Ausimètre 2024

Baromètre de la cybersécurité au Maroc

Livre blanc présentant la synthèse des résultats de l'enquête

Remerciement

Notre profonde gratitude à toutes les entités qui ont généreusement pris le temps de répondre à cette enquête et qui ont permis à cette édition de l’Ausimètre de voir le jour.

Nos remerciements sincères aux collaborateurs dévoués de PwC et de l’AUSIM qui ont travaillé inlassablement pour superviser cette enquête et garantir sa rigueur méthodologique.

Sommaire

Note : Le détail des statistiques de l'enquête est donné en annexe de ce document

1 - Propos introductifs

Contexte de l’étude

En partenariat avec l'AUSIM, PwC a mené une enquête approfondie visant à étudier la posture de la cybersécurité au sein des entreprises du territoire marocain.

Cette étude menée du 30 novembre 2023 au 19 janvier 2024 nous a permis de collecter des données riches et variées sur des thèmes cruciaux, tels que l'évolution des risques cyber, les priorités d'investissement en cybersécurité, les tendances technologiques émergentes, les évolutions réglementaires et le niveau de maturité en cybersécurité des entreprises.

Dans les pages qui suivent, vous explorerez les perspectives des acteurs marocains sur l'état de la cybersécurité au Maroc.

Nous vous invitons à découvrir les résultats captivants de cette étude, qui promettent d'enrichir la réflexion sur les meilleures pratiques et les prochaines étapes pour renforcer la sécurité numérique au sein des entreprises au Maroc.

Cybersécurité et cyber-résilience : Perspectives organisationnelles dans un écosystème numérique en mutation

Rachid BAARBI, Vice-Président de l'AUSIM / Chief Information & Digital Officer chez Assurances Lyazidi

Dans le labyrinthe de l'ère numérique, où la danse binaire de l'innovation et du risque dicte le rythme, les organisations se trouvent à la croisée des chemins entre l'avancée technologique et la croissance du paysage des menaces. Et se tiennent en sentinelles, chargées de protéger leurs biens inestimables contre un paysage de menaces en constante mutation.

La numérisation des fonctions commerciales critiques a apporté une efficacité sans précédent, mais a simultanément exposé les entreprises à des menaces cybernétiques de plus en plus sophistiquées.

Ce livre blanc explore le réseau complexe de la façon dont les organisations perçoivent et priorisent la cybersécurité et la cyber-résilience face à cet écosystème numérique dynamique et en constante évolution.

La montée exponentielle des menaces cybernétiques a propulsé la cybersécurité au premier plan des priorités organisationnelles. La prise de conscience qu'une seule violation peut infliger des dommages importants non seulement aux données sensibles, mais aussi à la réputation et à la rentabilité d'une organisation, a catalysé un changement de paradigme. Dans les salles de réunion de comex de divers secteurs, une sensibilisation accrue à l'impératif de fortifier les infrastructures numériques contre une vague de menaces cybernétiques est perceptible.

De plus, à mesure que le paysage numérique devient de plus en plus complexe, la cyber-résilience émerge comme un compagnon essentiel de la cybersécurité. Au-delà de la protection contre les menaces cybernétiques, les organisations doivent désormais se concentrer sur la construction de systèmes adaptatifs et résilients capables de résister, de répondre et de récupérer des attaques cybernétiques. Le livre blanc vise à disséquer la compréhension nuancée que les organisations ont de la relation symbiotique entre la cybersécurité et la cyber-résilience, explorant comment ces concepts se croisent pour former une stratégie de défense robuste.

À travers des entretiens, des études de cas et des informations sectorielles, ce livre blanc navigue à travers les perspectives diverses au sein des organisations - de la direction exécutive aux professionnels de l'informatique - pour dresser un tableau complet de la manière dont la cybersécurité et la cyber-résilience sont perçues, intégrées et valorisées dans les stratégies organisationnelles contemporaines. Alors que nous nous lançons dans cette exploration, l'objectif n'est pas seulement de comprendre l'état actuel des choses, mais aussi de fournir des recommandations pour les organisations cherchant à fortifier leurs forteresses numériques dans une ère définie par l'ubiquité numérique et les menaces cybernétiques persistantes.

Optimisation de la cyber-résilience organisationnelle: Approche intégrée de cybersécurité et de gestion des risques

Taieb Debbagh, Directeur d’Atlantic Engineering School et Expert en cybersécurité et gouvernance

Cybersécurité et Cyber-résilience

Ceux sont deux concepts complémentaires mais distincts, la première se concentrant sur la protection et la prévention, tandis que la seconde met l'accent sur la préparation, la réaction et la récupération face aux menaces cybernétiques.

La cybersécurité se réfère aux mesures techniques, organisationnelles et humaines mises en place pour protéger les systèmes informatiques, les réseaux et les données contre les cybermenaces telles que les attaques, les intrusions, les logiciels malveillants et le vol de données. Elle vise à garantir la confidentialité, l'intégrité et la disponibilité des informations, ainsi qu'à prévenir les dommages aux systèmes et aux utilisateurs.

La cyber-résilience se concentre sur la capacité d'une organisation à anticiper, à résister, à s'adapter et à se rétablir face aux menaces cybernétiques. Elle va au-delà de la simple protection des systèmes en intégrant des stratégies de prévention, de détection, de réponse et de récupération. La cyber-résilience implique la préparation proactive aux cybermenaces, la capacité à réagir rapidement en cas d'incident, et la capacité à maintenir les opérations essentielles malgré les perturbations.

La cybersécurité se concentre principalement sur la protection des systèmes et des données contre les attaques cybernétiques, tandis que la cyber-résilience englobe un ensemble plus large de capacités, y compris la préparation, la réponse et la récupération après un incident.

La cybersécurité est souvent considérée comme une série de mesures défensives pour empêcher les cyber-attaques, tandis que la cyber-résilience met l'accent sur la capacité à continuer à fonctionner malgré les attaques et à récupérer rapidement en cas de perturbation.

La cybersécurité se concentre sur la protection des actifs numériques, tandis que la cyber-résilience intègre également des aspects organisationnels, humains et de gestion des risques pour assurer une réponse efficace aux menaces cybernétiques.

Et afin de renforcer la résilience des organisations face aux cybermenaces dans l'écosystème en ligne, le référentiel CROE (Cybersecurity Resilience for the Online Ecosystem), à été conçu et développé pour promouvoir la collaboration entre les différentes parties prenantes.

CROE offre des lignes directrices et des meilleures pratiques pour améliorer la Cyber résilience. Il a été adopté par la BERD et retenu par Bank Al Maghrib comme référentiel de base pour les établissements en charge du marché financier.

Le Maroc a réalisé des progrès significatifs en matière de transformation digitale

La GenAI : nouvelle technologie de rupture

Jamal Basrire, Associé Leader Cloud Transformation & Cyber pour la France et le Maghreb, en charge du développement des activités de conseil en technologie pour le Maroc

Nous intervenons régulièrement au Maroc et à l'étranger pour évaluer et accompagner les entreprises à se préparer, se protéger, détecter et réagir face aux menaces cyber.

Les entreprises marocaines, quel que soit le secteur dans lequel elles sont engagées : finance, industrie, services, font face aux mêmes challenges en matière de cybersécurité que les autres entreprises à travers le monde : une menace qui s'accélère et s'intensifie.

C'est indéniable, le Maroc a réalisé des progrès significatifs en matière de transformation digitale. Le Maroc a déployé durant la dernière décennie plusieurs programmes nationaux pour le développement du digital (e-Maroc 2010, Maroc Numérique 2013, Maroc Digital 2020…). Un état des lieux permet en effet de dégager d'importants acquis réalisés à tous les niveaux, comme il permet de mettre le doigt sur des freins à cette transformation. Aux enjeux et challenges de la transition numérique, s'ajoutent désormais une accélération de l'adoption des technologies émergentes telles que l'intelligence artificielle (IA), qui démontre un grand potentiel aux domaines d'application multiples : santé, sécurité, transport, performance des services administratifs, éducation… Selon l'édition 2024 de l'enquête annuelle sur la cybersécurité de PwC, la « Digital Trust Insights survey », trois quarts des dirigeants d'entreprise et de responsables en technologie se montrent enthousiastes quant au potentiel de l'intelligence artificielle générative (ou « GenAI »). Plus des trois quarts des répondants à notre enquête indiquent que la GenAI apportera une augmentation tangible de la productivité dans les 12 prochains mois et qu'elle permettra le développement de nouvelles opportunités business dans les 3 années à venir. Cette nouvelle révolution positionne la GenAI comme une technologie de rupture qui viendra fondamentalement transformer les entreprises. Ainsi, la GenAI apportera de nouvelles solutions pour traiter le risque, mais contribuera par ailleurs à son accroissement avec son lot de nouveaux risques à appréhender (intégrité des données résultant du traitement de la GenAI, risques liés aux modèles, biais cognitifs...). Le risque cyber notamment restera toujours un des principaux risques à considérer dans le cadre de cette adoption technologique.

L’Ausimètre confirme la poursuite des investissements technologiques cyber

Efficacité cyber et rationalisation : 2 tendances à suivre

Jamal Basrire, Associé Leader Cloud Transformation & Cyber pour la France et le Maghreb, en charge du développement des activités de conseil en technologie pour le Maroc

Le Maroc apparaît selon plusieurs études comme le 15ème pays le plus ciblé au monde par des attaques cyber. Selon le rapport d'évaluation des cybermenaces d'Interpol de 2023, le Maroc est le pays africain le plus touché par les trojans bancaires et *stealers*, le deuxième le plus ciblé par les attaques de ransomwares (8% de toutes les attaques détectées), et 70% des courriels d'extorsion détectés en 2023.

L'Ausimètre 2024 confirme la prise de conscience du marché marocain des enjeux cyber. Selon le dernier classement NCSI (National Cyber Security Index), le Maroc est positionné à la 30ème place mondiale sur le plan de l'effort mis en œuvre pour endiguer le risque cyber.

Cette prise de conscience permet aux acteurs du marché marocain de se positionner en tant qu'observateurs avisés de l'évolution des menaces cyber et de confirmer les tendances suivantes :

- L’augmentation de l'intensité et de la sophistication des attaques,
- L'augmentation de l'impact financier des incidents cyber,
- La fuite de données comme principal scénario redouté.

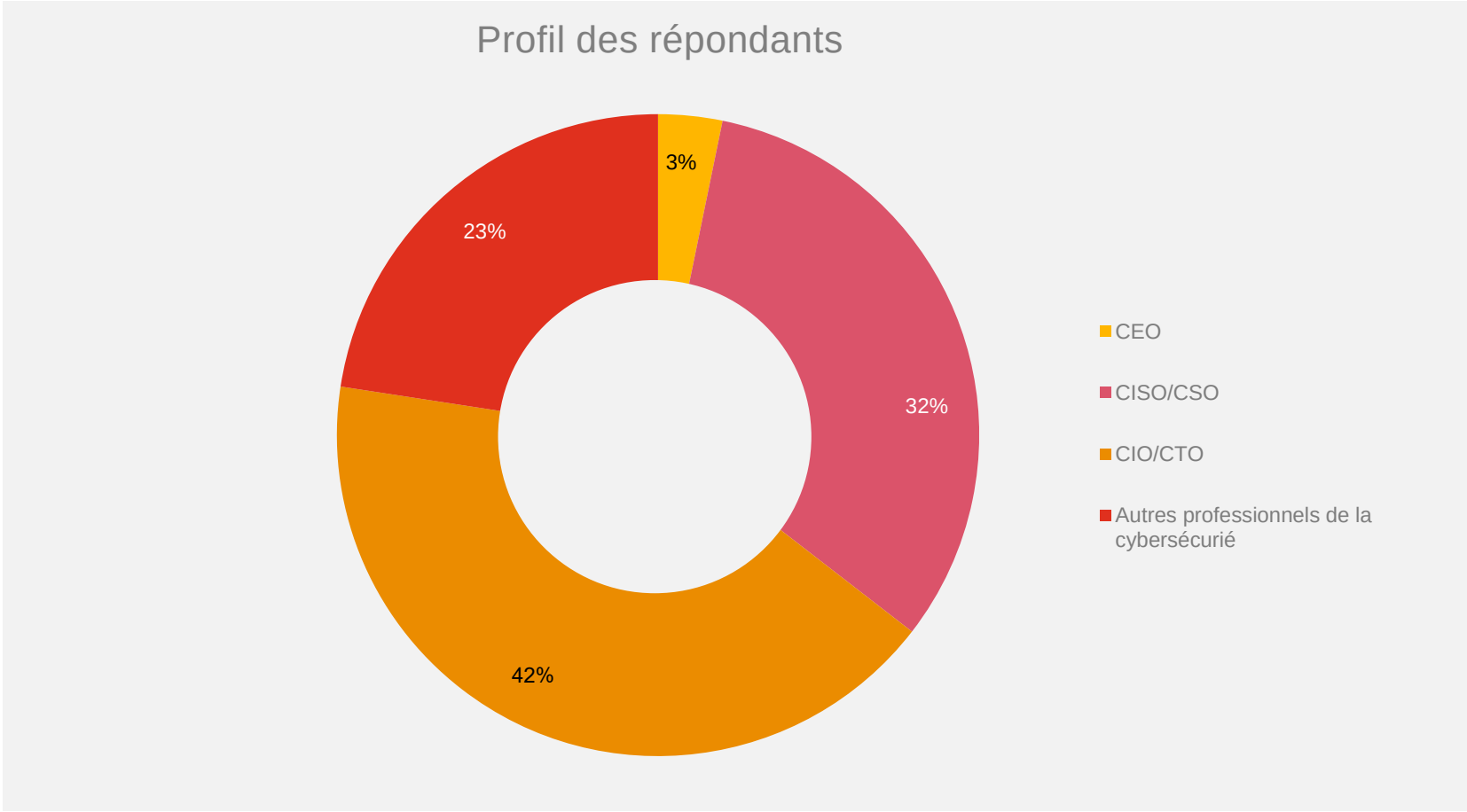
De manière plus globale, les enjeux de souveraineté sont au cœur des réflexions des entreprises marocaines qui sont à la recherche de levier pour débloquer les transitions vers le Cloud et l’adoption de la GenAI. Nous considérons que cette adoption requiert un effort significatif de mise sous maîtrise de ces technologies : déploiement des technologies, définition de cadres de gouvernance et de contrôle, formation, gestion du changement… pour permettre aux entreprises de bénéficier du potentiel offert par ces technologies.

La cybersécurité est plus que jamais une préoccupation majeure pour les dirigeants d’entreprise. La question de la cybersécurité doit ainsi être intégrée au plus tôt dans les démarches de transformation plutôt que de réagir en situation de crise. L’arrivée progressive de la GenAI dans le paysage constitue une opportunité fantastique de permettre aux métiers et aux experts de la cybersécurité de collaborer pour définir les cas d’usage futurs et les approches pour les sécuriser.

L’Ausimètre de cette année confirme la poursuite des investissements cyber avec une appétence forte au déploiement de nouvelles technologies. Il conviendra d’observer, dans les prochaines années, la pérennité des stratégies adoptées par les acteurs marocains, gardant en perspective une tendance de plus en plus marquée à la recherche et au suivi de l’efficacité et des retours sur investissements cyber.

