
# Ausimètre 2025

## Baromètre de la cybersécurité au Maroc

Livre blanc présentant la synthèse des résultats de l'enquête

pwc

AUSIM
beyond digital

# Remerciement

Nous adressons notre profonde gratitude à toutes les entreprises et organisations qui ont pris le temps de participer à cette seconde édition de l'AUSIMÈTRE, contribuant ainsi à enrichir la réflexion sur la cybersécurité au Maroc.

Nos sincères remerciements vont également aux équipes engagées de PwC et de l'AUSIM, dont le travail rigoureux et le dévouement ont permis de structurer, analyser et superviser cette enquête avec la plus grande précision méthodologique.

# Sommaire


| | | |
|---|---|---|
| 1 | Propos introductifs | 04 |
| 2 | Principaux enseignements de l'enquête | 09 |
| 3 | Analyse détaillée des réponses de l'enquête | 11 |
| 4 | Témoignages d'experts | 21 |
| 5 | Passage à l'action : Recommandations | 28 |
| 6 | Passage à l'action : Introduction à la gestion de crise | 29 |

# Propos introductifs

## Accélérer la résilience numérique du Maroc : un engagement collectif indispensable

Hicham CHIGUER
Président de l'AUSIM

Dans un monde en perpétuelle mutation, où l'innovation technologique dessine de nouvelles frontières économiques et sociétales, la cybersécurité n'est plus une option : elle est devenue un impératif stratégique.

À travers cette seconde édition du baromètre de la Cybersécurité, l'AUSIM confirme sa volonté d'agir en éclaireur, en catalyseur et en fédérateur pour aider notre écosystème à naviguer avec confiance et ambition dans cette ère de risques accrus et d'opportunités exponentielles.
Les constats tirés de ce baromètre révèlent des avancées notables, mais aussi des défis critiques qui doivent appeler chacun de nous, entreprises, institutions, décideurs, à **anticiper davantage**, à **investir intelligemment** et à **co-construire une culture numérique plus robuste, plus résiliente et plus souveraine**.

Car la cybersécurité n'est pas uniquement une affaire de technologies ou de conformité, elle est d'abord une affaire de leadership, de vision et de collaboration. Elle requiert que nous intégrions la sécurité au cœur de chaque stratégie de croissance, au même titre que l'innovation et la durabilité.

Comme le rappelait si justement **Warren Buffett** :

***"Il faut 20 ans pour bâtir une réputation et cinq minutes pour la ruiner. Si vous y pensez, vous agirez différemment"***

L'heure est venue de passer d'une posture défensive à une dynamique proactive. De faire du risque cyber un levier de performance durable et un marqueur de confiance dans notre économie numérique. De bâtir ensemble, au Maroc et avec l'Afrique, des écosystèmes où la confiance numérique est un facteur d'inclusion, de prospérité et de souveraineté.

Ensemble, continuons à agir, à innover et à renforcer notre cybersécurité pour faire du digital une véritable promesse d'avenir pour nos entreprises, pour nos citoyens et pour notre Nation.

**Merci à toutes les organisations qui se sont engagées dans cette démarche collective en participant à l'Ausimètre 2025. Merci aux équipes de notre partenaire PwC et aux équipes de l'AUSIM pour leur engagement rigoureux. Ensemble, poursuivons cet élan vers un Maroc numérique plus sûr, plus résilient et plus souverain.**

# Cybersécurité au Maroc : anticiper les menaces, optimiser les stratégies et intégrer les innovations pour une défense renforcée

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

Dans un monde où la numérisation est omniprésente, la cybersécurité est devenue un enjeu majeur pour les entreprises et les organisations. Ce livre blanc se propose d'explorer les défis actuels et futurs de la cybersécurité dans ce contexte, en mettant en lumière les stratégies et les technologies émergentes pour y faire face.

Tout d'abord, l'évolution et la quantification des risques cyber sont essentielles pour comprendre l'ampleur des menaces et prendre des décisions éclairées. Les cybermenaces ne cessent de se complexifier, avec des attaques de plus en plus sophistiquées et variées grâce et à cause de l'intelligence artificielle (IA).

La quantification des risques cyber permet d'exprimer ces menaces en termes financiers et stratégiques, facilitant ainsi la planification et l'allocation des ressources nécessaires pour y faire face.

Ensuite, le niveau et les stratégies cyber des entreprises marocaines sont évalués pour comprendre leur maturité en cybersécurité et leur capacité à atteindre leurs objectifs stratégiques. Cela implique d'analyser leur positionnement dans divers domaines de la sécurité informatique et d'identifier les secteurs nécessitant des améliorations.

Les stratégies mises en place doivent être adaptées aux défis actuels et futurs, en intégrant des technologies innovantes pour renforcer la sécurité, telles que le cloud et l'intelligence artificielle générative.

L'intelligence artificielle et le cloud sont des technologies émergentes essentielles pour améliorer la détection et l'anticipation des menaces cyber, tout en offrant des solutions flexibles pour la protection des données. Parallèlement, le cloud offre une évolutivité et une flexibilité cruciales pour protéger les données critiques.

Cependant, le capital humain est souvent considéré comme le maillon faible de la chaîne de sécurité, car les erreurs humaines sont impliquées dans la majorité des incidents cyber. Pour transformer cette vulnérabilité en force, un leadership engagé doit mettre en place des stratégies proactives, incluant des formations régulières, des simulations d'attaques et une culture de vigilance partagée.

En valorisant les compétences et en instaurant une responsabilisation collective, les organisations peuvent renforcer la résilience de leur personnel, le transformant ainsi en première ligne de défense efficace contre les cybermenaces, alignée avec les impératifs de la Stratégie Nationale de Cybersécurité marocaine.

Enfin, les priorités d'investissement en cybersécurité doivent être alignées avec les objectifs stratégiques des entreprises. Cela inclut l'allocation efficace des ressources pour les technologies et les formations nécessaires à la protection des actifs numériques. Les évolutions réglementaires en matière de cybersécurité influencent également la capacité des organisations à gérer les risques et assurer leur croissance future. Comprendre ces évolutions est essentiel pour se conformer aux normes et maintenir une position compétitive sur le marché.

En conclusion, ce livre blanc vise à offrir une vision complète des défis et des opportunités en cybersécurité au Maroc. En explorant ces différents aspects, nous espérons fournir aux entreprises et aux décideurs les outils nécessaires pour naviguer dans ce paysage en constante évolution et renforcer leur résilience face aux cybermenaces.

# Réinventer l’avenir : l’innovation technologique et la cybersécurité comme piliers de la résilience des entreprises

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

Dans un monde où les défis technologiques, géopolitiques, sociétaux et environnementaux façonnent l’avenir des entreprises, il est impératif que les dirigeants adoptent une approche stratégique intégrant à la fois l’innovation et la résilience numérique.

La 28e Global CEO Survey de PwC met en évidence que l'adoption de technologies émergentes, telles que la GenAI, est essentielle pour réinventer les modèles d’affaires et assurer la compétitivité à long terme.

L’enquête mondiale Digital Trust Insight 2025 de PwC révèle quant à elle un mouvement d'évolution des priorités en cybersécurité. L’IA générative et les technologies émergentes amplifient les risques cyber, obligeant les entreprises à repenser leurs stratégies de défense. 67% des responsables de la sécurité constatent une expansion de leur surface d’attaque due à la GenAI, et 78% ont accru leurs investissements pour atténuer ces nouveaux risques. Par ailleurs, les préoccupations en cybersécurité varient selon les perspectives des décideurs : 48% des chefs d’entreprise considèrent les cybermenaces comme une priorité stratégique, contre 66% des leaders technologiques, mettant en lumière un besoin d’alignement entre vision business et impératifs sécuritaires.

Les résultats combinés de ces deux enquêtes soulignent une vérité incontestable : dans un monde interconnecté et en constante évolution, la réinvention des modèles d’affaires doit aller de pair avec un renforcement de la résilience numérique. Les dirigeants, en particulier dans les secteurs à forte transformation, doivent traiter la cybersécurité non pas comme un sujet périphérique mais comme un pilier central de leur stratégie de croissance et de durabilité. Seuls ceux qui sauront allier innovation technologique et sécurité numérique pourront espérer prospérer dans les années à venir.

Ces tendances mondiales font écho aux enjeux particuliers du Maroc, où la digitalisation croissante et les exigences réglementaires imposent une gouvernance cyber robuste et une résilience accrue face aux menaces émergentes. Les derniers événements cyber observés sur le marché marocain l'ont démontré. A ce titre, disposer de dispositifs de gestion de crise et de plans de réponse à ces événements constitue un enjeu crucial afin d'être en capacité de répondre à une crise sur toutes ses dimensions de communication, de traitement des enjeux juridiques, légaux, réglementaires et techniques. La mise en œuvre d'une telle capacité présuppose un leadership fort, une approche holistique, un engagement de l'ensemble de l'organisation et des approches de collaborations / partenariats stratégiques.

Dans ce contexte, la collaboration entre entreprises et experts en cybersécurité devient non seulement nécessaire mais stratégique. Ce livre blanc, rédigé en collaboration avec l’AUSIM, vise à offrir un état de la de l'art de la cybersécurité sur le marché marocain et à dresser les tendances de fonds à projeter sur les prochaines années.

# Une deuxième édition pour décrypter l'évolution des pratiques cyber

Fort de son succès lors de sa première édition, l'enquête « Ausimètre de la Cybersécurité au Maroc » revient pour une deuxième édition afin de continuer à explorer les dynamiques de la cybersécurité au Maroc.

En partenariat avec l'AUSIM, PwC a mené une nouvelle enquête approfondie visant à évaluer la posture de cybersécurité des entreprises marocaines dans un contexte marqué par l'évolution constante des menaces et des technologies.

