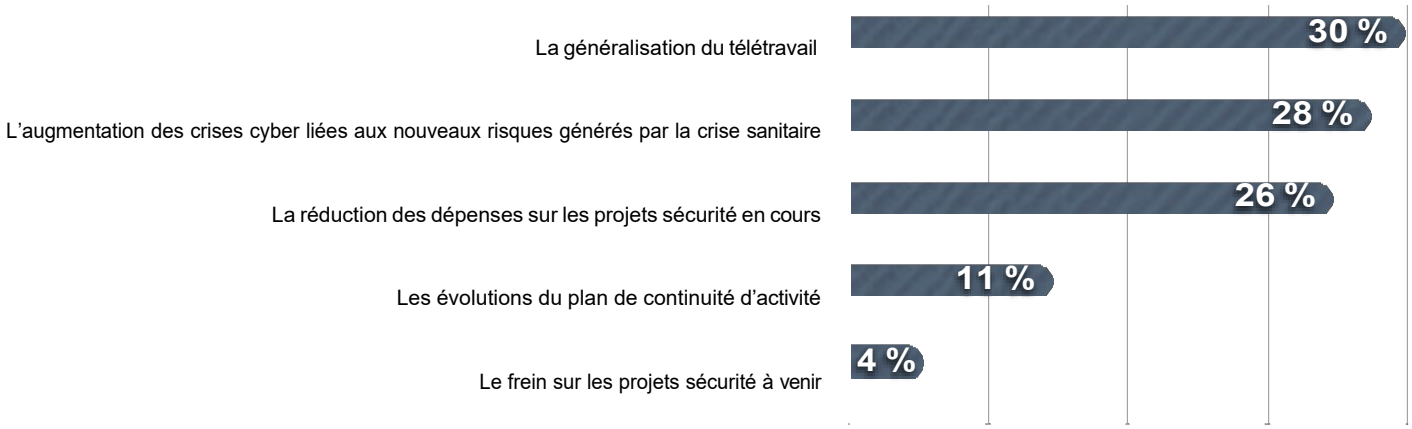
170 personnes



FOCUS : COVID-19

Q18 : Avec la crise sanitaire qui s'accentue, quel phénomène impacte le plus, l'activité cybersécurité de votre entreprise ?

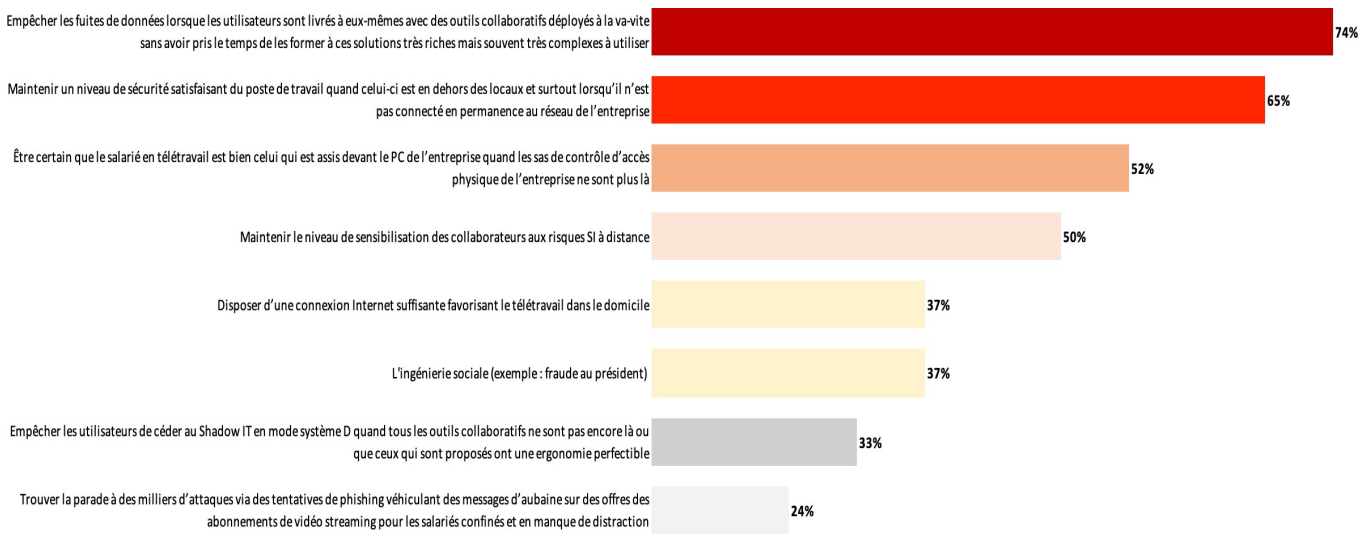
170 personnes



La crise sanitaire donne du fil à retordre aux professionnels de la sécurité afin déployer le télétravail.