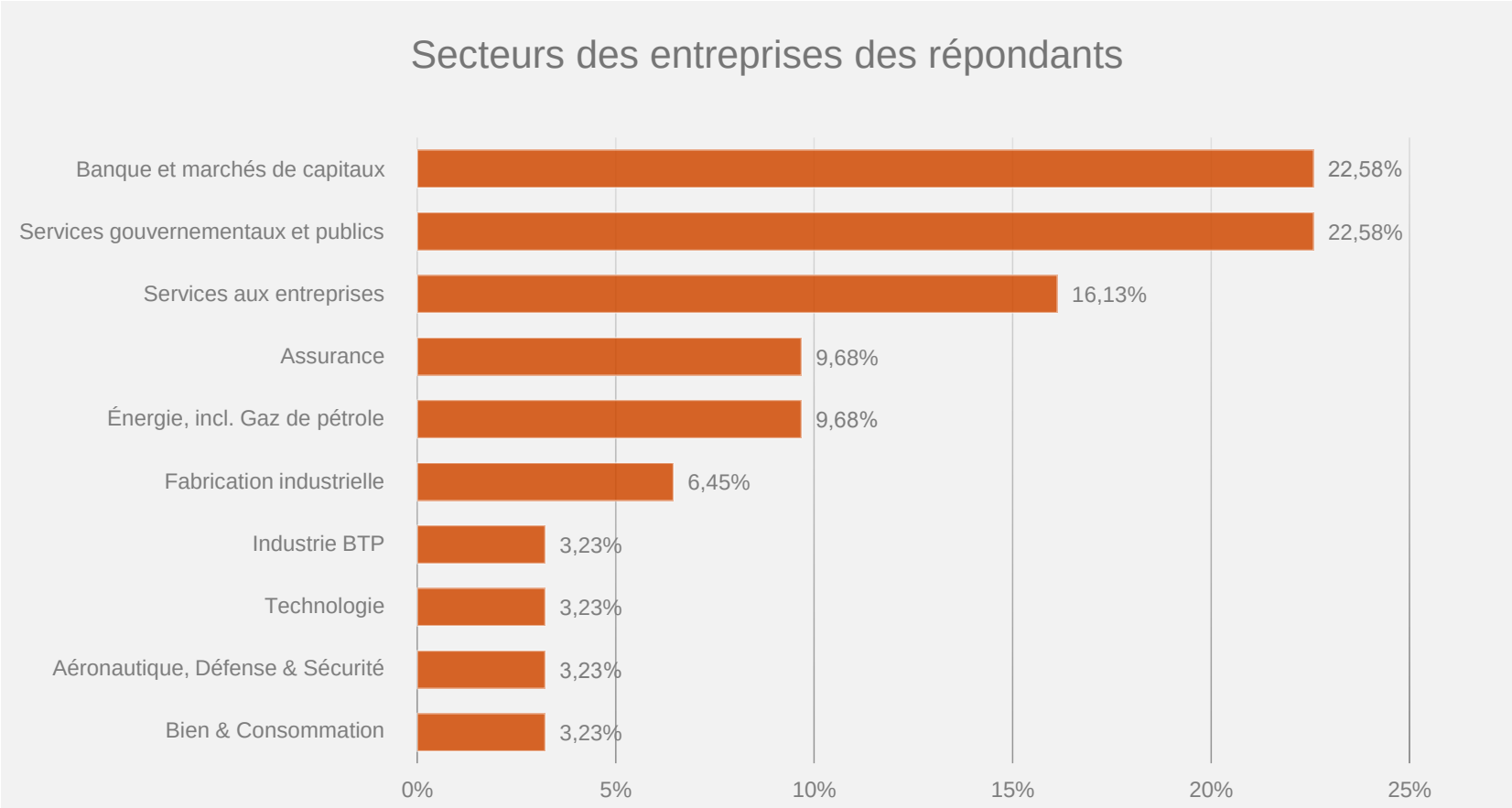
Une enquête mobilisant un panel représentatif du leadership cyber au sein des entreprises marocaines

Les répondants de notre enquête présentent une diversité de profils allant du dirigeant d'entreprise aux professionnels de la cybersécurité (CIO, CTO, CISO, consultants).



Un large spectre de secteurs d’activité représenté

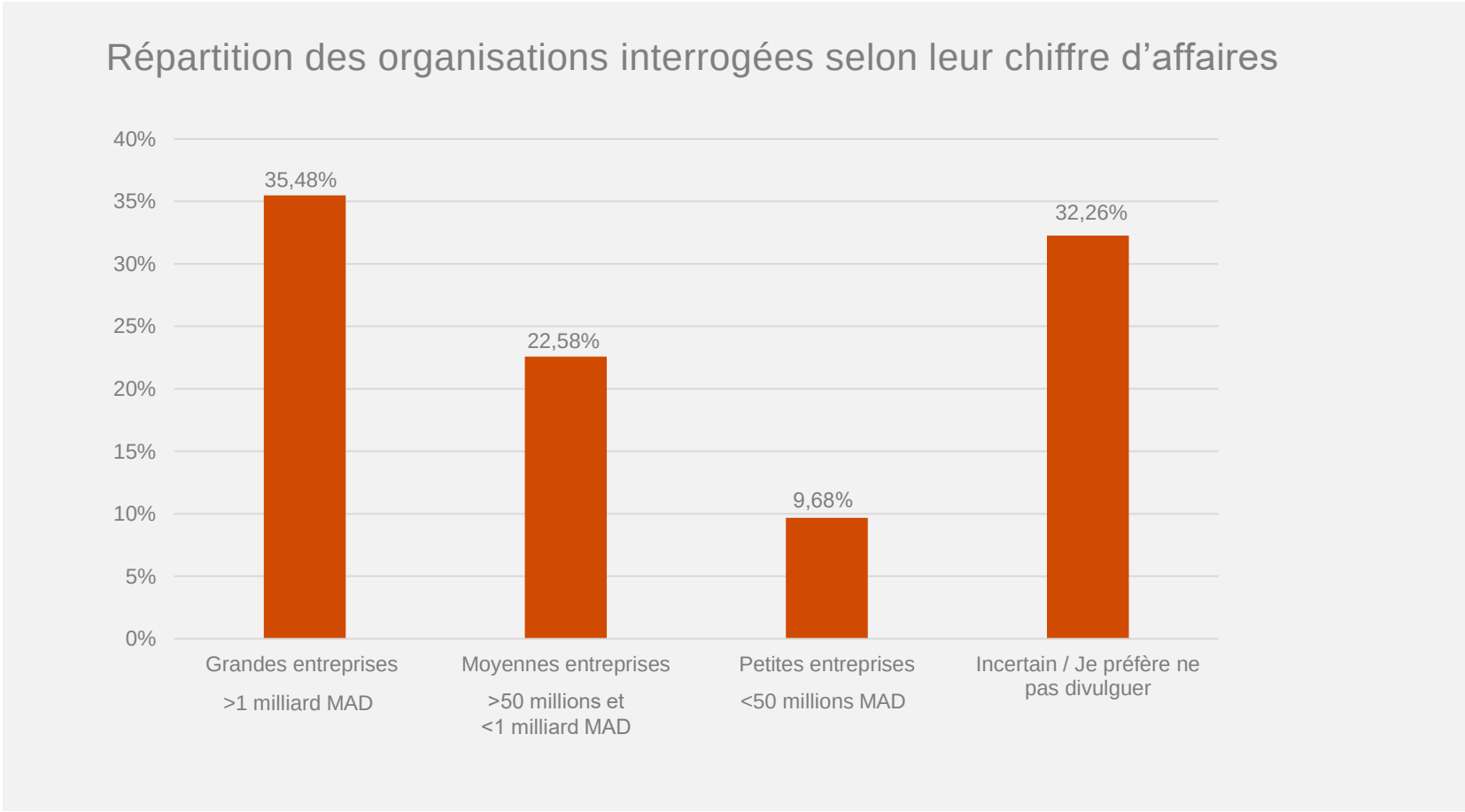
L’Ausimètre couvre un large spectre de secteurs d’activité avec une représentation forte des services financiers et des services gouvernementaux et publics.



Un panel de répondants représentant la diversité de l'écosystème d'entreprises marocaines

Le panel de répondants reflète la diversité des entreprises opérant au Maroc, de petites entreprises à de grandes multinationales.

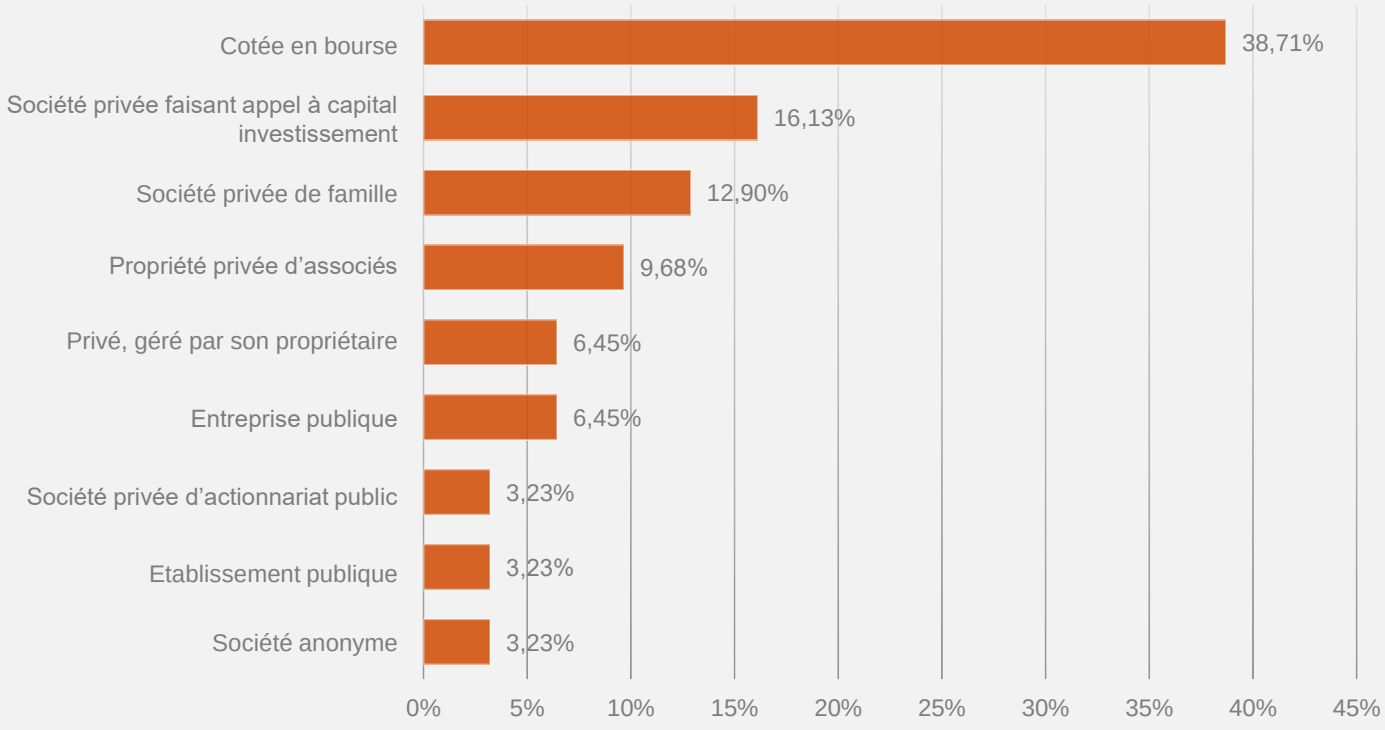
De notre expérience, le chiffre d'affaires comme la taille de l'entreprise ou encore l'intensité des investissements digitaux constituent des métriques permettant le benchmark des investissements cyber.



Une prédominance des sociétés côtées dans le panel de répondants

Les répondants proviennent d'une variété de structures d’entreprises : sociétés cotées, entreprises publiques, entreprises familiales.

La compréhension des statuts de propriété des entreprises, permet d'aligner les stratégies de sécurité sur les réalités opérationnelles et les contextes économiques spécifiques.



2 - Résultats de l’Ausimètre : état de la menace cyber au Maroc et synthèse des enseignements de l’Ausimètre

Le Maroc, une cible principale des attaques cyber en Afrique

1. 10 fuites de données signalées en 2023 ciblant des entités marocaines opérant sur les secteurs suivants : industrie pharmaceutique, éducation, services gouvernementaux et publics, télécommunications, technologie et médias.

2. D'après le rapport d'évaluation des menaces cybernétiques d'Interpol de 2023, le Maroc se trouve en tête des pays africains les plus touchés par les trojans bancaires et les "stealers", avec 18 000 détections. De plus, il occupe la deuxième place en termes d'attaques de ransomwares, représentant 8% des attaques détectées. En outre, 69,24% (soit 13 002) des courriels d'extorsion signalés au niveau des pays africains ont été identifiés au Maroc.

3. Depuis janvier 2023, 2 500 fichiers malveillants signalés comme Stealer, 130 comme Ransomware et 15 fichiers binaires liés aux TTP APT ont été téléchargés depuis le Maroc.

4. Yellow Nix (alias MuddyWater) a été très actif en 2022 en exploitant la vulnérabilité d'outils d'administration à distance de manière assez large notamment au Maroc.

Le risque cyber, la priorité numéro 1 des risques à traiter pour les entreprises marocaines en 2024

TOP 3 Des risques considérés par les entreprises

1. Risques cyber (**90%**)
2. Risques numériques et technologiques (**57%**)
3. Risques environnementaux (**40%**)

TOP 3 Des principales menaces identifiées par les entreprises

1. Rançongiciel (**84%**)
2. Fuite de données (**61%**)
3. Compromission de la messagerie (**45%**)

TOP 3 Des principales conséquences redoutées

1. Fuite de données des clients, employés ou transactions (**84%**)
2. Atteinte à l'image de marque de l'entreprise (**65%**)
3. Indisponibilité de service (**58%**)

$ Les pertes financières générées par les fuites de données

32% des répondants indiquent avoir subi des pertes liées à une fuite de données supérieur à **500 kMAD** sur les 3 dernières années. Ces pertes peuvent aller jusqu'à des montants dépassant **10 millions** de dirhams pour **6%** des entreprises des répondants.

Les entreprises au Maroc, ayant participé à notre enquête, accordent une priorité élevée à la protection de l'information. Elles reconnaissent l'importance cruciale de préserver la propriété intellectuelle, la confidentialité des données des clients et la réputation de l'entreprise.

Témoignages d’experts

Comment percevez l'évolution des menaces cyber au Maroc ?

M. Imad TABEUTE
IT Manager et RSSI
Organisme financier

M. Imad TABEUTE indique que « le Maroc est confronté à un paysage cybernétique en constante **évolution avec des menaces** de plus en plus sophistiquées ». Il identifie des tendances telles que « l'augmentation des attaques de **phishing** » exploitant la confiance des utilisateurs, la sophistication croissante des « attaques de **ransomwares** ». ciblant des entreprises marocaines, et l'émergence d'attaques ciblées comme le « **spear-phishing** » et les attaques **DDoS**.

Il souligne également les nouvelles menaces liées aux **appareils connectés (IoT**), notant que « les appareils non sécurisés peuvent être exploités pour accéder aux réseaux domestiques ou aux réseaux et données des entreprises ». En conclusion, il insiste sur l'importance de mesures de sécurité telles que le « **renforcement de la sécurité des systèmes**, la **sensibilisation** à la sécurité, la **formation des utilisateurs et la mise en place de protocoles de réponse aux incidents** » pour faire face à ces défis en constante évolution. M. Imad TABEUTE rappelle que la cybersécurité est un domaine dynamique, exhortant à rester vigilant et informé des dernières évolutions en matière de sécurité informatique.

M. Youness AIT BAMOH
IT Manager
Ciments du Maroc

M. Youness AIT BAMOH, souligne que le pays a connu une « croissance significative dans le domaine de la transformation digitale au cours des dernières années ». Il identifie les cybermenaces émergentes telles que « des attaques **Phishing, Spear-Phishing et Ransomware** ». En analysant la situation actuelle, il indique que le Maroc subit **les cybermenaces,** se positionnant comme l'un des pays les plus touchés en Afrique.

Il met en évidence la complexité croissante des attaques en ligne, soulignant que « les menaces deviennent de plus en plus sophistiquées ». Il explique que la croissance du numérique, combinée au développement géopolitique et régional, expose naturellement le Maroc aux attaques cybernétiques. Malgré ces défis, il perçoit des opportunités, affirmant que ces enjeux peuvent stimuler **la coopération entre parties prenantes**, créer de **nouveaux emplois**, **renforcer la résilience** des systèmes et favoriser la croissance des compétences et des entreprises liées à la cybersécurité.