**Un périmètre d'étude ciblé sur les défis stratégiques et opérationnels de la cybersécurité :**

Cette étude, menée du 4 décembre 2024 au 17 février 2025, se concentre sur les réflexions stratégiques des entreprises, leur maturité organisationnelle et leur capacité à adopter des technologies innovantes telles que l'intelligence artificielle. Elle explore également le rôle du leadership et de la culture d'entreprise dans la gestion des risques cyber ainsi que les priorités d'investissement et les implications des évolutions réglementaires.

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

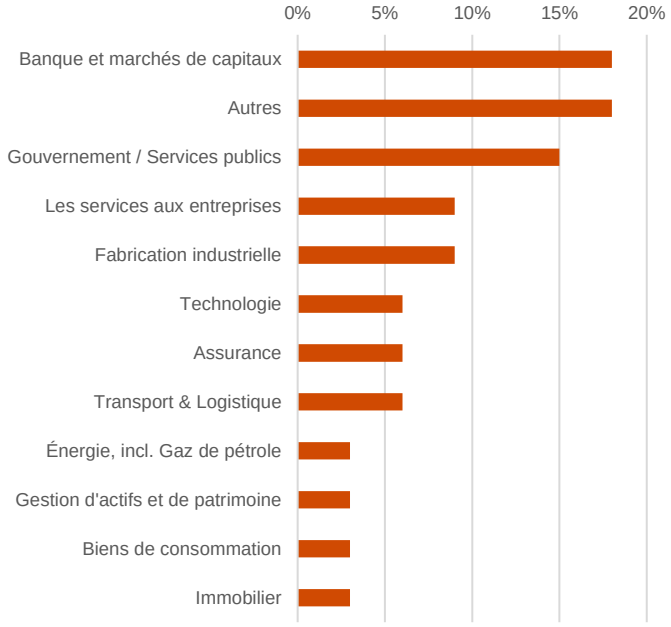
Nous vous invitons à découvrir les résultats captivants de cette étude, qui promettent d'enrichir la réflexion sur les meilleures pratiques et les prochaines étapes pour renforcer la sécurité numérique au sein des entreprises au Maroc.

## Un panorama sectoriel et des profils variés au cœur des décisions cyber

L'enquête AUSIMETRE 2025 reflète un échantillon représentatif et diversifié du paysage économique marocain, permettant d'analyser l'approche cyber des organisations en fonction de leur taille, leur secteur d'activité et leur structure de gouvernance.

### 1. Répartition sectorielle des répondants

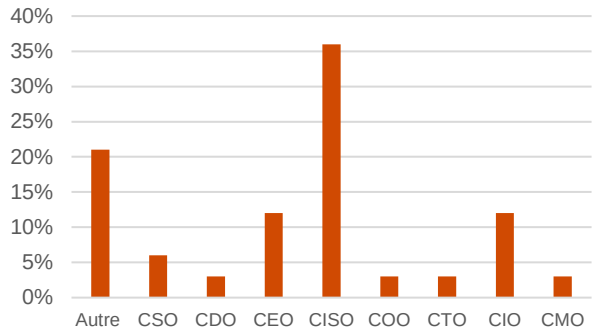
L'échantillon couvre un large éventail de secteurs, allant des industries manufacturières aux services financiers, en passant par les secteurs de technologie, de commerce et des institutions publiques. Cette diversité sectorielle permet de mieux comprendre les besoins spécifiques et d'identifier les tendances globales influençant les pratiques de sécurité numérique. En outre, des répondants provenant d'autres secteurs d'activité tels que le crédit à la consommation et le leasing, l'éducation/enseignement supérieur, ainsi que la recherche scientifique, viennent compléter cette diversité sectorielle.




G.01 : Répartition sectorielle des répondants

## 2. Répartition des fonctions des répondants

L'enquête a également recueilli les avis d'acteurs clés occupant des rôles stratégiques en cybersécurité au sein de leurs organisations :

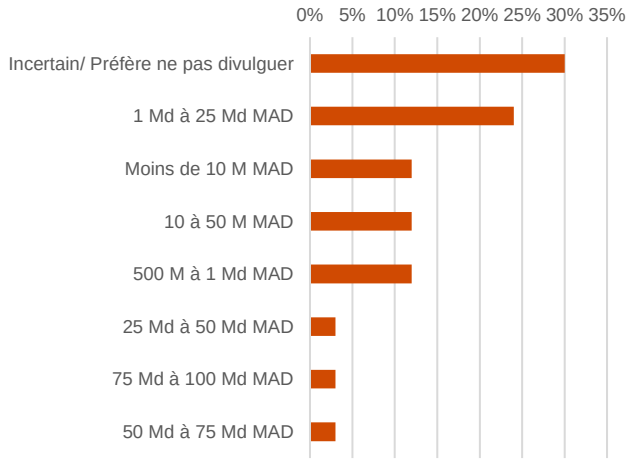



G.02 : Fonctions des répondants

Cette répartition permet d'avoir une vision globale et équilibrée sur les approches stratégiques et les défis opérationnels auxquels font face les entreprises marocaines.

## 3. Répartition des entreprises selon leur chiffre d'affaires

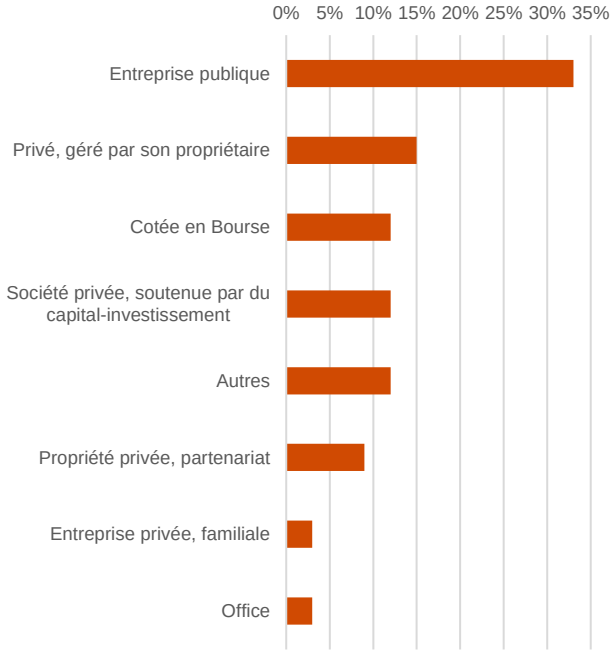
Les entreprises interrogées couvrent une large gamme de tailles et de chiffres d'affaires, ce qui permet d'analyser comment la cybersécurité est perçue et mise en œuvre en fonction des ressources disponibles.




G.03 Répartition des organisations selon leur chiffre d'affaires

## 4. Répartition selon le statut juridique

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




G.04 : Statut juridique des entreprises des répondants

# Principaux enseignements de l'enquête

## La digitalisation des entreprises marocaines : accélération et défis cyber

La transformation numérique des entreprises marocaines s'accélère, portée par l'adoption croissante des nouvelles technologies comme le Cloud, l'intelligence artificielle et l'IoT. Ce mouvement est soutenu par des initiatives nationales comme la Stratégie Maroc Digital 2030, qui vise à renforcer l'innovation et la compétitivité du pays à travers la digitalisation des services publics et privés.

Toutefois, cette digitalisation rapide expose les entreprises à des cybermenaces accrues. L'intégration de solutions cloud et la migration vers des infrastructures numériques élargissent considérablement la surface d'attaque et nécessitent un renforcement des dispositifs de cybersécurité. En effet, 30% des répondants estiment que le Cloud a légèrement augmenté la surface d'attaque cyber dans leurs environnements informatiques au cours des 12 derniers mois, tandis que 33% attribuent cet élargissement à l'IA.

## Faire face aux menaces cyber : pourquoi adapter la gestion des risques aux défis émergents ?

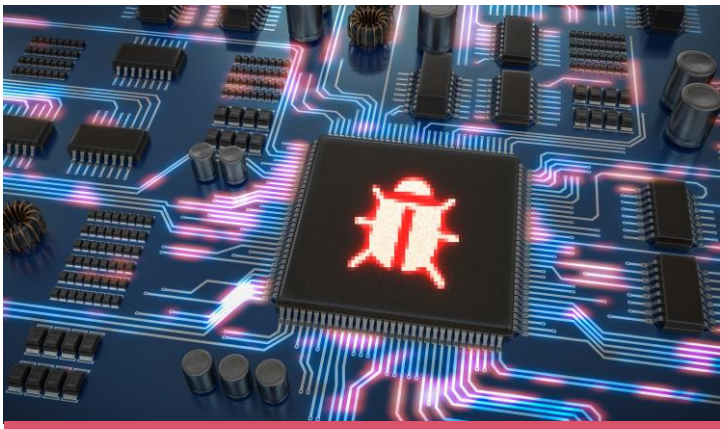
Les cybermenaces deviennent de plus en plus alimentées par l'essor des technologies émergentes telles que l'intelligence artificielle générative (GenAI), le cloud computing, l'IoT et la blockchain. Si ces innovations offrent des opportunités stratégiques considérables, elles élargissent également la surface d'attaque des entreprises et complexifient leur gestion des risques.

Les entreprises marocaines doivent ainsi adapter leur approche de gestion des risques en tenant compte des nouveaux vecteurs de menaces. La capacité des cybercriminels à exploiter l'IA pour automatiser les attaques (hameçonnage ultra-ciblé, deepfakes malveillants, génération de malwares avancés) impose un renforcement des systèmes de détection et de réponse.