Q20 : Pour vous quels sont les risques liés au Télétravail ?

170 personnes



LE CLOUD

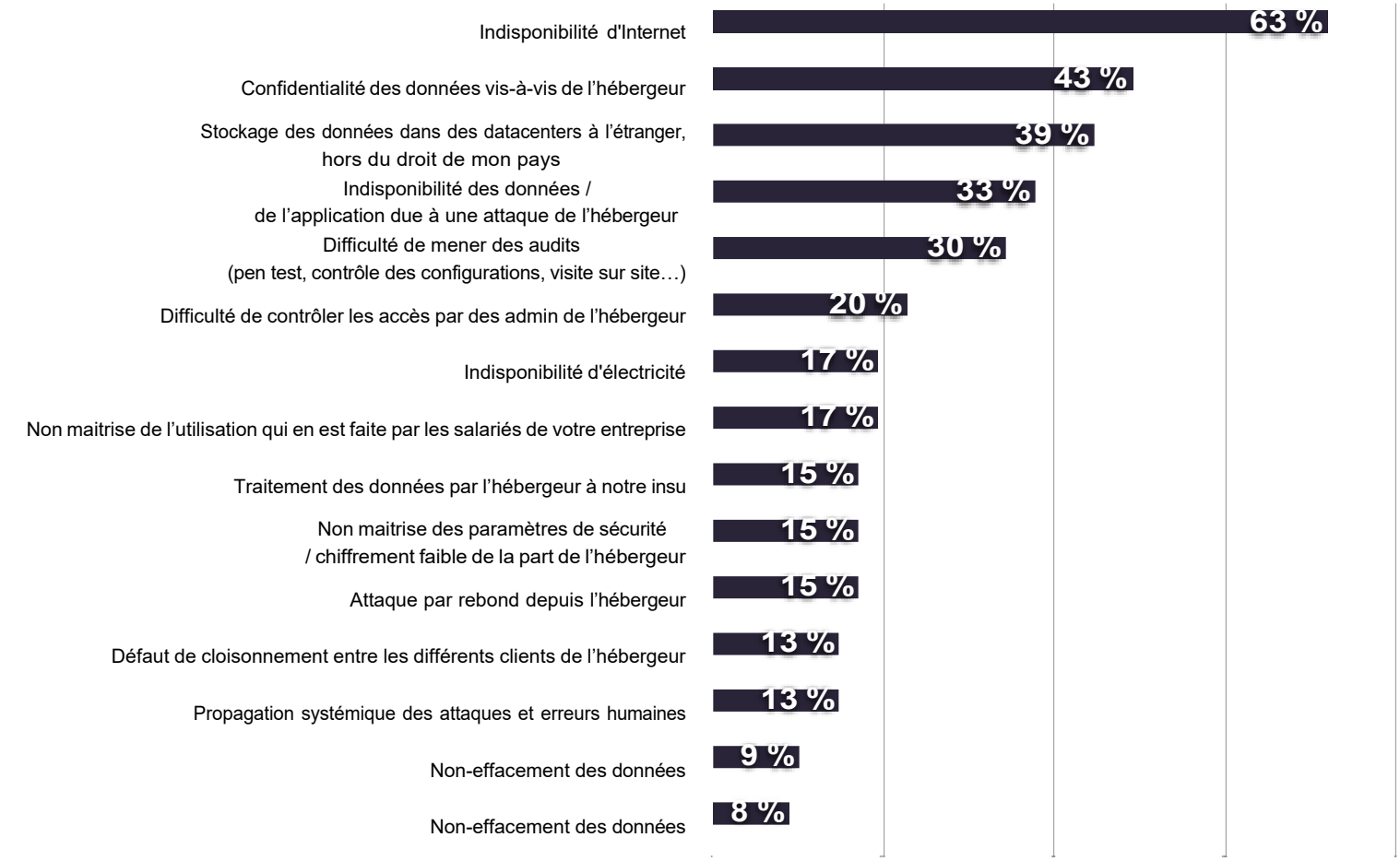
Pour **45%** des entreprises en Afrique héberger des données dans un cloud public ou privé n'est vraiment pas un sujet (33%) ou pas du tout (12%).

44% des entreprises hébergent leurs données dans des clouds publics ou hybrides.

Au nombre des risques identifiés, la **stabilité de la connexion Internet** arrive en première position cette année.

Q39 : Cochez 3 risques en ce qui concerne l'utilisation du Cloud ? Plusieurs réponses possibles.

170 personnes




contact@lecesia.com
www.lecesia.com


CESIA
CLUB D'EXPERTS DE LA SÉCURITÉ DE L'INFORMATION EN AFRIQUE