Des investissements cyber qui se poursuivent avec une appétence forte au déploiement de nouveaux outils

Des investissements technologiques considérables sont consacrées à la cybersécurité en 2023

78%

Des répondants ont affirmé dédier jusqu'à **25%** de leurs investissements technologiques à la cybersécurité.

Cette statistique met en lumière que le marché marocain est encore dans une phase de construction de ses fondements technologiques liés à la cybersécurité.

Une augmentation du budget allouée à la cybersécurité se poursuit de manière significative

52%

Des répondants envisagent une augmentation jusqu'à **14%** de leur budget cyber.

Cette tendance illustre la poursuite des investissements cyber dans un contexte de transformation digitale et d'adoption de nouvelles technologies de rupture telles que l'Intelligence Artificielle Générative.

Les organisations sont confrontées à une complexité croissante des technologies de cybersécurité. L'augmentation des budgets consacrés à la cybersécurité et la part importante allouée à la dimension cyber des investissements technologiques nécessiteront probablement, dans les années à venir, une attention accrue à l'efficacité de ces investissements et à la rationalisation des coûts cyber, à l'instar de ce qui se fait actuellement dans d'autres régions du monde telles que les États-Unis ou l'Europe.

Témoignages d’experts

Une tendance à la rationalisation des coûts cyber et notamment des portefeuilles technologiques s'observe en Europe. S'agit-il d'une tendance qui s'observe selon vous au Maroc ?

Comment appréhendez-vous l'augmentation constante des budgets cyber au sein de votre organisation ?

M. Imad TABEUTE
IT Manager et RSSI
Organisme financier

M. Imad TABEUTE souligne que « **L’augmentation constante du poste budgétaire** alloué aux investissements cyber au fil des dernières années reflète la prise de conscience du top management de l'importance et de la nécessité d’avoir une posture cybersécurité mature ». Il identifie plusieurs raisons motivant cette augmentation budgétaire, dont **l'évolution rapide des menaces cyber** de plus en plus sophistiquées, la nécessité de **protéger les données sensibles**, l**a conformité aux réglementations, l'impact des nouvelles technologi**es telles que l'intelligence artificielle, et l'importance croissante de la sensibilisation à la cybersécurité. M. Imad TABEUTE souligne également que malgré l'augmentation des budgets, une « **approche holistique de la cybersécurité** » est nécessaire, intégrant des processus, des technologies, des compétences humaines et une culture de sécurité pour faire face efficacement aux défis actuels et futurs.

M. Youness AIT BAMOH
IT Manager
Ciments du Maroc

M. Youness AIT BAMOH précise que « les entreprises prennent désormais plus au sérieux le risque cyber, principalement en raison des récentes attaques et de la prise de conscience croissante, renforcée par les règles établies par des organisations comme la DGSN ». Il constate une « **augmentation significative des investissements en cybersécurité**, notamment dans les domaines bancaires, les assurances, les institutions gouvernementales et les entreprises classées comme organisme d’importance vitale (OIV) ».

Cependant, M. AIT BAMOH note que la « **rationalisation des coûts cyber n'est pas encore mature au Maroc** », et que « les acquisitions en termes de solutions de cybersécurité se font suite à une éventuelle intrusion détectée, une recommandation d’un prestataire de service ou une conformité à respecter afin de passer un audit ». Il met en avant l'engagement de Ciments du Maroc dans la transformation digitale, la connectivité des usines, et les objectifs liés à l'ESG et à la décarbonisation. Il insiste sur la nécessité de promouvoir une « culture de sécurité » et souligne l’importance du soutien solide du Top management, permettant d'accéder aux ressources nécessaires pour garantir le succès des initiatives en matière de cybersécurité.

Bien que des efforts significatifs ont été entrepris ces dernières années, l'écosystème marocain doit encore renforcer sa maturité cyber

35% Indiquent que leur entreprise est **souvent** proactive dans l'**anticipation des risques cyber**, en tenant compte de l'environnement macroscopique et de la stratégie de l'organisation.

39% Affirment que leur organisation **réagit souvent** de manière rapide face aux **menaces**, visant ainsi à renforcer la résilience de l'entreprise face aux perturbations.

61% Affirment que leur entreprise met **souvent** en œuvre des contrôles à l'échelle de l'ensemble de l'organisation dans le but de **prévenir les perturbations cybernétiques graves**.

48% Indiquent que leur organisation **intègre souvent la cybersécurité dans les transformations technologiques** majeures de l'entreprise.

35% Indiquent que **parfois**, leur organisation **communique la stratégie et les pratiques en matière de cybersécurité** afin de gagner la confiance des clients et des partenaires commerciaux.

Ces statistiques témoignent d'efforts significatifs réalisés ces dernières années en matière de contrôles pour évaluer les risques cyber. Afin d'anticiper au mieux les menaces et notamment celles amenés par les transformations à venir (digitalisation, adoptions Cloud, adoption de l'Intelligence Artificielle Générative), il s'agira de s'assurer d'un alignement de l'effort cyber avec la stratégie et les initiatives business adoptées par l'entreprise. Cet effort permettra de positionner le cyber comme un atout à la confiance des clients et des partenaires.

Un marché marocain s'appuyant très largement sur les frameworks cyber internationaux pour leur cadre de contrôle: ISO27001 quasi unanimement adopté

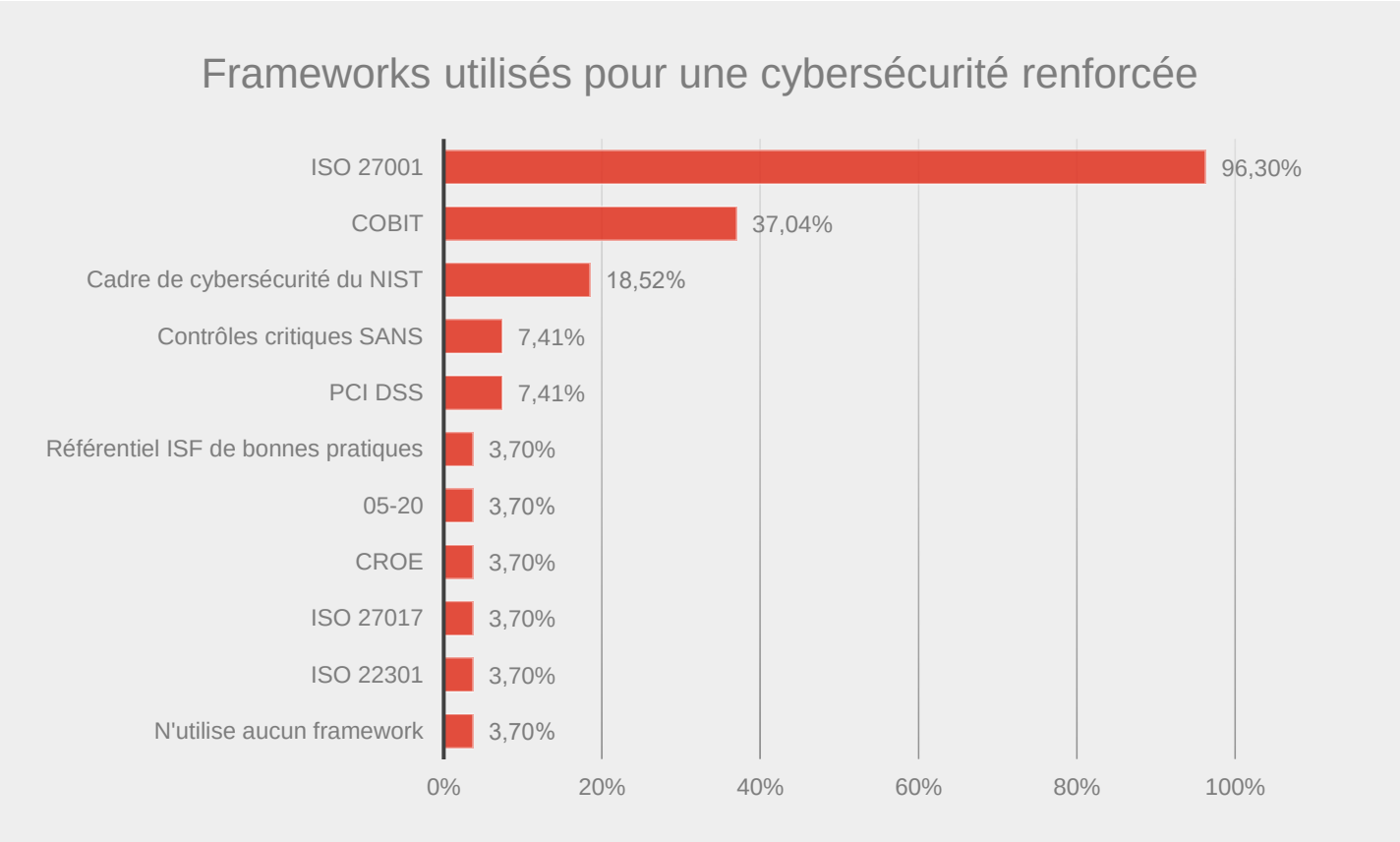
96% Des entreprises interrogées optent pour le Framework ISO 27001 comme cadre d'évaluation de leur position en matière de cybersécurité.

A l'échelle mondiale* :

Les entreprises montrent clairement une adoption accrue des frameworks suivants :

- NIST cybersecurity framework (**53%**) ;
- ISO 27001 (**45%**) ;
- Cloud Security Alliance (**34%**) ;
- Contrôles critiques SANS (**26%**) ;
- CIS CSC (**26%**) ;
- Cyber Resilience Review (**25%**).

*Source: Global Digital Trust Insights 2023, PwC



Upskilling, capacités technologiques cyber et capacités de reconstruction au coeur des priorités pour améliorer la cyber résilience des entreprises marocaines

Une stratégie de cyber résilience qui s'appuie sur le développement des talents

Les entreprises marocaines considèrent que l'investissement dans le développement des compétences cyber est crucial pour **renforcer leurs capacités de défense et de résilience cyber.**

56% des entreprises donnent la priorité à **l'amélioration** des **compétences** par le biais de l'**upskilling** et de la **formation**.

Le renforcement des capacités de reconstruction : une priorité au Maroc

41% des répondants ont mis en place un **plan de reconstruction informatique** suite à une **cyber attaque** dans certaines parties le l'organisation.

Des capacités technologiques cybers globalement satisfaisants

Les répondants témoignent d'une **satisfaction** quant au déploiement de leurs technologies dans les domaines suivants : **gestion des risques et conformité, sécurité des réseaux, sécurité des données,** ainsi que **sécurité des systèmes OT & IoT.**

En revanche, ils font part de leur **insatisfaction** concernant certains aspects technologiques, notamment **l'automatisation de la détection, la gestion des identités et la sécurité du Cloud.**

Une prise en compte des technologies émergentes dans l'approche de gestion des risques cyber

74% des répondants ont intégré la dimension **Cloud** dans leur **plan de traitement des risques.**

Pour la majorité des répondants, **l'intelligence artificielle**, la **réalité virtuelle** et la **crypto-monnaire ne** sont **pas** encore **applicables** au sein de leurs entreprises.

Le Move to Cloud, une démarche encore à développer : un enjeu de souveraineté, de sécurité et de maîtrise de la chaine de fournisseurs

Intégration de Cloud

38% des répondants n'ont pas recours au Cloud. Parmi ceux qui l'utilisent**,** **27%** favorisent l'hybridation de fournisseurs de cloud public et privé.

Principaux fournisseurs de services

Les entités, ayant choisi d'adopter des infrastructures Cloud, se tournent principalement vers les leaders du marché, tels que **Microsoft Azure (62%)**.

Défis associés aux prestataires de Cloud

La gestion de la reprise après sinistre constitue un défi significatif lors de la collaboration avec des prestataires de services Cloud.

L'utilisation des solutions technologiques

12% des entreprises cherchent à **avoir une suite intégrée de leurs solutions**, tandis que **68%** sont **satisfaits** de leurs fournisseurs diversifiés.

La réglementation cyber liée au Cloud au Maroc

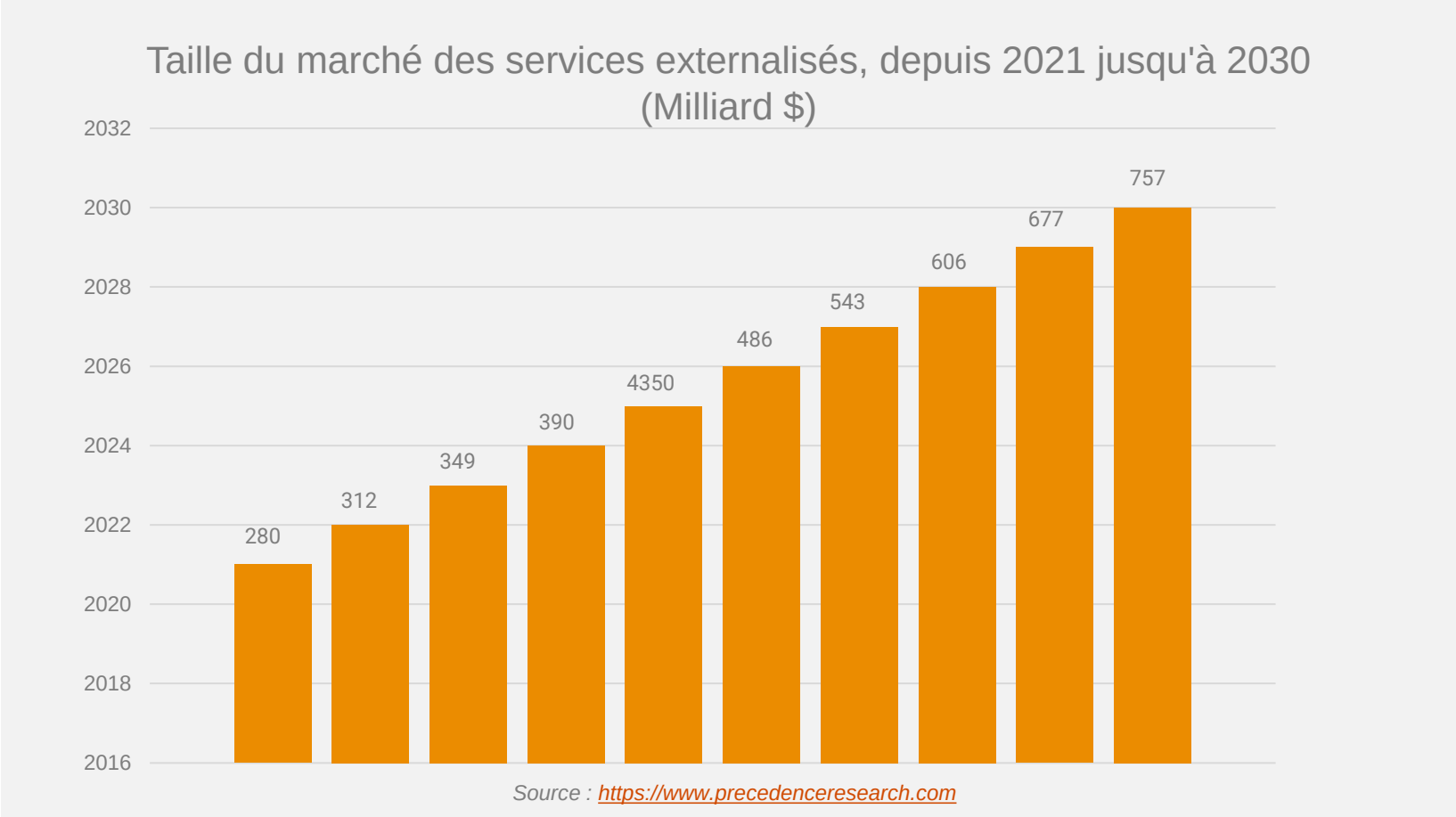
En réponse à l'essor du Cloud, le Maroc a récemment renforcé son encadrement réglementaire de cette technologie. En 2016, la 4ème édition du séminaire sur la cybersécurité "Mobile et Cloud Computing", était l'occasion de sensibiliser les DSI et les RSSI sur les opportunités et sur les risques liés à la sécurité des données dans le Cloud, ainsi que d'initier une réflexion sur le cadre législatif et réglementaire. Sur le même élan, le Maroc a adopté en 2020 la loi n° 05-20 imposant plusieurs lignes directrices, notamment la protection des données personnelles des citoyens marocains en exigeant qu'elles soient stockées sur des serveurs situés sur le territoire national.