## L'adaptation des stratégies de cybersécurité aux nouvelles menaces

L'évolution des cyberattaques exige une transformation des stratégies de défense des entreprises. L'approche traditionnelle de gestion des risques, souvent basée sur des analyses statiques et réactives, doit être remplacée par une approche dynamique, prédictive et automatisée.

Aussi, face à ces défis émergents, le leadership en cybersécurité devient également un levier stratégique incontournable. La sécurité ne peut plus être un enjeu technique isolé ; elle doit être intégrée dans la gouvernance globale des entreprises et alignée avec les objectifs stratégiques.



- Les dirigeants doivent s'impliquer directement dans la stratégie cyber et promouvoir une culture de sécurité à tous les niveaux de l'organisation.
- Les investissements en cybersécurité doivent être ajustés pour prioriser les technologies avancées (IA, SOC, Zero Trust) et le renforcement des compétences internes via la formation continue.
- La gestion des cyber-risques ne peut plus être statique : elle doit s'adapter aux tendances émergentes, s'appuyer sur l'analyse prédictive et intégrer une supervision en temps réel des menaces.

## Vers une approche réglementaire structurée pour encadrer la cybersécurité

Alors que la digitalisation s'accélère et que les cybermenaces se complexifient, les entreprises marocaines doivent non seulement adapter leurs stratégies technologiques et organisationnelles, mais aussi assurer une conformité rigoureuse aux cadres réglementaires nationaux et internationaux.

La montée en puissance des attaques ciblées, l'essor des technologies émergentes et l'expansion des environnements cloud exigent un cadre de gouvernance robuste pour garantir la résilience numérique et la protection des infrastructures critiques.

Dans ce contexte, les régulateurs marocains ont mis en place un cadre législatif en constante évolution visant à structurer les pratiques cyber et à garantir un niveau de sécurité optimal pour les organisations opérant sur le territoire.

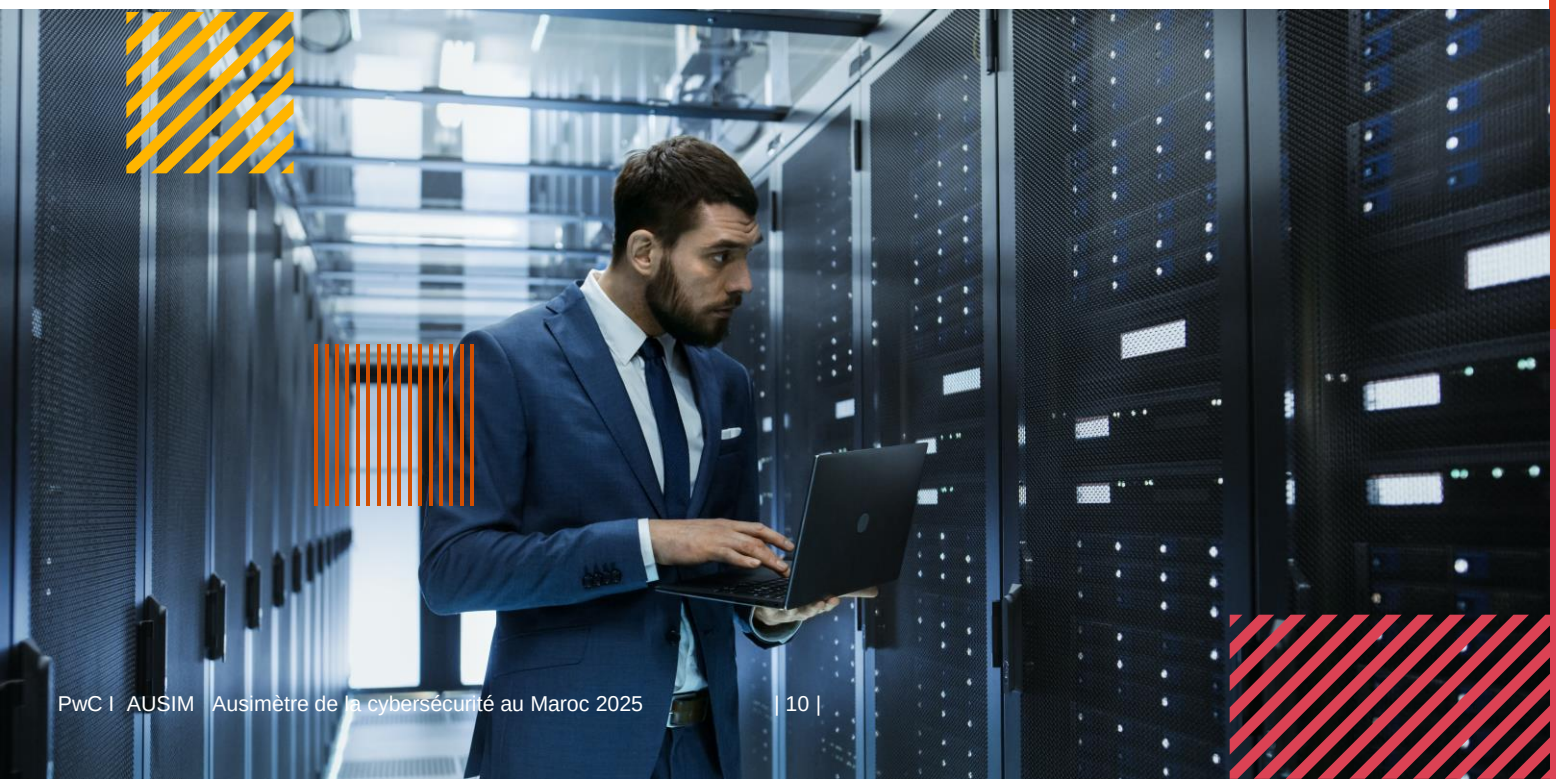
L'introduction de la Loi 05-20 sur la cybersécurité, les directives de la DNSSI (Directive Nationale de la Sécurité des Systèmes d'Information) et l'alignement progressif avec les standards internationaux (ISO 27001, RGPD, NIS2) témoignent d'une volonté d'encadrer les pratiques et d'accompagner les entreprises vers une approche proactive en matière de cybersécurité.

En effet, 61% des répondants déclarent avoir recours à la norme ISO 27001 pour évaluer et structurer leurs capacités en cybersécurité, soulignant ainsi l'importance croissante des cadres de référence internationaux.

## Recommandations pour une approche proactive de la conformité

Dans ce contexte en constante évolution, les entreprises marocaines doivent adopter une posture proactive en matière de cybersécurité et de conformité réglementaire. Voici les recommandations essentielles pour anticiper ces évolutions :

- Mettre en place une gouvernance cybersécurité alignée avec les exigences réglementaires : Structurer une stratégie de gestion des risques claire et documentée pour répondre aux obligations de la Loi 05-20 et des directives de la DNSSI.
- Investir dans des audits réguliers et des certifications : Adopter des frameworks comme ISO 27001 ou CIS Controls permet d'améliorer la maturité cyber et d'assurer une conformité continue. 18% des répondants indiquent que les évolutions réglementaires ont renforcé leurs investissements en cybersécurité au cours des 12 derniers mois, démontrant un impact direct des nouvelles exigences sur les stratégies d'entreprise.
- Anticiper l'impact des nouvelles réglementations : Suivre de près les évolutions législatives, notamment les nouvelles obligations prévues pour 2025, afin d'adapter rapidement les pratiques internes.
- Renforcer la sensibilisation et la formation des équipes : La conformité ne doit pas être perçue comme une contrainte technique mais comme une culture à instaurer au sein des organisations.

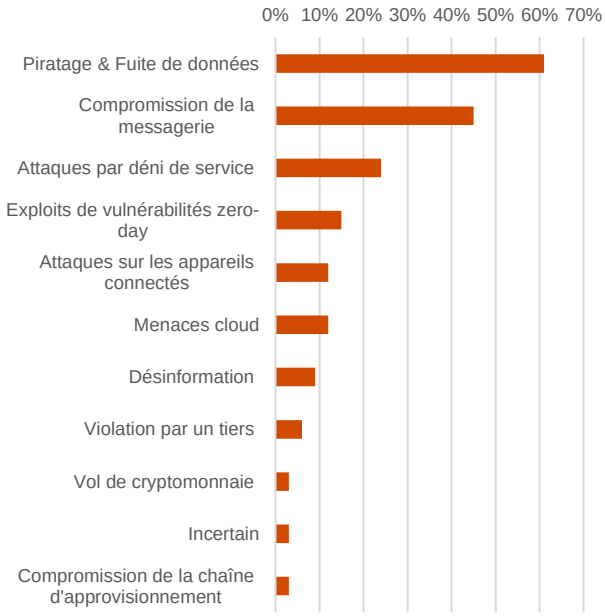


# Analyse détaillée des réponses de l'enquête

## Les entreprises marocaines donnent la priorité à l'atténuation des risques cyber, numériques et technologiques.

### Des risques globaux, mais les risques cyber restent la priorité numéro un des entreprises

**73%** des entreprises marocaines mettent les risques cyber en tête de leurs priorités pour les 12 prochains mois, face à un éventail de risques allant des bouleversements macroéconomiques aux crises environnementales.




G.05 : Principales menaces cyber identifiées par les différents répondants de l'enquête

L'analyse des résultats révèle une continuité dans les priorités des entreprises marocaines, avec les risques cyber confirmés comme leur principal enjeu. Cependant, en comparaison avec l'année dernière :

- La proportion d'entreprises mettant les risques cyber en priorité a diminué de 17%.
- Dans le même élan, les préoccupations liées aux risques macroéconomiques et environnementaux ont légèrement diminué, passant respectivement de 40% à 33%, suggérant une redirection des efforts vers des enjeux technologiques plus immédiats.