Les entreprises éprouvent de plus en plus le besoin de recourir à l'externalisation des services

Dans un contexte où les cybermenaces deviennent plus sophistiquées chaque jour et où le monde connaît des mutations technologiques sans précédent, les défis à relever pour assurer la sécurité des systèmes informatiques sont nombreux.

Toutefois, les ressources et les compétences nécessaires pour protéger efficacement les organisations sont très spécialisées et peuvent être complexes à mobiliser ou à maintenir en interne. Face à ce constat, l'externalisation de services se révèle être une véritable opportunité pour concilier efficacité, agilité et rentabilité.

La taille du marché mondial des services gérés s'élevait à 349 milliards de dollars américains en 2023 et devrait atteindre 757,10 milliards de dollars américains d'ici 2030, avec un taux de croissance annuel composé (TCAC) de 12,6% entre 2022 et 2030.



Témoignages

Les entreprises étrangères challengent de plus en plus les modèles opérationnels cyber à la recherche d'une cybersécurité plus simple, avec un niveau de résultat prédictible et à des coûts maîtrisés.

Le marché des services managés étant actuellement en pleine expansion, quelle est votre retour d'expérience sur l'utilisation de tels services et quelles perspectives votre entreprise se donne-t-elle à l'utilisation de ces services ?

M. Youness AIT BAMOH
IT Manager
Ciments du Maroc

M. Younes AIT BAMOH, interrogé sur l'essor croissant des entreprises étrangères cherchant des modèles opérationnels de cybersécurité plus simples, a souligné que " **l'adoption d'un modèle de ventes axé sur le service et la mensualisation explique également la popularité croissante des Managed Services**". Il a mis en avant la flexibilité offerte par ces services, permettant aux organisations "d'accéder à des services de cybersécurité de premier ordre tout en ajustant les coûts à leurs besoins". Selon lui, des aspects cruciaux tels que "**l'analyse de risque, l'assistance, la gouvernance de sécurité, la surveillance contre les menaces, la gestion des sauvegardes, le stockage cloud**" peuvent être **externalisés avec succès**. M. Younes AIT BAMOH a souligné l'importance de compter sur "un partenaire de confiance possédant une expertise spécialisée dans les domaines clés de la cybersécurité". En concluant, il a mis en avant les avantages de ce partenariat, affirmant qu'il "simplifie la gestion opérationnelle, garantit un niveau de résultats prédictibles et renforce la résilience de l'entreprise face aux menaces cyber".

Malgré les challenges d'adoption amenés par les lois de souveraineté au Maroc, le Cloud est toujours perçu comme une opportunité à l'accélération de la digitalisation.

Quelle est votre approche de l'adoption du Cloud et au traitement de ses risques ?

M. Youness AIT BAMOH met en avant que « même pour les entreprises confrontées à ces problèmes de souveraineté, le cloud offre des avantages indéniables à l'investissement dans des datacenters conventionnels ». Il souligne l'importance d'une approche pragmatique, débutant par « la spécification précise des exigences et le soutien actif du haut management ». Il souligne que chez Ciments du Maroc, la stratégie « **cloud-first** » est adoptée, favorisant **l'innovation**, la **digitalisation** des processus, et la **gestion efficace** de projets tels que le **Big Data et l'IoT**, améliorant ainsi la **résilience et l'expérience des clients**. Par ailleurs, il mentionne l'émergence des Services Managés, soulignant que cette approche offre « **une grande flexibilité aux organisations** » en matière de cybersécurité, permettant une externalisation stratégique de services clés pour renforcer la résilience face aux menaces cyber.

Un fort enthousiasme des répondants marocains sur les apports de l'Intelligence Artificielle Générative pour la cyber défense

48% Des participants ont déjà mis en place un processus d'évaluation des risques liés à l'IA au sein de leurs organisations.

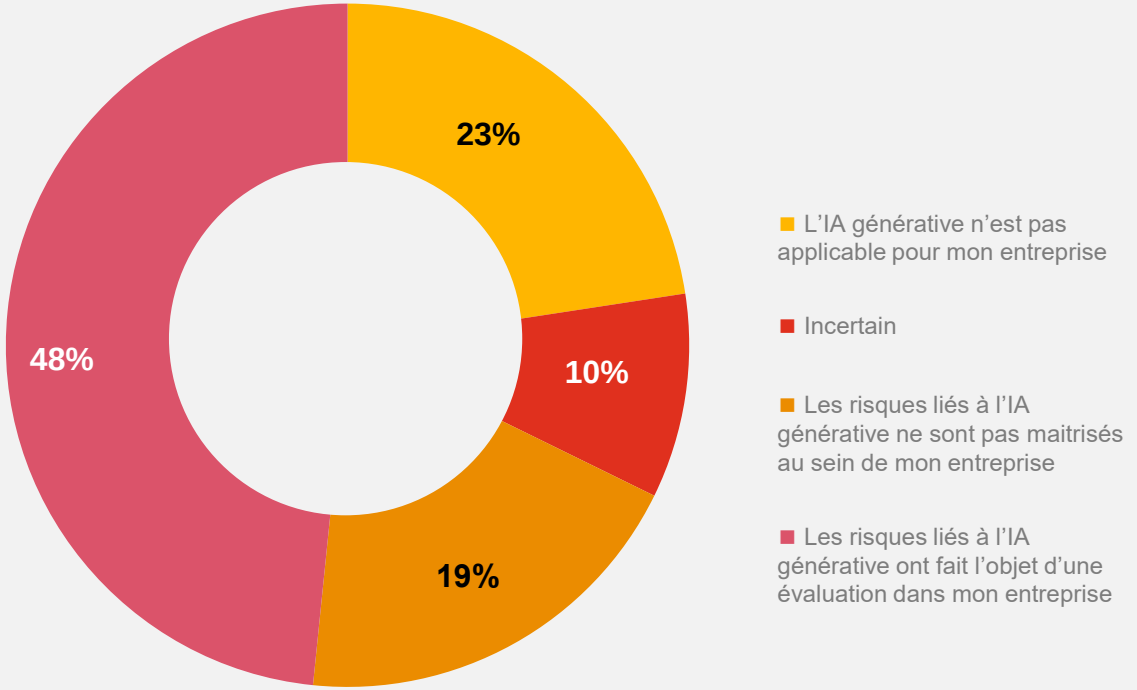
A l'échelle mondiale* :

l'IA Générative suscite un grand enthousiasme :

- Plus des deux tiers **(69%)** déclarent qu'ils utiliseront GenAI pour la défense cybernétique au cours de l'année 2024.
- Près de la moitié **(47%)** l'utilisent déjà pour renforcer la cyber défense (pour la détection notamment).
- Un cinquième **(21%)** ont déjà pu constater les bénéfices de l'Intelligence Artificielle générative pour la cyber défense, quelques mois seulement après son lancement public.

*Source: Global Digital Trust Insights 2024, PwC

Avis des répondants sur la maitrise des risques liés à l'IA générative



Témoignages

L'IA générative s'impose actuellement comme une technologie de rupture. Elle apportera vraisemblablement des opportunités de renforcement de la cybersécurité des entreprises mais amènera aussi son lot de challenges.

Comment appréhendez-vous cette technologie au sein de votre organisation ?

M. Imad TABEUTE
IT Manager et RSSI
Organisme financier

M. Imad TABEUTE souligne que « **l'adoption de l'IA générative nécessite une expertise technique et des ressources adéquates** ». Il souligne l'importance d'évaluer « **les avantages, les risques et les coûts associés** », tout en accordant une attention particulière à la « **conformité réglementaire en matière de protection des données et de confidentialité** ». Dans le cadre de leur démarche d'adoption, l'IA générative est exploitée principalement dans deux domaines cruciaux de renforcement de la protection cyber. D'une part, elle est utilisée dans la « **détection des menaces** », où elle permet d'analyser d'importantes quantités de données liées à la cybersécurité pour identifier des modèles et anomalies échappant aux méthodes de détection traditionnelle. D'autre part, elle contribue à « **l'amélioration des systèmes de détection d'intrusion** » en générant des signatures et des règles plus précises, facilitant ainsi l'identification de nouvelles variantes de logiciels malveillants et de techniques d'attaque avancées. En résumé, M. Imad TABEUTE souligne la nécessité d'une approche stratégique, tactique et opérationnelle pour tirer pleinement parti des opportunités offertes par l'IA générative tout en gérant ses défis associés.

M. Youness AIT BAMOH
IT Manager
Ciments du Maroc

M. Youness AIT BAMOH indique que « **l'intelligence artificielle générative offre aux entreprises une opportunité similaire à celle de l'émergence d'internet dans les années 90** ». Il met en avant l'importance de considérer divers facteurs tels que « le modèle commercial, les pratiques opérationnelles, le secteur industriel et le mindset des collaborateurs » pour déterminer l'impact de cette technologie sur l'entreprise. Selon lui, l'adoption de l'IA générative n'est pas seulement une mise en œuvre technique, mais nécessite également « **une formation, une communication, une mesure de l'adoption et un soutien continu** ». Il partage l'expérience de Ciments du Maroc, décrivant le déploiement progressif de l'IA générative à différents niveaux de l'entreprise. Il souligne que son organisation a commencé par des cas d'usage simples tels que la « **génération de texte et les chatbots** », en mettant l'accent sur le « **développement des compétences**" et l'identification de « **champions collaborateurs réceptifs** ». Il indique que l'objectif est d'utiliser cette technologie pour « **améliorer la prise de décision** », « **optimiser les ressources** » et « **réduire la consommation** », tout en poursuivant des initiatives visant l'excellence opérationnelle. Il met également en avant la collaboration avec des parties prenantes locales dans le domaine de l'IA générative, notamment des startups et d'autres organisations partageant la même vision.

Au plan mondial*, 4 objectifs réglementaires qui amélioreront la posture cyber des entreprises

Mise en place d'un cadre réglementaire des technologies d'Intelligence Artificielle

37%

36%

Harmonisation des textes réglementaires sur la cybersécurité et la protection des données

Obligation de reporting cyber

35%

32%

Exigences réglementaires de résilience opérationnelle

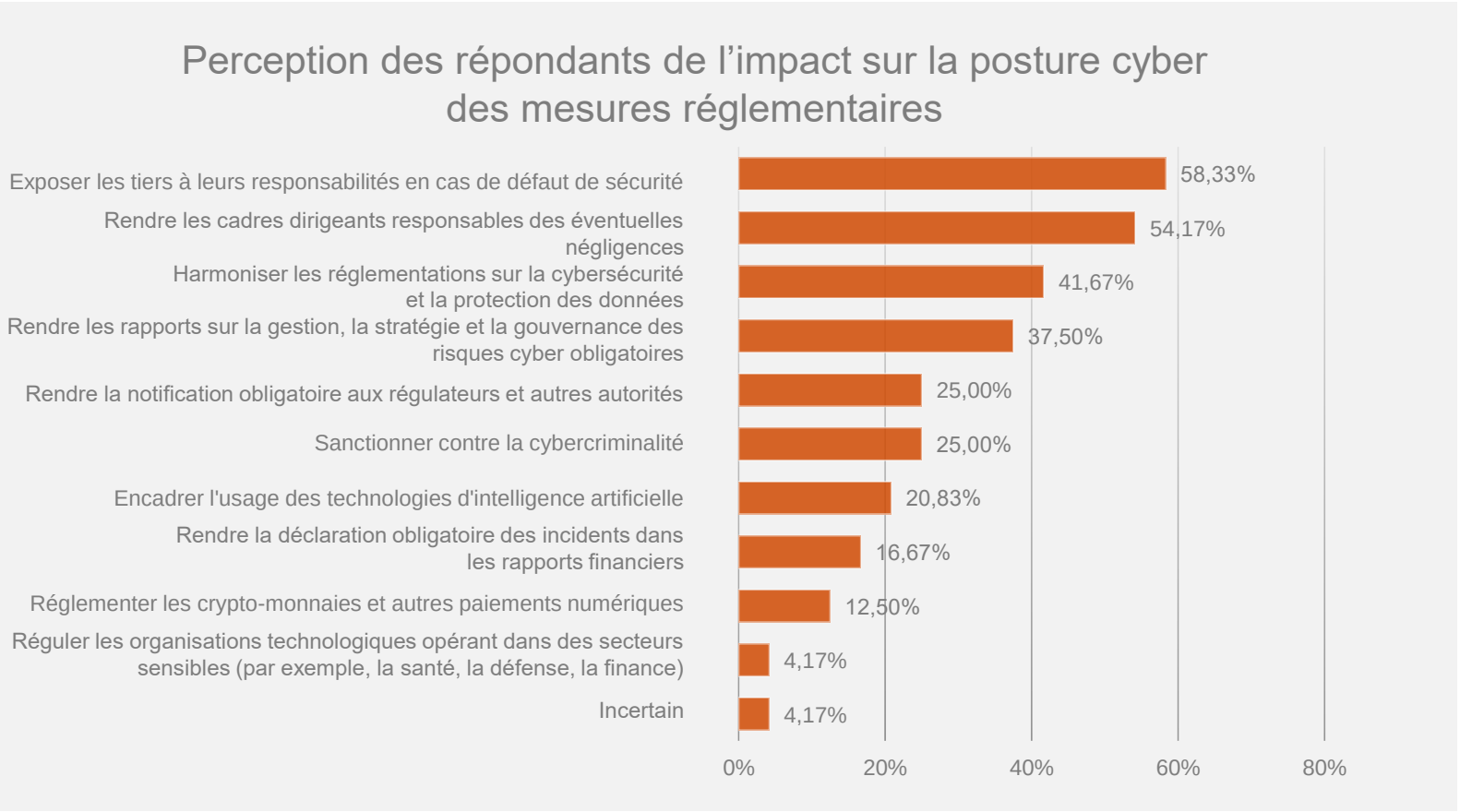
*Source: Global Digital Trust Insights 2024, PwC

Au Maroc, 58% des répondants déclarent qu'exposer les tiers à leurs responsabilités en cas de défaut de sécurité amènerait un meilleur levier à l'amélioration cyber

Pour répondre aux enjeux de cybersécurité et de protection des données, un arsenal juridique a été mis en place depuis 2009 avec différentes lois notamment la loi 09-08 relative à la protection des données personnelles.

En outre, la DGSSI (Direction Générale de la Sécurité des Systèmes d'Information) a promulgué la Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI) en 2014, puis l'a révisée en 2023. Cette directive vise à améliorer et à standardiser le niveau de protection et de maturité de la sécurité des systèmes d'information dans
toutes les administrations et organismes publics, ainsi que dans les infrastructures d'importance vitale.

Cet arsenal a été enrichi par la promulgation de la loi n° 05-20 relative à la cybersécurité, représentant un ensemble de mesures de sécurité qui sont destinées à accroître les capacités nationales dans le domaine de la cybersécurité.



Témoignages

Comment percevez-vous et abordez-vous les enjeux liés à l'évolution du cadre réglementaire sur la cybersécurité au Maroc ?

M. Imad TABEUTE
IT Manager et RSSI
Organisme financier

M. Imad TABEUTE souligne l'importance pour les institutions financières de maintenir une « culture de sécurité forte et proactive » face à l'évolution du cadre réglementaire sur la cybersécurité au Maroc. Il indique qu' « En adoptant une approche proactive, elles peuvent mieux répondre aux enjeux de cybersécurité et assurer la protection de leurs activités et de leurs clients ». Il met en avant plusieurs stratégies pour aborder ces enjeux, notamment la « **veille réglementaire** » en **suivant de près les nouvelles lois et directive**s émises par les autorités compétentes, telles que la Banque centrale, la DGSSI et la CNDP. Il précise l'importance de la « conformité aux réglementations », en adaptant les pratiques et les politiques pour répondre aux exigences spécifiques en matière de cybersécurité. Il indique que cela inclut la **protection des données personnelles, la gestion des incidents de sécurité et la mise en place de mesures de prévention et de détection des cyberattaques.**

En outre, il insiste sur le « **renforcement des capacités internes** » par le biais de la formation du personnel sur les bonnes pratiques de sécurité, les **nouvelles réglementations** et les techniques de prévention et de détection des cyberattaques. Il indique également qu'en cas de besoin, des « expertises externes en cybersécurité » sont sollicitées pour soutenir les équipes internes.

M. Youness AIT BAMOH
IT Manager
Ciments du Maroc

M. Youness AIT BAMOH indique que « Le Maroc a acquis une certaine **maturité juridique** en matière de cybersécurité depuis des années grâce à l'**adoption de lois** spécifiques et à la création d'organismes régulateurs spécialisés, comme les **lois 05-20, 53-08, 09-08** et des institutions importantes telles que la **Direction Générale de la Sûreté Nationale et la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel** », marquant ainsi une « évolution positive ».

Cependant, il souligne la nécessité de r**enforcer la sensibilisation et la communication** autour de ces lois, notamment en mettant en évidence le manque de connaissance de la **loi 09-08** par la majorité des citoyens. Il insiste sur l'importance de **diffuser ces informations** non seulement aux entreprises mais aussi aux citoyens en précisant que « les utilisateurs d'Internet, y compris les enfants, sont confrontés aux risques liés à la violation de leur vie privée ».

En conclusion, M. Youness AIT BAMOH met en avant la nécessité de renforcer la diffusion d'informations pour assurer une protection globale dans l'utilisation quotidienne de la technologie.

3 - Quelques recommandations clés

Quels enseignements retirer de cette enquête ?

En conclusion, cette enquête a révélé plusieurs points clés qui peuvent éclairer nos décisions et stratégies futures en matière de cybersécurité :

Évolution des risques cyber

Mettre en place une activité de veille sur la menace cyber pour couvrir le contexte spécifique de l'entreprise

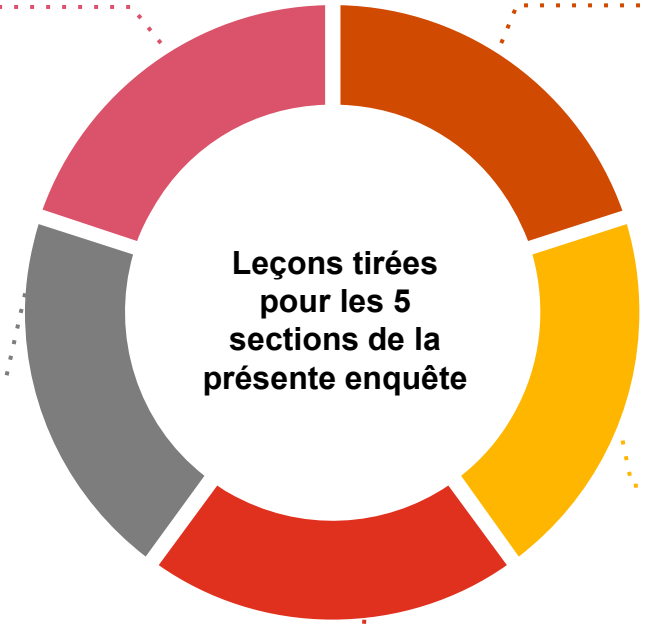
Renforcer les efforts de sensibilisation au risque cyber dans un contexte où le cout des incidents cyber pour l'entreprise augmente

Mettre en place un processus de due diligence cyber dans le contexte des fusions et acquisition

Priorités d'investissement cyber

Poursuivre les investissements réalisés sur l'upskilling des talents

Etudier les opportunité de rationnalisation du portefeuille technologique cyber



Tendances technologiques

Définir la stratégie de Move to Cloud et de sécurisation associée

Etudier les impacts de l'IA générative et définir l'approche de maitrise des risques liés à cette technologie de rupture afin d'en permettre le passage à l'échelle

Enjeux réglementaires

Analyser les exigences attendues de la réglementation marocaine afin de déterminer la meilleur stratégie de Move to Cloud (hybridation)

Niveau de maturité cybersécurité des entreprises

Poursuivre l'utilisation de frameworks reconnus pour évaluer la posture cyber de l'entreprise, piloter son programme cyber et analyser ses coûts

Osez faire évoluer les modes de fonctionnement établis : quelques réflexions pour appréhender l'évolution actuelle du risque cyber

Faites évoluer le language cyber
CISO, CFO, Direction Générale

Permettez à vos équipes d'être créatives
(automatisation, intelligence artificielle générative, services *managés*)
CISO, CIO, CTO, CRO, COO

Explorez des nouvelles façons pour gérer les risques cyber
CISO, CRO, IA, CCO, COO

Élevez la cybersécurité au niveau des comités exécutifs et des conseils d'administration
CISO, Board, CEO

Construisez le cadre de maîtrise du risque cyber
CISO, CIO, Direction Générale, Direction juridique

Intégrez la perspective business dans l'approche cyber
CISO, CEO

Annexe : détail des statistiques de l’enquête

La cybersécurité est plus que jamais une préoccupation majeure pour les dirigeants d'entreprise

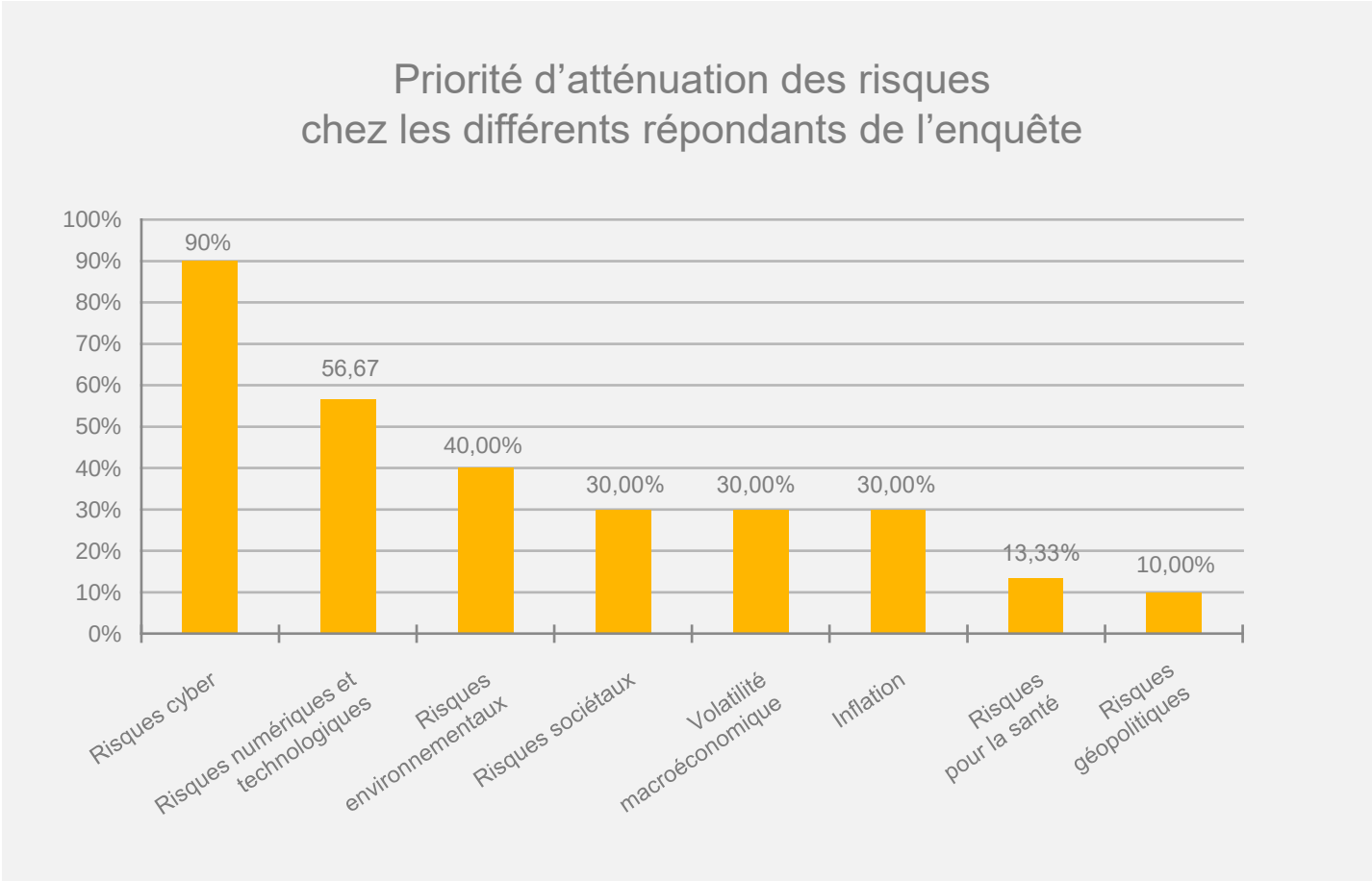
90%

Des répondants ont identifié les risques cyber comme une priorité majeure d'atténuation au cours des 12 prochains mois.

A l'échelle de l'Afrique* :

La cybersécurité est jugée d'une importance moyenne de **3,6** sur une échelle de **0 à 5** par les répondants en Afrique francophone subsaharienne, ce qui en fait un sujet crucial dans la région. Les répondants du secteur financier accordent une importance plus élevée (moyenne de **4,05**), tandis que ceux du secteur de la consommation affichent la moyenne la plus basse (**2,88**) et seulement **29%** des répondants travaillant dans des institutions publiques estiment que la cybersécurité est une priorité pour leurs organisations.

* Source : Les enjeux et défis de la cybersécurité en Afrique francophone subsaharienne (Mars 2021), PwC



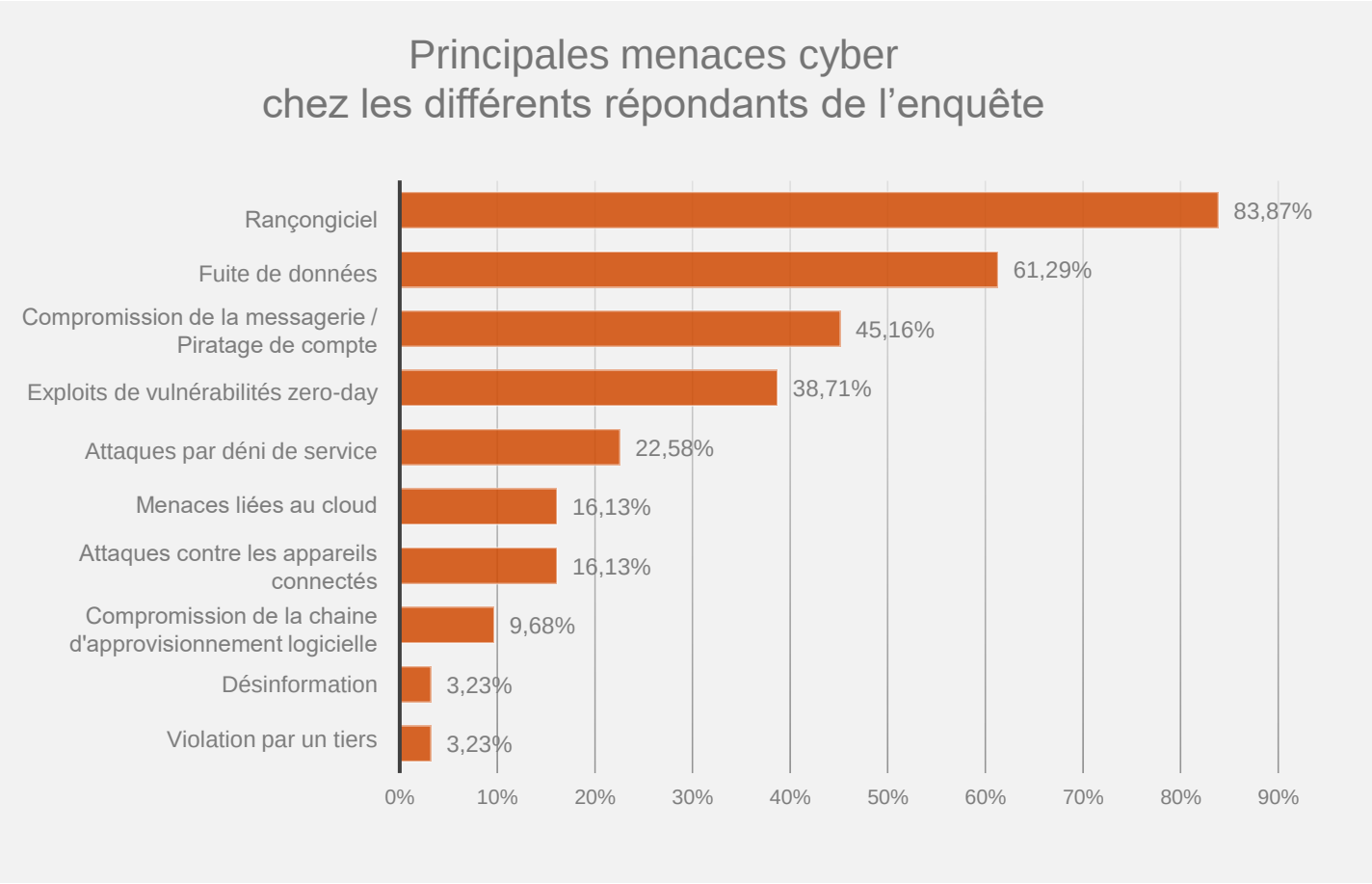
Les organisations se préoccupent principalement des rançongiciels en termes des menaces cyber

84% Des répondants se préoccupent, au cours des 12 prochains mois, des attaques par rançongiciels.

A l'échelle mondiale* :

45 % des cadres de la sécurité et des technologies de l'information prévoient une augmentation supplémentaire des **attaques de rançongiciel**.

* Source : Global Digital Trust Insights 2023, PwC



La fuite de données, principale préoccupation des répondants marocains

84% Des répondants expriment une forte inquiétude concernant les fuites de données client, employé ou transaction.