Ce maintien de cette orientation vers les enjeux cyber s'explique par une prise de conscience accrue des menaces spécifiques. Parmi ces menaces, le piratage et la fuite de données émergent comme des préoccupations majeures.

### Défis de quantification des risques cyber

La quantification de l'impact financier des risques cyber reste un défi stratégique majeur. Les organisations signalent des obstacles qui ralentissent leur capacité à évaluer les pertes potentielles et à planifier leurs investissements en cybersécurité.

**45 %** des organisations mentionnent le manque de clarté sur l'étendue de l'impact des risques comme un obstacle majeur.

**12 %** seulement des organisations considèrent la complexité des outils comme un obstacle majeur.

# Niveau de préparation des entreprises marocaines face aux cybermenaces et aux enjeux de sécurité

Les entreprises marocaines évaluent leur maturité cyber selon une échelle progressive – du niveau initial au niveau optimisé, en passant par les niveaux développé et standardisé. L'analyse met en évidence des écarts entre les domaines, soulignant où les efforts doivent être renforcés pour atteindre une maturité optimale.

### Anticipation des risques

**40%** des répondants déclarent avoir un niveau standardisé en matière de gestion des risques cyber.

### Réaction rapide aux menaces cyber

Seuls **6%** des entreprises se situent au niveau initial, indiquant que la majorité des organisations disposent d'une capacité de réponse structurée.

### Gestion budgétaire et alignement stratégique

**33%** des répondants se situent encore au niveau initial, montrant que l'investissement en cybersécurité reste sous-évalué par de nombreuses entreprises.

### Relations avec les régulateurs et gouvernance externe

**60%** des répondants déclarent un niveau entre développé et standardisé, traduisant une volonté de conformité et de structuration des relations avec les autorités.

**Messages clés**

Renforcer les investissements, structurer la réponse aux menaces et optimiser la gestion des relations institutionnelles pour une cybersécurité plus robuste et alignée avec les risques actuels.

## S'appuyer sur des cadres reconnus pour structurer et professionnaliser les pratiques

Pour structurer leurs approches en cybersécurité, les entreprises marocaines adoptent de plus en plus des cadres et outils reconnus à l'échelle internationale.

**Top cadres adoptés :**

- La norme **ISO 27001** est utilisée par **61%** des entreprises, contre 96% l'année précédente.
- **NIST Cybersecurity Framework** gagne en popularité, adopté par **27 %** des répondants.
- Les cadres **sectoriels spécifiques** sont également cités par **3% des répondants**.

## Le Zéro Trust au cœur des priorités pour renforcer la résilience

La stratégie Zéro Trust est désormais au cœur des priorités des entreprises marocaines pour limiter les accès non autorisés et renforcer leur sécurité. Les organisations se concentrent sur des piliers comme :

- **La sensibilisation :** Une priorité pour **52%** des répondants

La sensibilisation des employés aux risques de sécurité est un enjeu clé pour les entreprises. En effet, **52%** des répondants estiment que former et informer les collaborateurs sur les bonnes pratiques en matière de sécurité informatique est essentiel pour limiter les risques liés aux erreurs humaines, telles que l'ouverture de courriels de phishing ou la gestion imprudente des mots de passe.

- **La gestion des identités et des accès (IAM) :** Une priorité pour **39%** des répondants

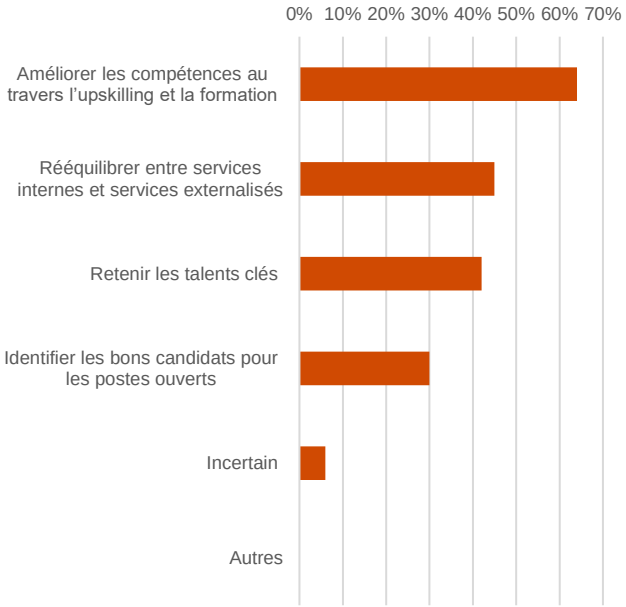
La gestion des identités et des accès est cruciale pour garantir que seules les personnes autorisées peuvent accéder aux ressources sensibles de l'entreprise. 39% des répondants soulignent l'importance de la mise en place des outils IAM efficaces pour assurer une gestion rigoureuse des permissions et prévenir les accès non autorisés, contribuant ainsi à la sécurité globale des infrastructures.

- **La gouvernance :** Une priorité pour **36%** des répondants

La gouvernance de la sécurité passe par l'établissement de politiques claires et de stratégies adaptées pour encadrer les pratiques de sécurité au sein de l'entreprise. 36% des entreprises jugent ce point essentiel pour garantir une gestion cohérente des risques et une réponse adéquate aux incidents. Une gouvernance bien définie permet d'assurer la conformité aux normes et de structurer la gestion des ressources et des informations critiques.

# Optimiser les compétences internes : stratégies d'upskilling et de formation continue

**La majorité des entreprises privilégient une stratégie de développement de talents cyber basée sur l'amélioration des compétences au travers l'upskilling et la formation.**




G.06 : Talents Cyber : Former, attirer et renforcer

La majorité des entreprises adoptent une stratégie de développement des talents dans le domaine de la cybersécurité en mettant l'accent sur l'amélioration continue des compétences internes, via des initiatives telles que l'upskilling et la formation.

Ces démarches permettent aux employés de renforcer leurs connaissances et de s'adapter aux évolutions rapides des menaces et des technologies. Voici quelques éléments clés de cette stratégie.

## Upskilling

L'upskilling consiste à permettre aux employés déjà en poste de développer des compétences supplémentaires ou de se perfectionner dans de nouveaux domaines de la cybersécurité. Cette approche est cruciale dans un secteur en constante évolution, où de nouvelles vulnérabilités et attaques apparaissent régulièrement. En offrant des formations avancées ou spécialisées, les entreprises peuvent adapter les talents existants aux exigences spécifiques de la cybersécurité, sans devoir chercher à recruter de nouveaux profils spécialisés. Cette stratégie permet également de fidéliser les talents et de les encourager à rester dans l'entreprise en offrant des opportunités de croissance professionnelle.

## Formation continue

Les entreprises investissent également dans des programmes de formation continue pour garantir que leurs équipes restent à jour face aux dernières tendances et défis de la cybersécurité.

Ces formations peuvent être dispensées en interne, à travers des ateliers et des séminaires, ou bien en externe via des certifications reconnues telles que celles proposées par des organismes comme CompTIA, CISSP ou COFRAC.

# Vers une cybersécurité externalisée : un virage stratégique pour les entreprises marocaines ?

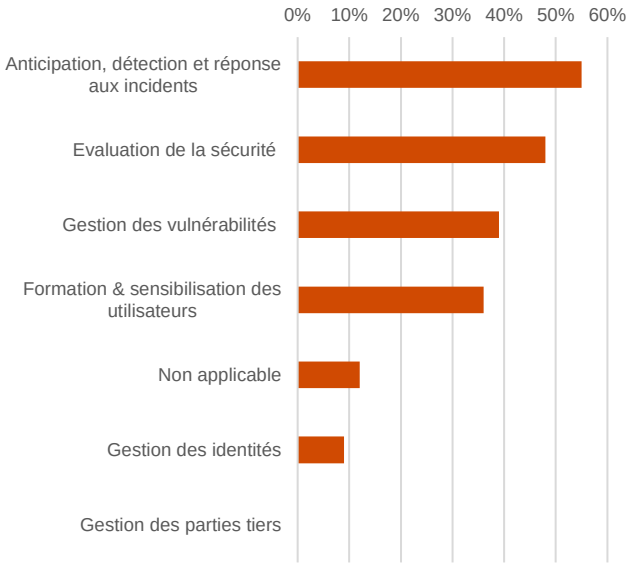
L'évolution rapide des menaces cyber et le manque de talents en cybersécurité poussent de plus en plus d'entreprises à revoir leur modèle opérationnel. Si certaines choisissent de renforcer leurs équipes internes, d'autres privilégient l'externalisation de certaines fonctions clés via des services managés.

L'externalisation permet d'accéder à une expertise de pointe, d'améliorer la surveillance et la réactivité face aux attaques, et de réduire les coûts opérationnels.

**64%** Des entreprises marocaines déclarent externaliser totalement ou partiellement leurs services de cybersécurité, révélant une adoption croissante des services managés.

## Quels services de cybersécurité sont externalisés ?

Les entreprises marocaines externalisent en priorité les services techniques nécessitant une expertise avancée et une surveillance continue.




G.07 : Utilisations principales des services managés

## Ce que cela signifie :

### Anticipation, détection et réponse aux incidents (Top 1 des services externalisés)

- Les entreprises cherchent à renforcer leur capacité de cybersurveillance 24/7, avec une réactivité accrue en cas de cyberattaque.
- L'externalisation permet d'accéder à des équipes spécialisées en SOC (Security Operations Center), souvent trop coûteuses à internaliser.

### Évaluation de la sécurité (Top 2 des services managés)

- La réalisation d'audits réguliers et de tests d'intrusion est essentielle pour garantir une protection efficace.
- L'externalisation répond à un besoin d'indépendance et de certification pour garantir la conformité avec les normes de cybersécurité (ISO 27001, NIST, etc.).