A l'échelle mondiale* :

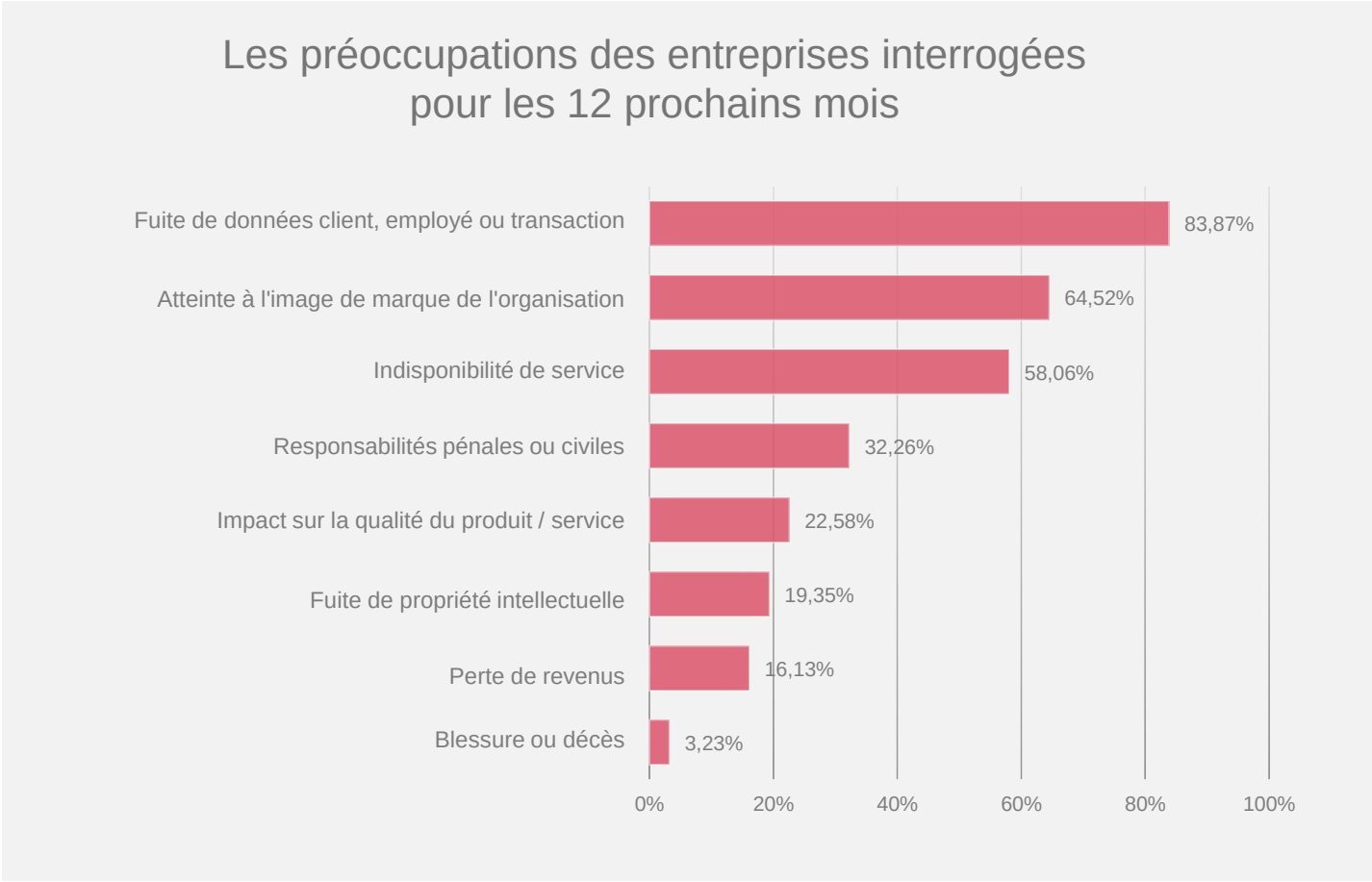
D'après l'étude de PwC, **38%** des organisations expriment des inquiétudes concernant les attaques futures via le cloud, soulignant que l'impact majeur de ces attaques serait l'**atteinte à l'image** de l'entreprise. **49%** des responsables informatiques et de la sécurité anticipent une augmentation des attaques de type ransomware, susceptibles de perturber ainsi la **disponibilité des services de production**.

* Source : Global Digital Trust Insights 2024, PwC

A l'échelle de l'Afrique* :

Selon l'enquête menée auprès des entreprises d'Afrique subsaharienne*, les pirates informatiques ou les cyber-mercenaires ne sont pas toujours motivés par l'argent, contrairement à la cybercriminalité traditionnelle. Leur objectif principal est de **voler des données privées** afin de les monétiser autrement, souvent en fournissant des conseils ou des informations basés sur ces données et ainsi divulguer un avantage concurrentiel.

* Source : Les enjeux et défis de la cybersécurité en Afrique francophone subsaharienne, PwC



D'importantes pertes financières engendrées par la divulgation de données confidentielles

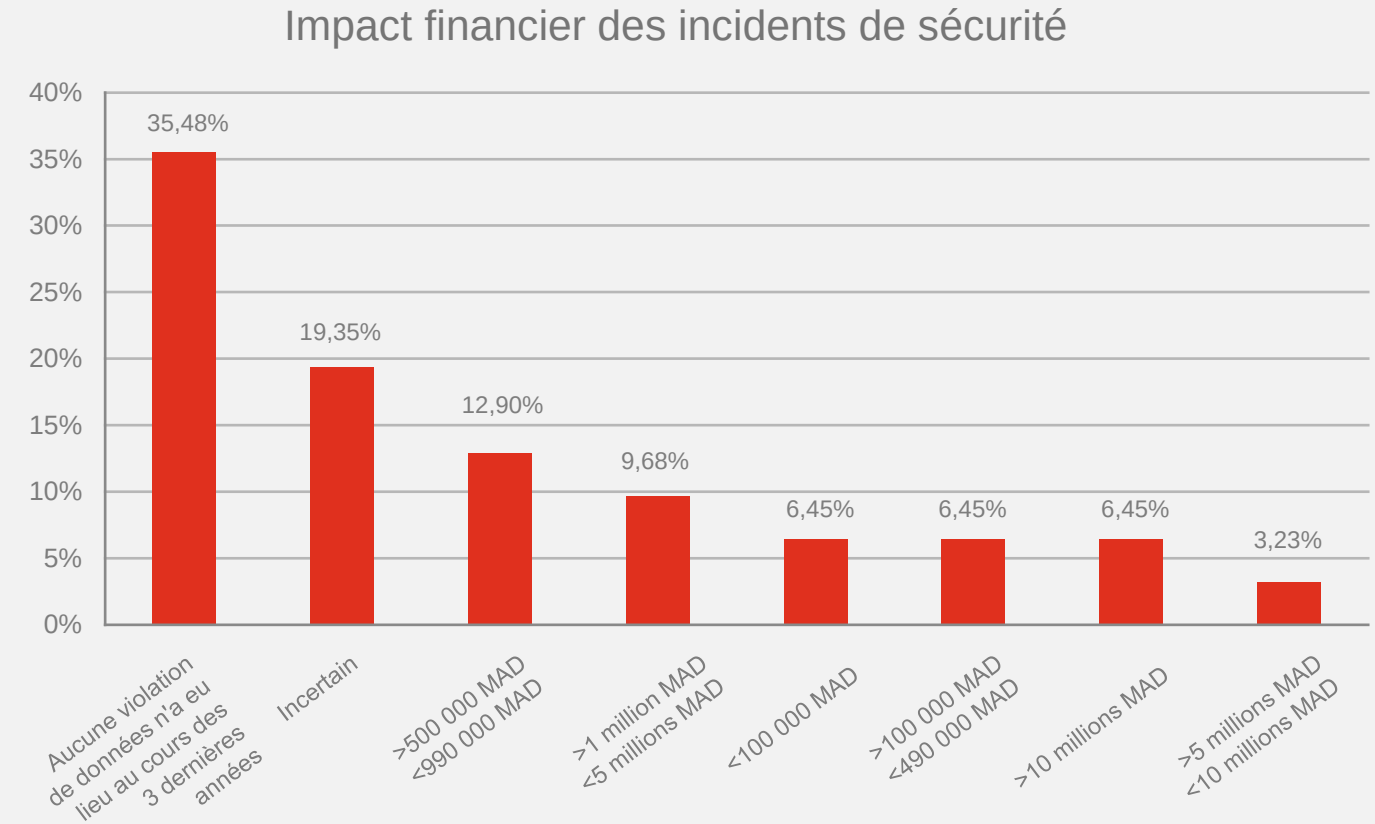
+500
K MAD

Les coûts associés aux incidents de fuite de données sont différents d'une organisation à l'autre, mais une proportion significative (32%) se situe principalement dans les tranches de 500 000 MAD et plus.

A l'échelle mondiale* :

Le taux s'élève à **36%** pour ceux qui ont connu une **violation de données** entraînant des coûts d'au moins **1 million de dollars**, comparativement à **27%** de l'année précédente.

* Source : Global Digital Trust Insights 2024, PwC



Les entreprises investissent considérablement dans la cyber, soulignant leur prise de conscience de son importance

78% Des entreprises interrogées estiment que leur budget en cybersécurité représente jusqu'à 25% de leurs dépenses technologiques en 2023.

A l'échelle mondiale* :

De nombreux acteurs ont entrepris de revoir leur stratégie d'investissement en cybersécurité afin qu'elle :

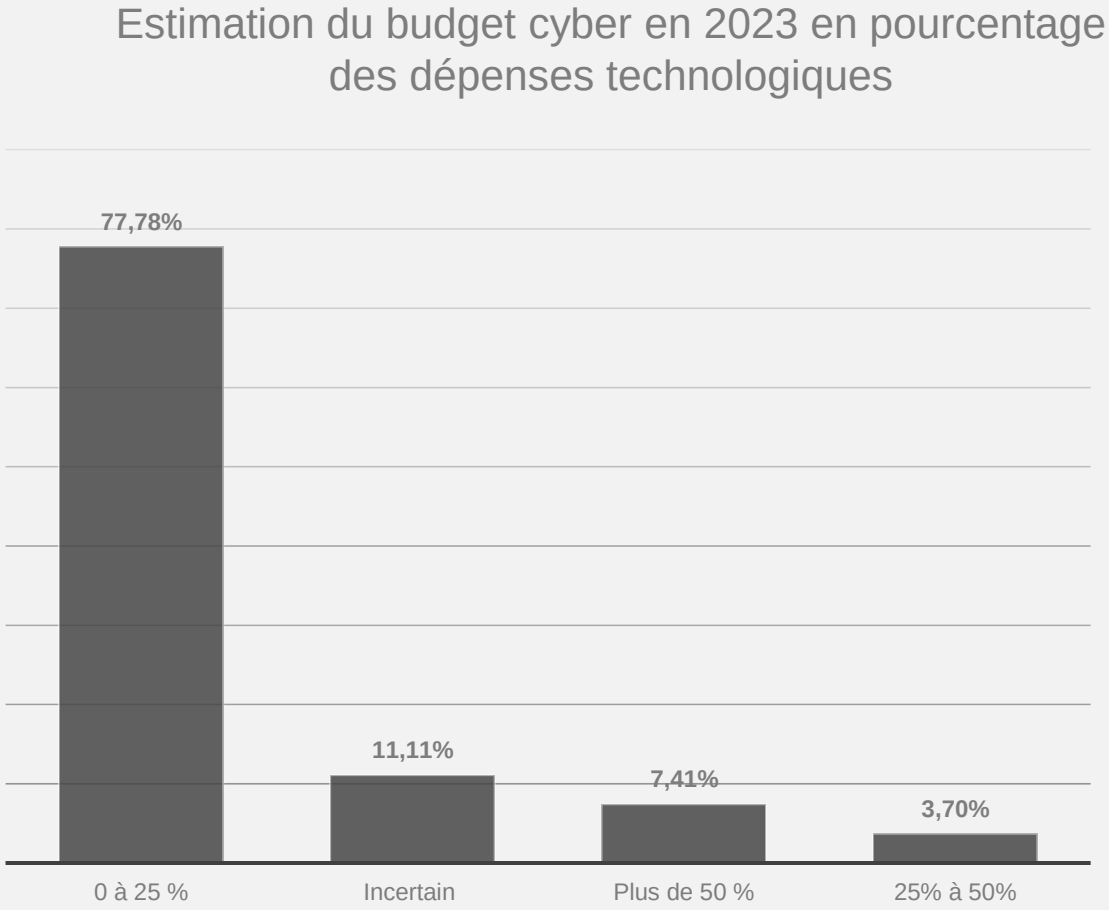
- Soit alignée avec la stratégie globale de l'entreprise (**55%**)
- Reflète les priorités en cybersécurité (**55%**)
- Ajoute de la valeur à l'organisation (**52%**)
- Équilibre les besoins immédiats et à long terme (**51%**)
- Soit informé par la quantification des risques (**51%**)
- Considère l'appétit pour le risque de l'organisation (**51%**)
- Alloue de manière adéquate contre les risques auxquels l'organisation est confrontée (**51%**)

* Source : Global Digital Trust Insights 2023, PwC

A l'échelle de l'Afrique* :

En Afrique Francophone Subsaharienne (AFSS), la cybersécurité est évaluée à **3.6** en moyenne par les répondants africains sur une échelle de 0 à 5. Ce constat confirme que la cybersécurité est un sujet d'importance capitale dans la région de l'AFSS.

*Les enjeux et défis de la cybersécurité en Afrique francophone subsaharienne (Mars 2021), PwC



Les entreprises augmentent leurs budgets de cybersécurité, illustrant une prise de conscience croissante des risques numériques

52%

Des entreprises répondantes envisagent d'augmenter leur budget cyber jusqu'à 14%, reflétant ainsi une prise de conscience croissante des enjeux cybernétiques.

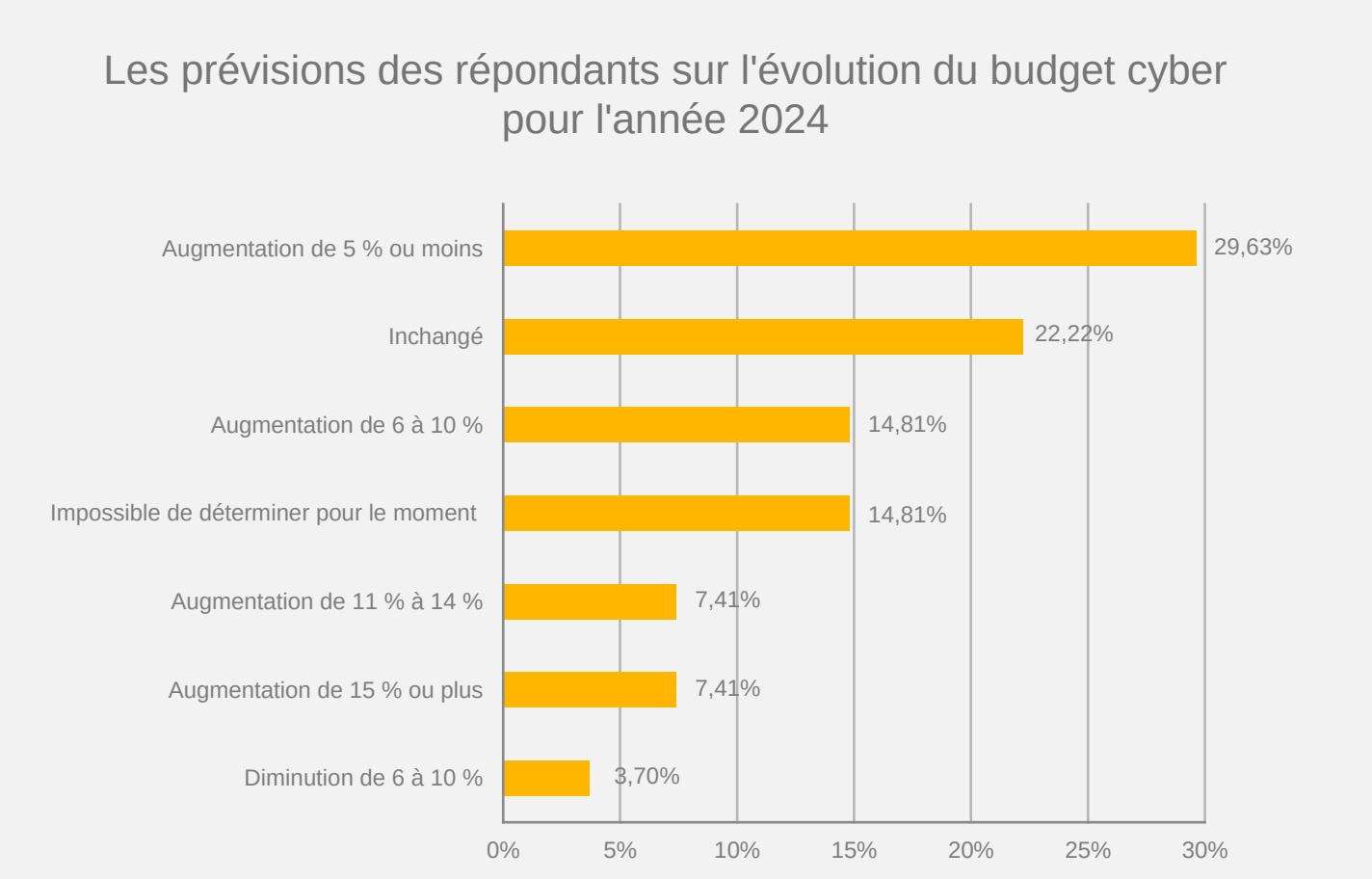
À l'échelle mondiale* :

Les entreprises continuent d'augmenter leurs dépenses en cybersécurité. **65%** des répondants à notre enquête ont indiqué prévoir une **augmentation de leur budgets cyber** en 2023 contre **69%** en **2022**.

De manière prévisible, les organisations ayant fait l'objet d'un incident de sécurité ont manifesté une propension notablement plus élevée à envisager d'augmenter leurs dépenses en cybersécurité pour l'année 2023.

Et parmi les grandes entreprises (avec des revenus annuels supérieurs à 1 milliard de dollars), **10%** ont déclaré que leurs dépenses en cybersécurité **augmenteraient** de **15% ou plus.**

* Source : Global Digital Trust Insights 2023, PwC



L'amélioration des compétences au coeur de la stratégie de développement des talents cyber

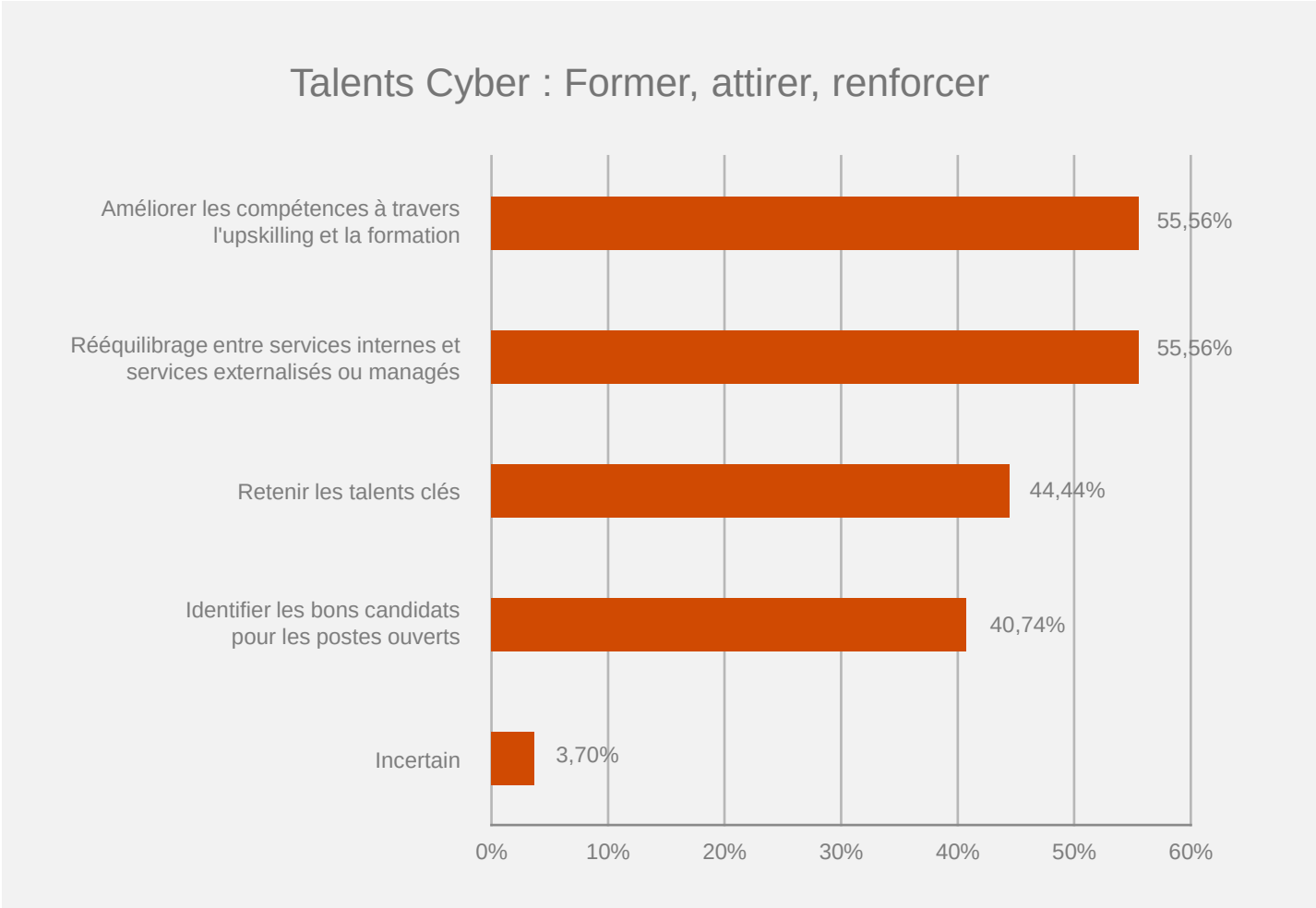
56%

Des entreprises interrogées priorisent la gestion des talents en cybersécurité à travers l'amélioration des compétences grâce à l'upskilling et la formation.

A l'échelle de l'Afrique* :

Spécifiquement en Afrique francophone subsaharienne, **55%** des répondants **ne disposent pas d'un programme de sensibilisation à la cybersécurité** ou estiment que le programme de sensibilisation existant ne répond pas complètement aux besoins de l'entreprise en matière de cybersécurité.

* Source : Les enjeux et défis de la cybersécurité en Afrique francophone subsaharienne (Mars 2021), PwC



Diverses initiatives déployés par les entreprises marocaines pour renforcer leur posture en matière de cybersécurité face aux menaces digitales

A l'échelle de l'Afrique* :

Moins de **40%** des répondants ont effectué une analyse des risques durant les 6 mois précédant l'enquête. **26%** des entreprises n'ont pas effectué une analyse des risques depuis plus de deux ans, parmi celles-ci, **16 %** font partie du secteur financier.

Les actions nécessaires pour la correction des écarts constatés à la suite de l'analyse des risques, ont été mises en place partiellement ou pas du tout dans **64%** des entreprises interrogées.

* Source : Les enjeux et défis de la cybersécurité en Afrique francophone subsaharienne (Mars 2021), PwC

Cette enquête a permis d'explorer les initiatives variées mises en œuvre par les organisations marocaines, afin de renforcer leur position en matière de cybersécurité face aux menaces cyber. Parmi les principales actions mises en avant par les répondants nous retrouvons :

36%

Ont déjà mis en œuvre l'identification des processus métiers critiques dans certaines parties de l'organisation.

41%

Ont déjà mis en en place une cartographie des dépendances technologiques dans certaines parties de l'organisation.

41%

Ont déjà mis en en place un plan de reconstruction informatique après une cyberattaque dans certaines parties de l'organisation.

37%

Déclarent que des solutions technologiques favorisant la résilience, telles que les sauvegardes et les environnements de restauration isolés, sont mis en œuvre dans toute l'organisation.

30%

Déclarent actuellement mettre en œuvre une équipe « Résilience » , englobant des fonctions telles que la cybersécurité, la continuité des activités et la gestion de crise dans l'ensemble de l'organisation.

L'état des capacités technologiques des organisations révèle une satisfaction modérée (½)

A l'échelle mondiale* :

Les entreprises expriment leur satisfaction à l'égard de leurs compétences technologiques de la manière suivante :

- **56%** sont satisfaits de leurs compétences en réseau / pares feux / VPN.
- **52%** sont satisfaits de leur gestion et gouvernance en matière de sécurité.
- **50%** sont satisfaits de leur gestion des accès et des identités (IAM).
- **42%** sont satisfaits de leur capacité d'automatisation et d'orchestration de la réponse aux incidents de sécurité (SOAR).
- **43%** sont satisfaits de la sécurité de leur chaîne d'approvisionnement.

* Source : Global Digital Trust Insights 2024, PwC

La satisfaction modérée des organisations interrogées envers leurs capacités technologiques souligne un besoin urgent d'amélioration. En comprenant les lacunes perçues et en agissant rapidement pour les combler, les entreprises peuvent mieux se préparer face aux défis croissants de cybersécurité.

Les répondants ont évalué leurs capacités par rapports à diverses technologies, ci-dessous le premier volet de celles qui ont été sondées :

48%

Indiquent être assez satisfaits de leurs capacités en matière de gestion et de gouvernance des risques et contrôles.

24%

Affirment ne pas être très satisfaits de leurs capacités en matière d'automatisation et d'orchestration de la réponse aux incidents de sécurité (SOAR).

56%

Indiquent être assez satisfaits de leurs capacités en matière des technologies réseau/pare-feux/VPN.

28%

Expriment une incertitude envers leurs capacités en matière de sécurité de leur chaîne d'approvisionnement.

28%

Affirment être assez satisfaits de leurs capacités en matière de gestion des identités et des accès.

L'état des capacités technologiques des organisations révèle une satisfaction modérée (2/2)

A l'échelle mondiale* :

Les entreprises expriment leur satisfaction à l'égard de leurs compétences technologiques de la manière suivante :

- **52%** sont satisfaits de leur capacité de détection et de réponse.
- **52%** sont satisfaits de leurs mesures de sécurité des données et de confidentialité.
- **41%** sont satisfaits de leurs mesures de sécurité des systèmes industriels et IoT (Internet des objets).
- **53%** sont satisfaits de la sécurité en matière de cloud.

* Source : Global Digital Trust Insights 2024, PwC

Nous aborderons à présent le deuxième volet des technologies et techniques évalués par les répondants :

36%

Indiquent être assez satisfaits de leurs capacités en matière de détection et de réponse.

40%

Affirment être très satisfaits de leurs capacités en matière de sécurité OT.

36%

Indiquent être assez satisfaits de leurs capacités en matière de sécurité des objets connectés (IoT).

24%

Affirment être assez satisfaits de leurs capacités en matière de Cloud.

28%

Indiquent être assez satisfaits de leurs capacités en matière de sécurité et confidentialité des données.

Sécurité du cloud : une vigilance collective est attendue depuis longtemps

74% Des participants ont déjà intégré les risques liés au cloud et à la virtualisation dans leur plan de gestion des risques.

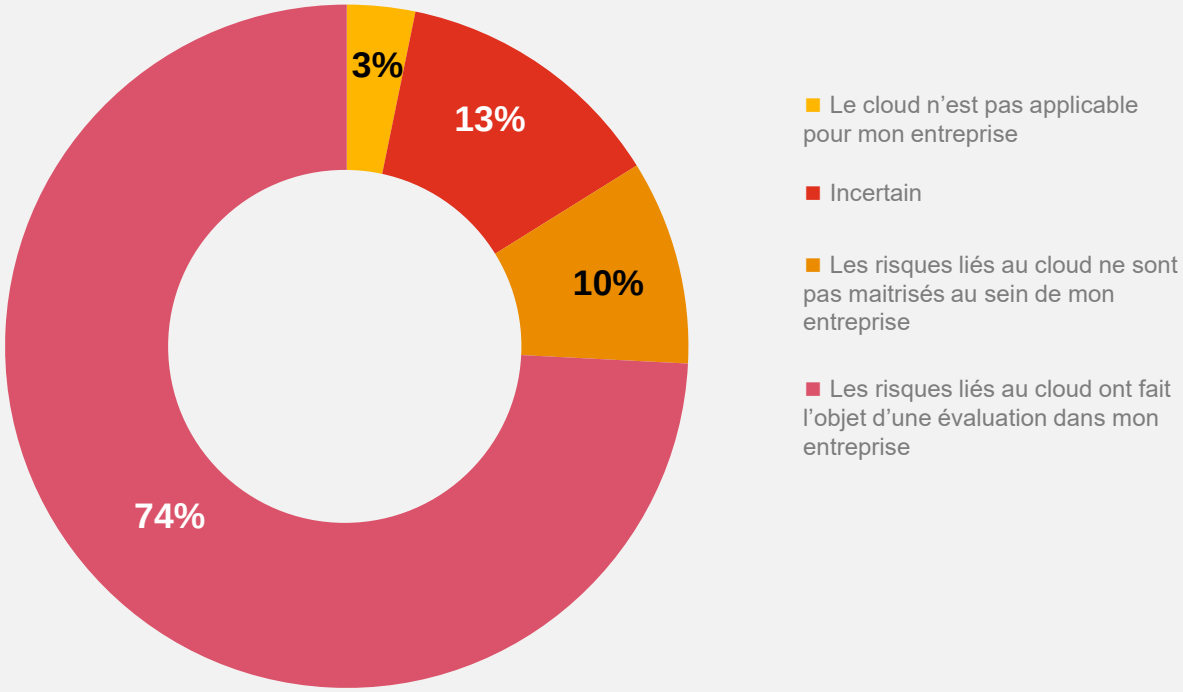
À l'échelle mondiale* :

47% des répondants sont particulièrement préoccupés par les attaques liées au cloud. Ce pourcentage atteint **54%** parmi les utilisateurs de fournisseurs de cloud hybride.

Principales priorités pour l'année 2024 :

- **47%** sont principalement préoccupés par les menaces liées au cloud.
- **33%** sont préoccupés par l'investissement dans la cybersécurité.
- Seulement **3%** ont mis en place un plan et le maintiennent constamment à jour dans tous les domaines.

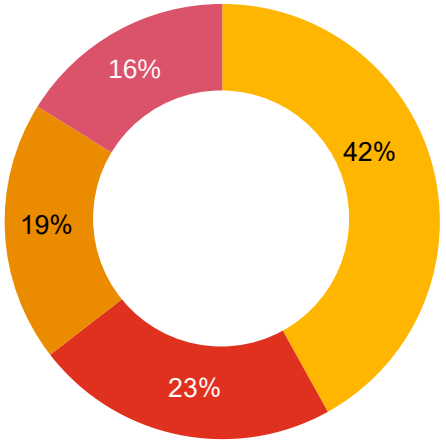
* Source : Global Digital Trust Insights 2024, PwC



La blockchain, la réalité virtuelle et la crypto-monnaie ne sont pas considérées comme des priorités au Maroc

La Blockchain, la réalité virtuelle et la crypto-monnaie ne sont pas actuellement identifiées comme des priorités dans le paysage technologique marocain. Les entreprises et les organisations marocaines semblent accorder moins d'attention à ces domaines par rapport à d'autres aspects technologiques. Cette observation peut s'expliquer par divers facteurs, tels que le manque de sensibilisation quant aux avantages potentiels de ces technologies, les défis réglementaires associés à leur adoption, ou encore la priorisation de la mise en œuvre d'autres technologies émergentes telle que l'intelligence artificielle générative.

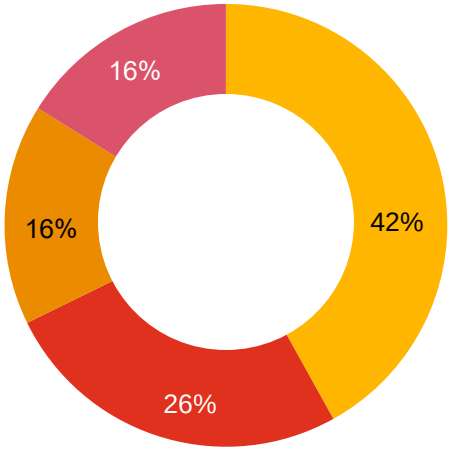
Blockchain



42% des participants affirment que la Blockchain n'est pas implémentée au sein de leurs organisations.

Cependant, **16%** des participants ont déjà mis en place un processus d'évaluation des risques liés à la blockchain.