### Gestion des vulnérabilités (Top 3 des services managés)

- La gestion des vulnérabilités demande une mise à jour continue des bases de données de menaces, ce qui justifie l'externalisation à des experts en cybersécurité.
- Les entreprises cherchent à utiliser des outils spécialisés et automatisés pour détecter et corriger les failles plus rapidement.

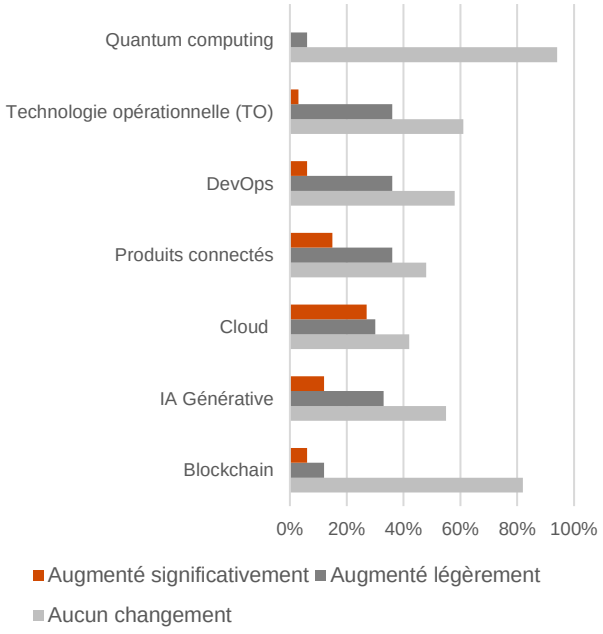
L'externalisation est devenue une réponse stratégique aux défis cyber, mais les entreprises doivent s'assurer d'un équilibre entre dépendance aux services managés et maîtrise interne des risques.

# Les défis des technologies émergentes avec un focus éventuel sur l'IA

## Une surface d'attaque en pleine expansion : quelles menaces à anticiper ?

L'intégration de nouvelles technologies comme l'IA, le Cloud et la Blockchain dans les infrastructures IT entraîne une augmentation significative de la surface d'attaque des entreprises.

Par ailleurs, les entreprises doivent repenser leur architecture cyber en intégrant une approche de sécurité dynamique, capable de s'adapter aux menaces en constante évolution.




G.10 : Influence des technologies émergentes sur la surface d'attaque

En particulier, l'adoption de l'Intelligence Artificielle soulève plusieurs défis opérationnels et stratégiques.

Les répondants ont identifié trois principaux freins à l'intégration efficace de l'IA en cybersécurité :

### Absence de politiques internes standardisées régissant son utilisation

**42%** des entreprises signalent une absence de politiques internes liés à l'IA générative en vue de contrôler son utilisation de manière adéquate.

### Manque de ressources de formation pour les employés

**42%** des organisations expriment un manque de ressources de formation relatives à l'IA générative pour leurs collaborateurs.

### Utilisation abusive non supervisée et potentiellement risquée de la technologie GenAI

**36%** des répondants déclarent une utilisation délibérée de la GenAI par leurs employés, ce qui pose un véritable défi pour ces organisations.

Ces préoccupations ne sont pas isolées. À l'échelle internationale, l'enquête « **Global CEO PwC** » dans sa 28ème édition met en lumière une adoption mesurée de l'IA générative. Si seuls 33% des chefs d'entreprise expriment une grande confiance dans son intégration aux processus critiques, un autre tiers affiche une confiance modérée. Ce constat suggère que, bien que des incertitudes persistent, une majorité des dirigeants reconnaît le potentiel de l'IA générative, tout en adoptant une approche prudente et progressive, un phénomène également observé au Maroc.

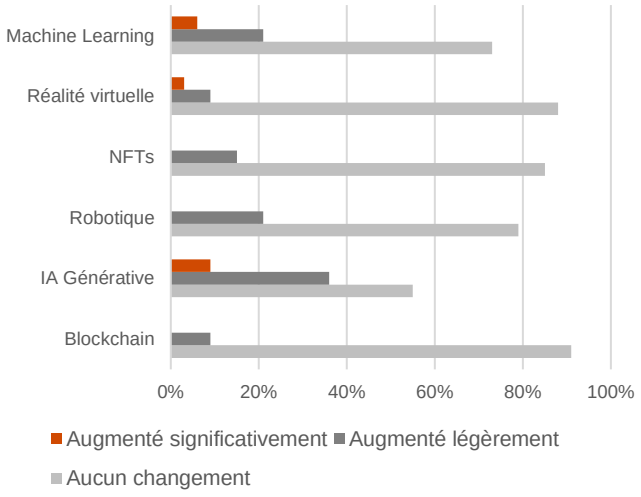
Un cadre de gouvernance et des politiques de cybersécurité adaptées sont essentiels pour maximiser le potentiel de l'IA, tout en contrôlant ses risques.

# Les opportunités offertes par les technologies émergentes en cybersécurité, avec un accent particulier sur l'IA

## Investissements en cybersécurité : Les entreprises marocaines sont-elles prêtes pour les technologies émergentes ?

L'évolution technologique s'accélère, et avec elle, de nouvelles menaces émergent. L'IA Générative, la blockchain, la robotique, le cloud, le machine learning et la réalité virtuelle s'imposent progressivement dans l'écosystème numérique des entreprises marocaines. Mais ces dernières ont-elles adapté leur investissement en cybersécurité pour recueillir ces technologies ?

Les résultats de l'enquête révèlent une approche encore prudente vis-à-vis de ces nouvelles technologies. Seul un faible pourcentage des entreprises a augmenté significativement ses investissements en cybersécurité pour l'adoption des technologies émergentes.




G.08 : Investissement dans les technologies émergentes au cours des 12 derniers mois

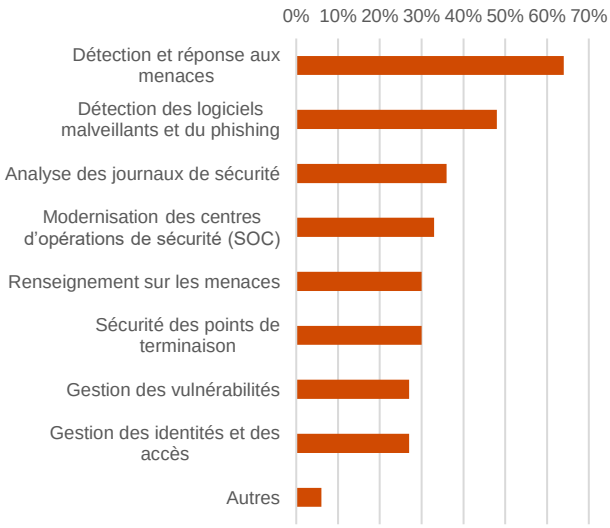
Ce constat montre un besoin urgent d'aligner les budgets cybersécurité sur la transformation numérique en cours.

## L'IA générative en cybersécurité : entre opportunité et nouveaux usages

L'essor des technologies émergentes telles que l'IA générative, le cloud, la blockchain et le Quantum Computing transforme profondément les stratégies de cybersécurité des entreprises.

l'IA générative se positionne comme un outil clé pour renforcer les stratégies de défense en cybersécurité.

L'enquête révèle les domaines spécifiques où les organisations marocaines prévoient de prioriser son utilisation au cours des 12 prochains mois, notamment pour améliorer la détection des menaces, la détection des logiciels malveillants et du phishing et également l'analyse des journaux de sécurité.




G.09 : Principaux aspects relatifs à l'utilisation de l'IA générative pendant les 12 prochains mois

L'IA générative est perçue comme un levier d'efficacité et de compétitivité. Selon l'enquête **« Global CEO PwC »** dans sa 28ème édition**,** 46% des dirigeants mondiaux s'attendent à une augmentation de la rentabilité grâce à la GenAI dans les 12 prochains mois.

# Le Cloud, un pilier de la transformation numérique au Maroc

L'adoption du cloud s'inscrit dans une dynamique stratégique portée par la vision Maroc Digital 2030, qui vise à accélérer la digitalisation des entreprises et des services publics.

Cette transition vers le cloud favorise une plus grande agilité opérationnelle, optimise les coûts IT et renforce la compétitivité des entreprises marocaines sur la scène internationale.

Cependant, cette migration massive vers le cloud s'accompagne de défis majeurs en cybersécurité, souvent sous-estimés par les organisations.

## Une adoption massive, mais une sécurité encore fragile…

Selon l'enquête mondiale « Digital Trust Insight 2025 de PwC », 34% des leaders technologiques identifient la sécurité du cloud comme l'investissement prioritaire en cybersécurité dans les 12 prochains mois.

En revanche, 42% des dirigeants mondiaux considèrent les menaces liées au cloud comme leur principale préoccupation cyber.

Cette prise de conscience croissante souligne une réalité incontournable : le cloud est devenu un terrain majeur d'attaques cyber.

## Les défis liés aux fournisseurs de services cloud

Si le cloud offre une flexibilité et une évolutivité, il introduit également une dépendance croissante aux fournisseurs de services cloud (CSP - Cloud Service Providers).

Cette relation, souvent perçue comme une solution simplifiée à la gestion des infrastructures IT, présente en réalité plusieurs défis majeurs.

Notre enquête révèle que de nombreuses organisations font face à des obstacles majeurs lorsqu'il s'agit des relations avec leurs fournisseurs Cloud.