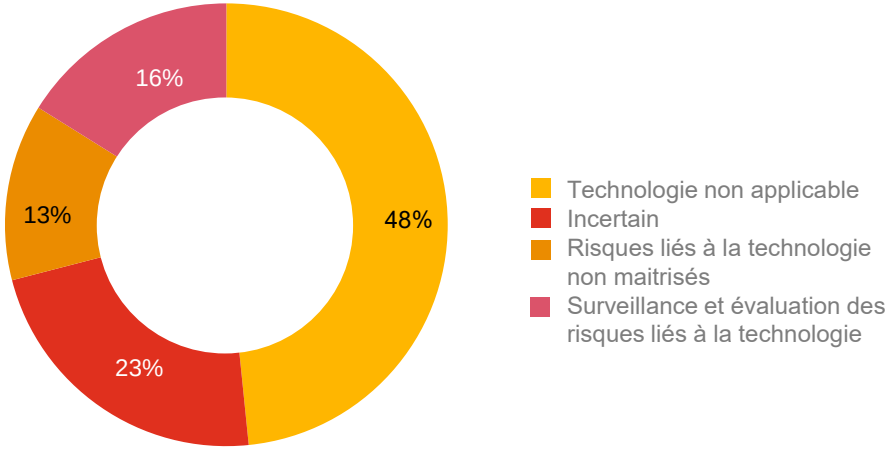
Réalité virtuelle



42% des participants déclarent que la réalité virtuelle n'est pas déployée au sein de leurs organisations.

Néanmoins, **16%** des participants ont confirmé l'intégration des risques liés à la réalité virtuelle dans leurs plans de gestion des risques.

Crypto-monnaie



48% des participants indiquent que la crypto-monnaie n'est pas intégrée au sein leurs organisations.

Toutefois, **16%** des participants ont déjà réalisé une évaluation des risques associés à la crypto-monnaie.

Le Move to Cloud : une démarche encore à développer, l'hybridation comme approche

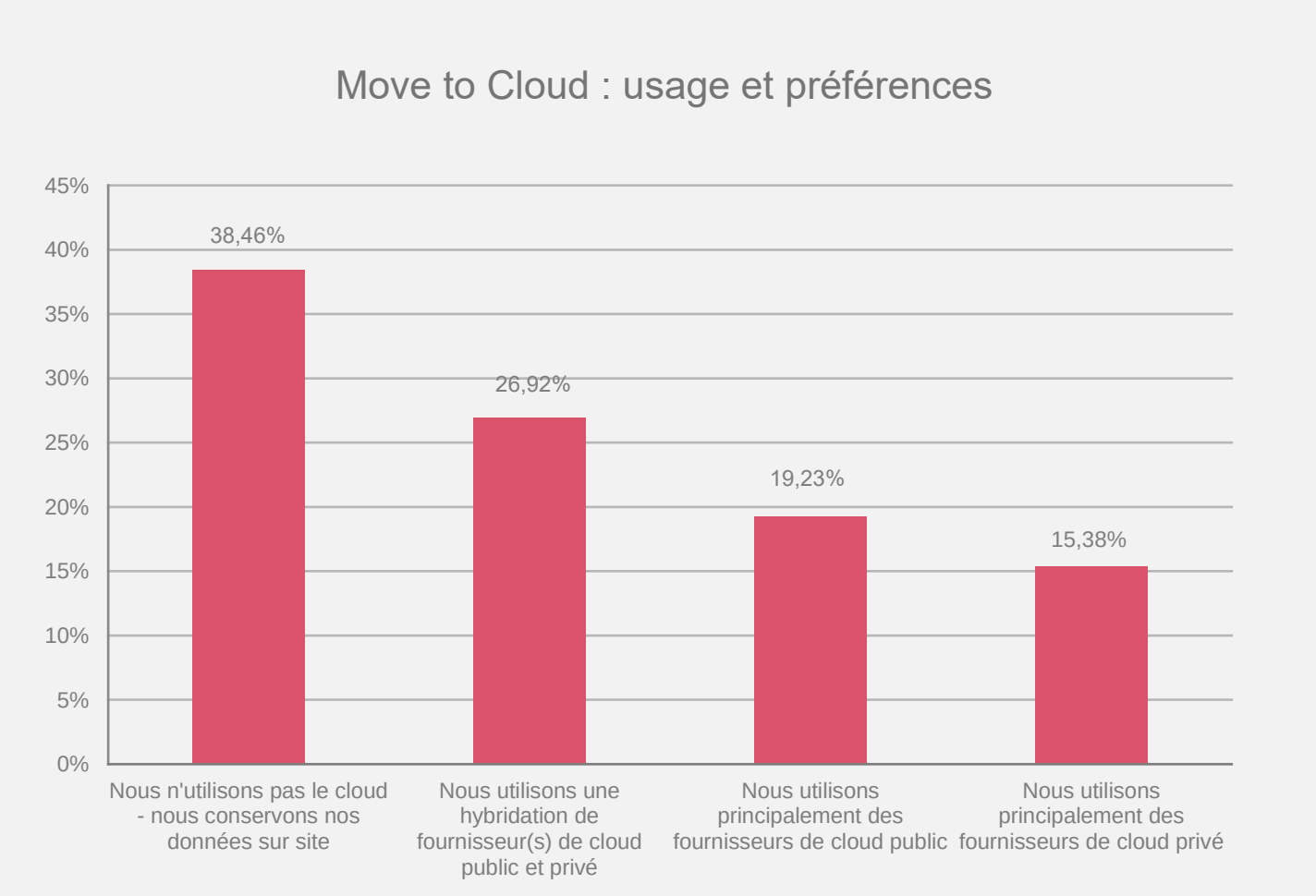
62%

Des répondants utilisent le Cloud, avec une adoption différenciée entre le mode d'utilisation: public, privé ou hybride.

À l'échelle mondiale* :

38% des répondants s'attendaient à des **attaques plus sérieuses via le Cloud** en 2023 démontrant la confiance relative des organisations dans la sécurité de leurs environnement déployés dans le Cloud.

* Source : Global Digital Trust Insights 2023, PwC



Microsoft Azure se positionne en tête des choix privilégiés par les entreprises recourant aux services cloud

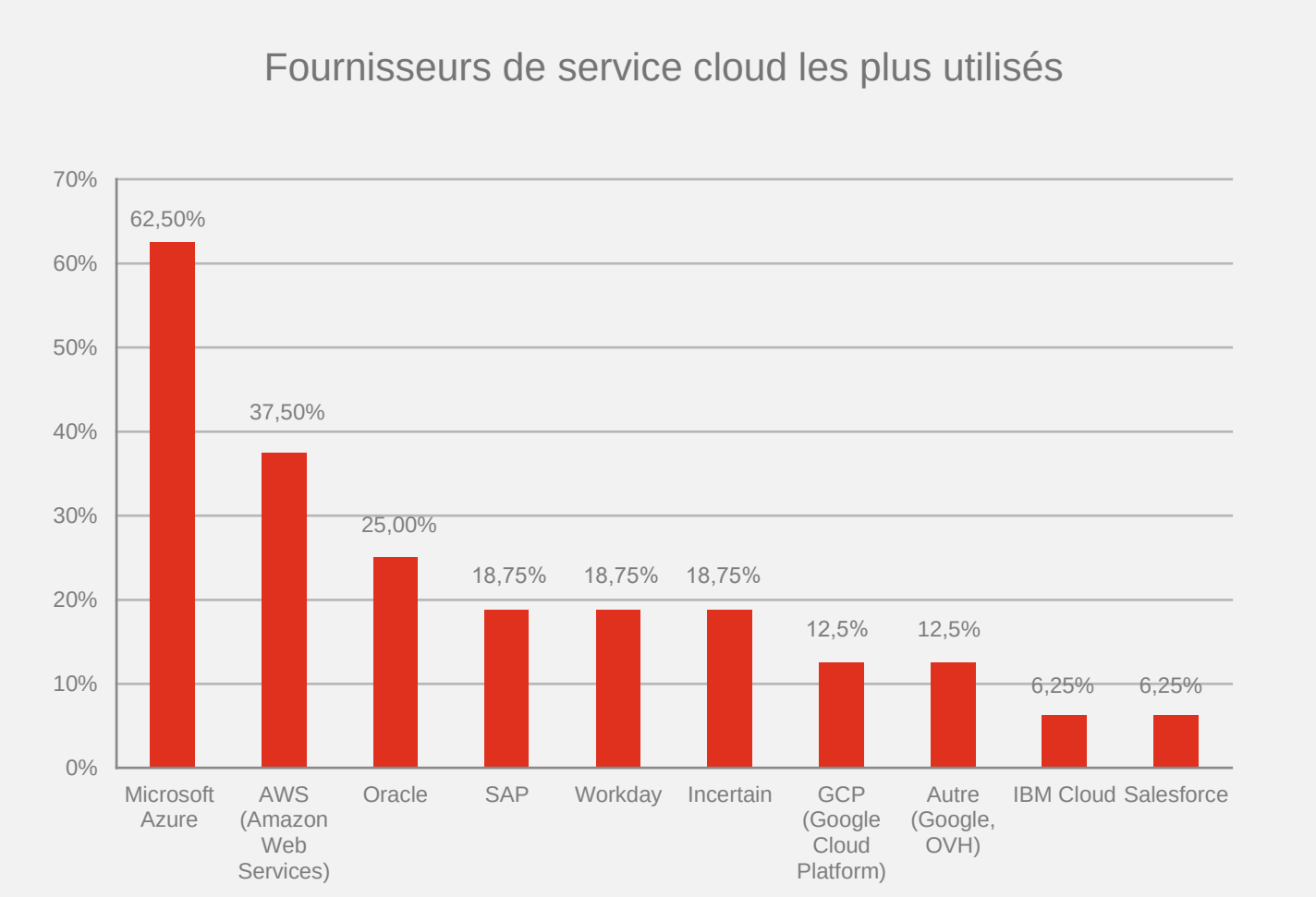
62% Des organisations interrogées utilisent Microsoft Azure.

À l'échelle mondiale* :

Les principaux leaders des solutions de cloud, selon l'étude de Gartner réalisée en 2023 sont :

- AWS (Amazon Web Services)
- Microsoft
- Google
- Oracle

* Source : Magic Quadrant for Strategic Cloud Platform Services (December 2023), Gartner



Une surveillance et une évaluation continues ont été constatées chez les organisations interrogées à l'égard de leurs fournisseurs

À l'échelle Africaine* :

Seuls **35%** des répondants déclarent avoir mis en place un programme de gestion des risques de cybersécurité émanant des tiers (Supply chain, Support Technique, etc.).

Parmi les **65%** qui n'en disposent pas d'un programme pareil, **31%** ont déclaré avoir prévu de s'en doter à moyen terme, tandis que **19%** ne prévoient pas de le faire (dont **9%** appartenant au secteur financier et **33%** appartenant au secteur gouvernemental et public).

* Source : Les enjeux et défis de la cybersécurité en Afrique francophone subsaharienne, PwC

47%

Des répondants surveillent et évaluent les risques liés :

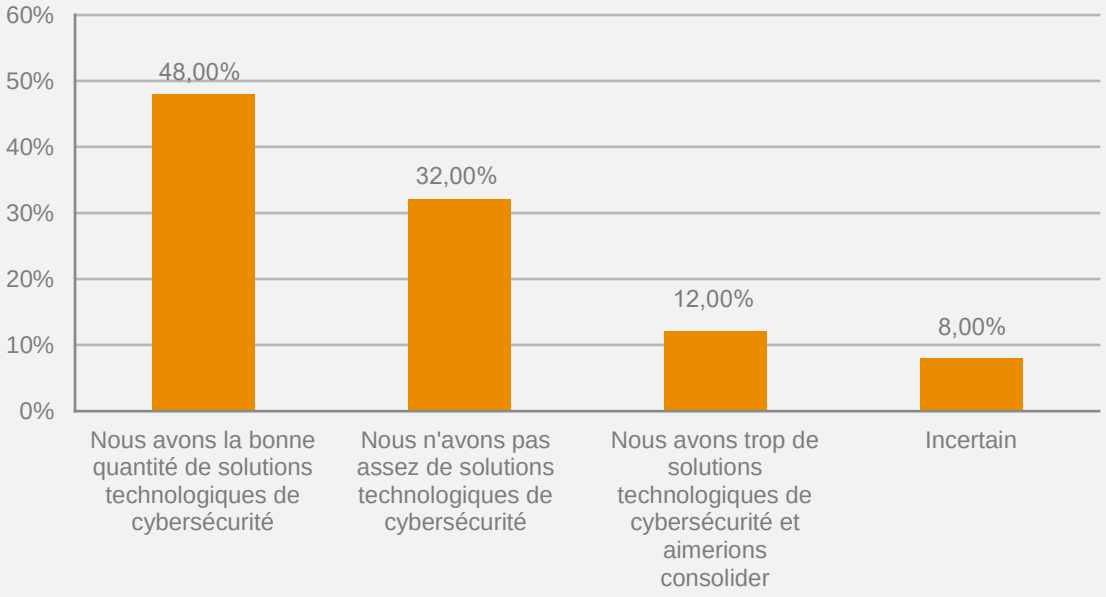
- A leur capacité à reprendre leurs activités en cas de sinistre.
- Aux exigences réglementaires.
- Aux programmes de concentration liés à leurs fournisseurs.

Adoption et évaluation des solutions cybersécurité au niveau des organisations marocaines

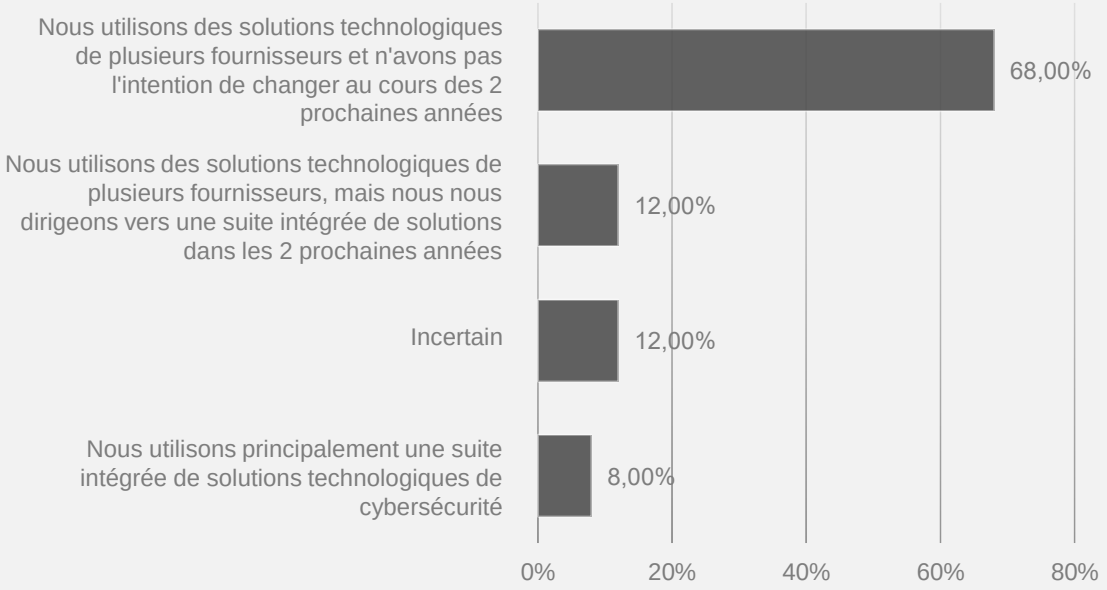
48% Des organisations affirment avoir déployées un portefeuille technologique cyber répondant à leur besoin.

68% Des organisations répondantes, utilisent des solutions de plusieurs fournisseurs et n'ont pas l'intention de changer au cours des 2 prochaines années.

Satisfaction en termes de solutions technologiques utilisées



L'approche technologique actuelle



Merci