Principaux défis identifiés :

- **Partage des responsabilités**
  Le modèle de responsabilité partagée entre le fournisseur cloud et l'entreprise est souvent mal interprété. Une mauvaise répartition des rôles peut engendrer des failles de sécurité et des risques de non-conformité, notamment sur la protection des données sensibles et la gestion des accès.
- **Capacité à reprendre en cas de sinistre**
  Une panne chez un fournisseur de cloud ou une violation de données peut avoir des conséquences majeures sur la continuité des activités. Pourtant, de nombreuses entreprises n'ont pas mis en place de plan de reprise efficace ni testé leur capacité à rétablir leurs systèmes en cas d'incident.
- **Négociation des contrats cloud**
  Les contrats standards proposés par les fournisseurs ne tiennent pas toujours compte des spécificités des entreprises, notamment en matière de cybersécurité et de conformité. L'absence de clauses claires sur la gestion des incidents, la résilience des infrastructures et la souveraineté des données peut poser des défis importants.

Adopter le cloud, ce n'est pas externaliser la responsabilité !
Les entreprises doivent renforcer leurs capacités internes en matière de gestion des fournisseurs, négocier des contrats plus adaptés à leurs exigences en cybersécurité et conformité, et développer des plans de résilience pour prévenir toute dépendance excessive à un seul prestataire.

# Le leadership face aux enjeux cyber : un levier stratégique essentiel

L'implication du Leadership est un levier essentiel pour renforcer la posture de cybersécurité des entreprises. Leur engagement permet non seulement d'améliorer la maturité cyber, mais aussi d'intégrer la sécurité dans les décisions stratégiques à long terme.

L'enquête révèle que les dirigeants marocains participent activement à plusieurs discussions stratégiques en matière de cybersécurité. Les trois principales actions menées sont :

**Discussion des implications cyber dans le cadre de la future stratégie**

**55%**

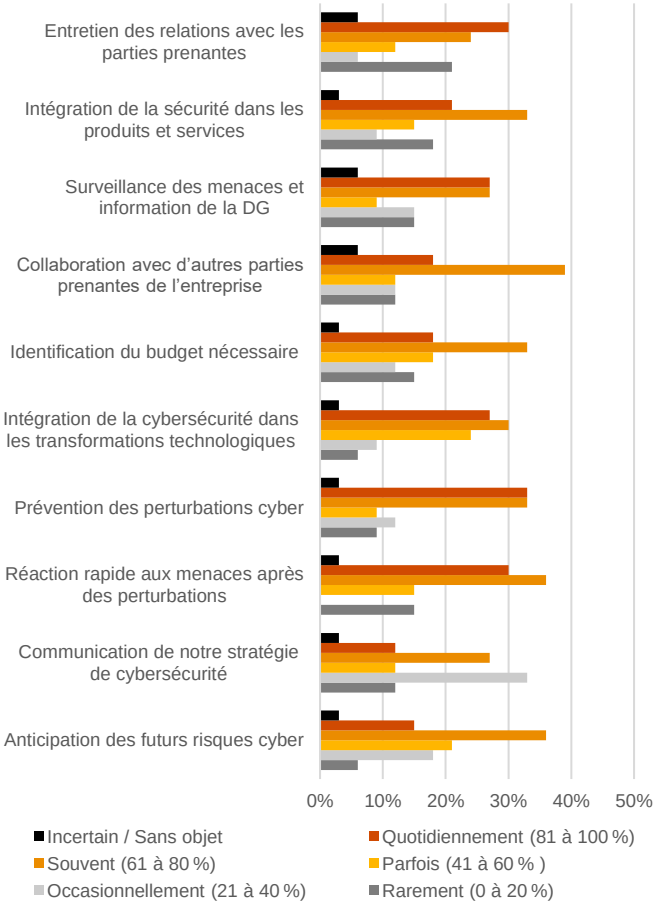
**Discussion des plans d'action après une attaque cyber majeure dans l'organisation**

**45%**

**Discussion des principaux indicateurs cyber au niveau du conseil d'administration**

**39%**

Plusieurs tendances se dégagent :




G.11 : Objectifs de cybersécurité atteints

La majorité des répondants ont indiqué que leur équipe cybersécurité atteint fréquemment ou quotidiennement les objectifs fixés dans plusieurs domaines clés.

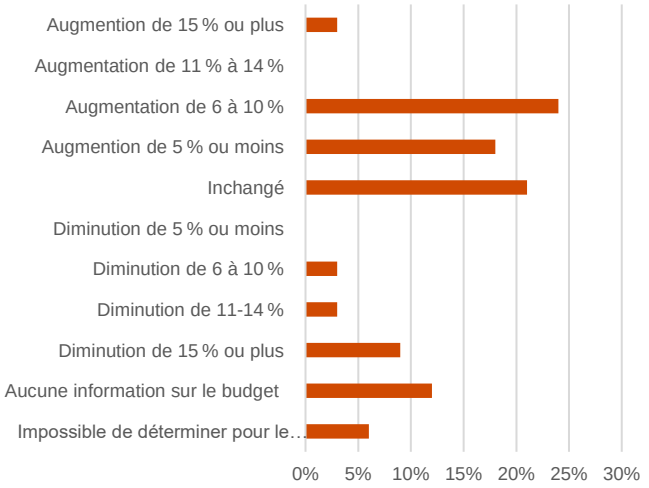
D'autres ont considéré que la mise en place de contrôles pour prévenir les perturbations cyber graves et l'intégration de la cybersécurité dans les transformations technologiques majeures ont également été des objectifs souvent atteints.

Les organisations semblent accorder une attention croissante à la surveillance des menaces et à l'information de la direction générale, tout en travaillant activement à l'identification et au suivi des budgets nécessaires pour traiter les risques cyber.

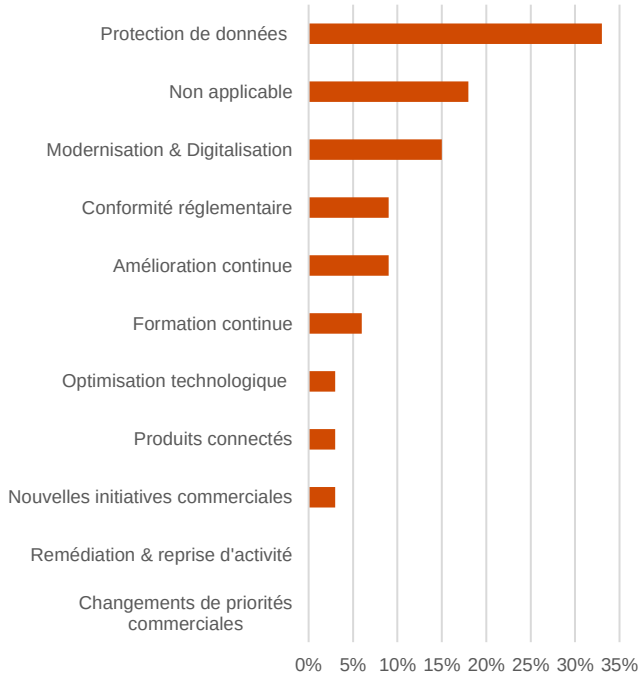
# L’accélération des investissements en cybersécurité : un impératif stratégique

## Des investissements en hausse face à une menace croissante

L’évolution rapide des cybermenaces et l’adoption massive des nouvelles technologies ont poussé les entreprises marocaines à revoir leurs stratégies de cybersécurité.




G.12 : L’évolution des investissements cyber en 2025




G.13 : Allocation du budget cyber pour les 12 prochains mois

## Comprendre les choix d’investissement en cybersécurité représente un enjeu stratégique

L’allocation des budgets en cybersécurité est un indicateur clé de la maturité des entreprises face aux cybermenaces.

Savoir où et comment les entreprises investissent permet de comprendre leurs priorités stratégiques, leurs vulnérabilités perçues et leur niveau de préparation face aux risques émergents.

## Une part importante des entreprises ne définit pas clairement ses investissements cyber

Un fait marquant ressort également de notre étude : la deuxième catégorie la plus représentée est celle des organisations déclarant un investissement "non applicable". Cette donnée soulève plusieurs questions :

- **Un manque de visibilité** sur les priorités cyber ? Certaines entreprises peinent encore à structurer une approche budgétaire claire en cybersécurité.
- **Une sous-estimation des risques** ? Le fait de ne pas allouer de budget spécifique peut refléter une perception atténuée des menaces.

**Alerte**

Investir efficacement en cybersécurité, ce n’est pas seulement protéger l’existant, c’est aussi anticiper les risques, garantir la conformité et renforcer la résilience de l’entreprise face aux menaces futures.

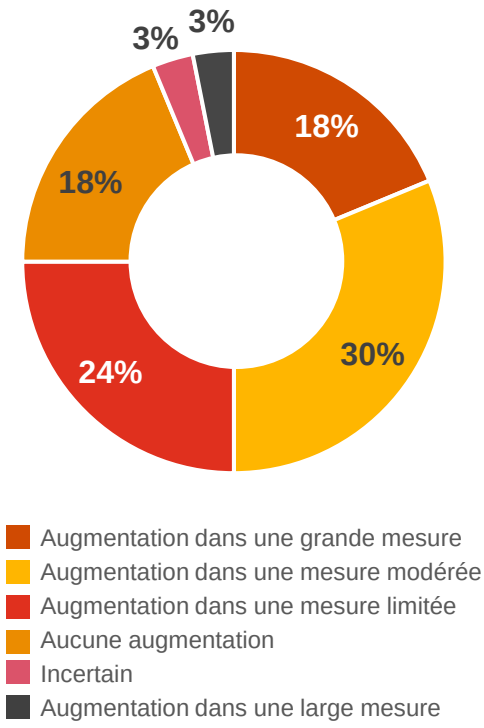
# Budgets stables et régulations respectées : moteurs complémentaires de la cybersécurité

## Les cadres réglementaires agissent comme un levier pour diriger les investissements vers des initiatives prioritaires

La mise en conformité avec des réglementations pousse les organisations à allouer davantage de ressources pour renforcer leur posture de sécurité et garantir leur résilience numérique.

Les résultats de notre enquête révèlent que l'impact des réglementations sur les investissements en cybersécurité varie considérablement d'une entreprise à l'autre. Cependant, une tendance générale se dégage, indiquant que la majorité des entreprises reconnaissent un impact direct des réglementations sur l'augmentation de leurs investissements cyber au cours des 12 derniers mois.

L'analyse des réponses met en évidence une répartition des impacts selon différents niveaux :




G.14 : Evolution des investissements réglementaires au cours des 12 derniers mois

Les exigences croissantes en matière de conformité représentent un défi de taille pour les organisations modernes, et influencent de plus en plus leurs stratégies d'investissement, notamment en matière de cybersécurité, de gestion des données et de gouvernance. À mesure que les réglementations évoluent et se multiplient, les entreprises sont contraintes d'adapter leurs processus et leurs infrastructures pour rester conformes aux normes locales et internationales.

L'introduction de la Loi 05-20 sur la cybersécurité, les directives de la DNSSI (Directive Nationale de la Sécurité des Systèmes d'Information) et l'alignement progressif avec des standards internationaux tels que l'ISO 27001 témoignent d'une volonté d'encadrer les pratiques et d'accompagner les entreprises vers une approche proactive en matière de cybersécurité. Les entreprises doivent ainsi investir non seulement dans des technologies de pointe pour se protéger contre les cybermenaces, mais aussi dans des systèmes permettant de collecter, de traiter et de stocker les données de manière conforme aux exigences légales et sécuritaires locales.

L'alignement des investissements sur les impératifs réglementaires est devenu crucial pour garantir non seulement la résilience organisationnelle, mais aussi la compétitivité sur le marché. En effet, une entreprise qui ne respecte pas les normes de conformité s'expose à des sanctions financières lourdes, à des poursuites judiciaires, ainsi qu'à une perte de confiance de ses clients et partenaires. À l'inverse, une organisation qui parvient à anticiper les exigences réglementaires et à investir dans des solutions de conformité de manière proactive peut se positionner comme un leader de confiance dans son secteur.

# Témoignages d’experts

## Question 1

*Face à une évolution constante des menaces cyber, telles que les rançongiciels et les violations de données, les entreprises marocaines sont confrontées à des attaques de plus en plus sophistiquées.*

*À votre avis, quelles stratégies les entreprises doivent-elles adopter pour anticiper et contrer efficacement ces menaces tout en préservant leurs opérations ?*

**M. KHALID OCHI**
Responsable de la sécurité du système d'information
Les Eaux Minérales d'Oulmès

Les entreprises marocaines ne sont pas en reste quant aux cybermenaces qui affectent les organisations à travers le monde, dont les rançongiciels et les violations de données.

Il est donc crucial d’adopter des stratégies de défense en profondeur qui s’articulent autour des axes clés :

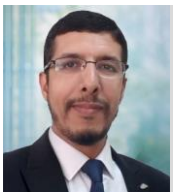
- **Gouvernance :** A travers une politique de sécurité solide adossée à l’engagement du top management, une gestion des risques efficace, une définition claire des rôles et responsabilités, et l’adoption de Frameworks de cybersécurité (ISO2700X, NIST CSF…).
- **Sensibilisation :** Il n’est pas plus imprudent que de laisser le personnel agir sans qu’il n’ait l’immunité nécessaire face aux menaces cyber. Un programme de sensibilisation adapté au profil et continu dans le temps n’est plus une option.
- **Durcissement :** Elément clé d’une gestion de configuration efficace, le périmètre du durcissement doit être élargi au-delà des actifs, systèmes et accès traditionnels à spectre plus large, notamment celui de l’OT des IOT et des systèmes intelligents.
- **Surveillance et réponse :** Garder un œil permanent sur les événements de sécurité, ne laisser aucun angle mort et réagir à temps. Le choix des outils (XDR, SIEM, SOAR…) est aussi important, et doit tenir en compte les spécificités de l’activité et les contraintes réglementaires.
- **Gestion des vulnérabilités :** Rester en veille des bulletins de sécurité, appliquer les correctifs à temps, réaliser des audits techniques réguliers et adopter une approche « secure by design ».
- **Résilience :** Une crise pourrait, malgré toutes les préparations, être inévitable. Il est nécessaire donc de s’y préparer, en mettant en place un dispositif de continuité d’activité robuste, régulièrement testé et actualisé.

**M. Abdessamad LIMY**
Responsable de sécurité de l’information et de continuité d’activité
Bourse de Casablanca

Face à l’évolution constante des menaces cyber et à la sophistication croissante des attaques, les entreprises marocaines se doivent de renforcer leur gouvernance en matière de cybersécurité et d’assurer leur conformité en s’alignant sur les standards internationaux et en respectant les réglementations locales et globales.

L’adoption de dispositifs techniques de protection, la sensibilisation des collaborateurs, le renforcement des capacités de détection et de réponse aux incidents, ainsi que l’évaluation régulière des risques doivent constituer les piliers essentiels de leur stratégie de sécurité et de résilience.

Désormais, la cybersécurité ne peut plus être envisagée de manière isolée, mais doit être abordée sous l’angle d’une défense collective. Il est impératif d’adopter une approche collaborative et solidaire : agir en meute. Ainsi, les entreprises marocaines sont appelées à structurer des communautés sectorielles afin de renforcer la cybersécurité de leur écosystème et d’ériger un rempart collectif contre les cybermenaces.



**M. Nabil CHIADMI**
RSSI
CMR

Face à l'évolution des menaces comme les ransomwares et les violations de données, les entreprises marocaines doivent adopter une approche proactive et pluridisciplinaire à travers deux axes principaux :

- Axe organisationnel par la mise en place d’un cadre de gouvernance de la sécurité SI basé sur des standards tel que ISO 27001 , NIST…etc. Il faut également mettre un focus important sur l’aspect humain, souvent le maillon faible de la chaine de valeur de la sécurité SI via des formations et sensibilisations régulières aux bonnes pratiques de la sécurité SI.
- Axe technique :

✓ Déploiement d'outils de détection avancés utilisant l'IA et le machine Learning pour identifier les anomalies en temps réel (XDR, SIEM nouvelle génération, anti DdoS, etc.).

✓ Implémentation d'outils de réponse automatisée (SOAR, EDR, NDR, etc.).

✓ Protection renforcée des sauvegardes, dernier recours lors d'une cyberattaque quand toutes les mesures précédentes ont échoué, en utilisant des méthodes comme 3-2-1 et également des solutions de sauvegarde anti Ransomware (air gap).

## Question 2

*Dans un contexte où les entreprises cherchent à optimiser leurs modèles opérationnels cyber pour allier simplicité, efficacité et maîtrise des coûts, les services managés continuent de gagner en popularité à l’échelle internationale.*

*Quelles évolutions avez-vous observées dans l’adoption de ces services au Maroc, et quels axes d’amélioration ou opportunités identifiez-vous pour leur développement futur ?*

**M. KHALID OCHI**
Responsable de la sécurité du système d'information
Les Eaux Minérales d'Oulmès

Les entreprises marocaines prennent effectivement de plus en plus conscience des opportunités offertes par les services managés pour répondre aux besoins de protection, de partage de risque, d’expertise technique, et de réduction du coût d’investissement.

Il est notamment important de souligner que les fournisseurs MSSP devraient actualiser leur portefeuille de services pour répondre aux contraintes budgétaires des petites et moyennes entreprises, de fournir des solutions adaptées aux besoins spécifiques par secteur d’activité, ainsi que d’élargir leurs offres technologiques.

**M. Nabil CHIADMI**
RSSI
CMR

Les services managés cyber au Maroc accusent un retard d'adoption par rapport au niveau international pour plusieurs raisons : manque d'expertise spécialisée (analystes SOC, pentesters), rareté des MSSP locaux disposant du savoir-faire et des capacités financières nécessaires, coûts élevés des solutions techniques (XDR, SIEM, SOAR) et réticence des organisations, particulièrement secteur public et semi public, face aux risques de dépendance externe. Pour développer ce marché, trois axes sont prioritaires : certification des prestataires locaux pour renforcer la confiance, développement d'offres adaptées aux spécificités marocaines, et mise en place de solutions évolutives accompagnant la croissance des entreprises.

**M. Abdessamad LIMY**
Responsable de sécurité de l’information et de continuité d’activité
Bourse de Casablanca

L’essor des services managés en cybersécurité au Maroc suit une dynamique ascendante, porté par plusieurs facteurs déterminants, notamment la demande croissante d’externalisation face à la sophistication des menaces et à la pénurie de compétences spécialisées, ainsi que l’adoption progressive du modèle OPEX.

Néanmoins, le potentiel de ces services demeure insuffisamment exploité. Pour en accélérer l’adoption et en maximiser l’impact, plusieurs leviers stratégiques doivent être mobilisés : la montée en maturité des entreprises, qui requiert un accompagnement ciblé et une sensibilisation approfondie aux bénéfices et aux enjeux contractuels de l’externalisation, l’évolution du cadre réglementaire, ainsi que l’innovation technologique, essentielle pour renforcer l’efficacité et l’attractivité des offres disponibles sur le marché.

## Question 3

*L'IA générative et les autres technologies émergentes redéfinissent la manière dont les entreprises renforcent leur cybersécurité, mais ces technologies élargissent aussi la surface d'attaque.*

*Dans votre expérience, comment les entreprises marocaines peuvent-elles exploiter ces technologies pour en maximiser les bénéfices tout en minimisant les risques ?*

**M. KHALID OCHI**
Responsable de la sécurité du système d'information
Les Eaux Minérales d'Oulmès

Personne ne peut nier l'apport significatif des technologies d'intelligence artificielle générative au quotidien des entreprises marocaines, que ce soit pour faciliter la prise de décision, d'améliorer la visibilité opérationnelle, ou encore de renforcer la détection et la réponse aux incidents de sécurité.

Il est toutefois indispensable, avant d'opter pour une technologie d'IA générative particulière, de sensibiliser les utilisateurs aux risques potentiels résultant de son usage, tels que la divulgation de données sensibles, les biais dans la prise de décision automatisée et l'utilisation de résultats inadaptés au contexte spécifique de l'entreprise.

L'aspect contractuel ne demeure pas moins important que les autres, notamment en intégrant des clauses spécifiques sur la protection des données, la transparence des modèles, la gestion des incidents et la propriété intellectuelle.

**M. Abdessamad LIMY**
Responsable de sécurité de l'information et de continuité d'activité
Bourse de Casablanca

L'IA générative et les technologies émergentes offrent aux entreprises marocaines des opportunités majeures pour renforcer leur cybersécurité, notamment en automatisant la détection et la réponse aux menaces. Toutefois, elles élargissent également la surface d'attaque, exposant les organisations à de nouveaux risques comme les deepfakes et l'ingénierie sociale avancée. Pour maximiser les bénéfices tout en limitant les vulnérabilités, il est essentiel de mettre en place une gouvernance rigoureuse, d'encadrer l'usage de ces technologies et d'assurer une veille proactive. Une approche équilibrée entre innovation et maîtrise des risques permettra aux entreprises d'exploiter ces avancées en toute sécurité.

**M. Nabil CHIADMI**
RSSI
CMR

Les technologies émergentes comme l'IA générative (IAG) représentent une arme à double tranchant pour la cybersécurité des entreprises marocaines. D'un côté, l'IAG apporte une valeur ajoutée considérable aux services SOC nouvelle génération en automatisant la détection des menaces et la réponse aux incidents. Elle améliore également la prédiction des attaques grâce à l'analyse avancée basée sur des modèles LLM sophistiqués. De l'autre côté, ces mêmes technologies peuvent être exploitées par des cybercriminels pour orchestrer des attaques plus sophistiquées. Pour maximiser les bénéfices tout en minimisant les risques, les entreprises marocaines doivent investir dans des solutions d'IA sécurisées et auditées, former leurs équipes à l'utilisation responsable de ces technologies et implémenter des contrôles stricts limitant les risques potentiels comme les fuites de données ou les détournements malveillants.

## Question 4

*Un leadership fort est souvent cité comme un facteur clé de succès en cybersécurité.*

*Dans votre expérience, quels comportements et actions des dirigeants influencent positivement la mise en place d’une culture cybersécurité solide et l’atteinte des objectifs stratégiques ?*

**M. KHALID OCHI**
Responsable de la sécurité
du système d'information
Les Eaux Minérales
d'Oulmès

Il est certain que l’engagement du top management est toujours un facteur prépondérant à la réussite de n’importe quelle initiative cybersécurité. Les principales manifestations de cet engagement sont brièvement :

- Allocation des moyens financiers et organisationnels, à savoir, équipes, budgets, outils et upscaling.
- Prise de décision équilibrée entre opportunité business, tolérance au risque et impératifs de sécurité.
- Conduite de changement à travers l’exemplarité et l’encouragement des bonnes pratiques.
- Tolérance aux effets de bords opérationnels issus de la mise en place des contrôles.

**M. Nabil CHIADMI**
RSSI
CMR

Le leadership fort en cybersécurité est crucial pour établir une culture de sécurité solide et atteindre les objectifs stratégiques. En effet, le top management doit montrer que la cybersécurité est une priorité stratégique, au même titre que d'autres objectifs stratégique métiers et commerciaux. Cela peut se manifester par le sponsoring effectif et fort par la mise en place d’un cadre de gouvernance cyber (SMSI) et par la participation active aux initiatives cyber, comme les comités de sécurité, les formations et les simulations de crise.

Le top management doit s'assurer que chaque employé comprend son rôle dans la protection des actifs de l'entreprise et doit s'assurer que les équipes cyber disposent des ressources financières, pédagogiques (formation et sensibilisation continue en cybersécurité) et technologiques nécessaires pour protéger l'entreprise.

**M. LIMY Abdessamad**
Responsable de sécurité de
l’information et de continuité d’activité
Bourse de Casablanca

Un leadership fort en cybersécurité repose sur l’engagement des dirigeants, leur exemplarité et une intégration claire des enjeux cyber dans la stratégie de l’entreprise. Ils doivent allouer des ressources adaptées, sensibiliser activement les collaborateurs et promouvoir une culture de vigilance. L’implication du RSSI dans la gouvernance et la gestion des risques est essentielle. Encourager la collaboration et le partage d’informations renforce la résilience collective. En adoptant ces actions, les dirigeants ancrent durablement la cybersécurité dans l’ADN de l’entreprise.

## Question 5

*Face à des menaces cyber de plus en plus complexes et à des ressources souvent limitées, les entreprises doivent faire des choix stratégiques dans leurs investissements.*

*Selon vous, quels sont les domaines prioritaires où les budgets cybersécurité devraient être concentrés pour maximiser l'impact tout en restant alignés sur les objectifs de l'organisation ?*

**M. KHALID OCHI**
Responsable de la sécurité du système d'information
Les Eaux Minérales d'Oulmès

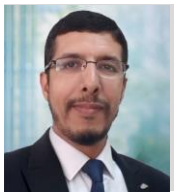
Il est primordial pour une organisation de prioriser l'investissement dans les domaines qui permettent le maintien et l'évolution de son activité. Il est toutefois nécessaire d'adopter une approche de sécurité holistique basée sur une analyse de risques pointues.

Il est aussi impératif pour n'importe quelle organisation d'établir la Baseline pour pouvoir survivre en cas de cyberattaque. Cela peut inclure :

- Le renforcement de la résilience humaine à travers la sensibilisation.
- La protection des données critiques via le chiffrement, la sauvegarde et la destruction sécurisée.
- La correction des vulnérabilités critiques sur – au moins – les systèmes exposés.
- La détection – même basique – par l'antivirus, le pare-feu et l'IDS.
- La mise en place d'un plan de réponse aux incidents qui prenne en compte au mois les événements les plus récurrents.

**M. LIMY Abdessamad**
Responsable de sécurité de l'information et de continuité d'activité
Bourse de Casablanca

Pour maximiser l'impact des investissements en cybersécurité avec des ressources limitées, les entreprises doivent prioriser plusieurs domaines clés. Cela inclut le renforcement des capacités de détection et de réponse, la sécurisation des accès et des identités, et la protection des données sensibles par chiffrement. La formation continue des collaborateurs et la sécurisation des environnements cloud sont également essentielles. Ces priorités permettent de renforcer la posture de sécurité tout en restant aligné sur les objectifs organisationnels. Un focus stratégique sur ces domaines assure une meilleure résilience face aux menaces cyber.



**M. Nabil CHIADMI**
RSSI
CMR

Pour maximiser l'impact des budgets cybersécurité tout en restant alignés sur les objectifs stratégiques de l'organisation, il est primordial de concentrer les investissements cyber sur des domaines prioritaires qui offrent le meilleur ROI en termes de réduction des risques, de protection des actifs critiques et de conformité réglementaire.

Dans un premier temps il est essentiel d'investir dans la mise en place d'un système de management de la sécurité de l'Information (SMSI) avec une identification et classification de tous les actifs (IT et OT) sensibles de l'entreprise.

Dans un deuxième temps il est fortement recommandé d'investir dans l'adoption d'une architecture zéro trust solides et pérenne avec des contrôles continus et en profondeur (SASI,ZTNA, SDWAN , CASBE…….etc.).

Les outils de gestion des identités et des accès IAM, les outils PAM et MFA sont également essentiels pour maitriser et limiter les risques liés aux accès aux systèmes, aux données sensibles et aux comptes à privilèges.

Dans le domaine de la détection et réponse, les solutions XDR, EDR et NDR avec des mécanismes embarqués d'IA sont devenus des atouts indispensables pour renforcer la capacité de détection et de réponse des SOC.

Sans oublier bien sûr l'upskilling des ressources IT en cyber sécurité et la sensibilisation cyclique des collaborateurs de l'entreprise.

## Question 6

*Les évolutions réglementaires au Maroc poussent les entreprises à structurer davantage leurs pratiques en cybersécurité.*

*Quels défis majeurs identifiez-vous dans la mise en conformité des entreprises marocaines ?*

**M. KHALID OCHI**
Responsable de la sécurité du système d'information
Les Eaux Minérales d'Oulmès

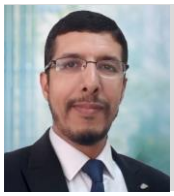
Dans un contexte géopolitique complexe, l'arsenal juridique marocain encourage les organisations à privilégier un usage souverain des données et des services.

Cependant, certaines entreprises se tournent vers des technologies émergentes (NTIC) hébergées à l'étranger, où les réglementations peuvent différer ou ne pas répondre aux exigences locales, afin de s'aligner sur leurs stratégies business, en l'absence d'offres locales adaptées.

Le défi principal réside dans la capacité à concilier conformité réglementaire et utilisation de ces technologies.

**M. LIMY Abdessamad**
Responsable de sécurité de l'information et de continuité d'activité
Bourse de Casablanca

Les entreprises marocaines font face à plusieurs défis dans la mise en conformité avec les évolutions réglementaires en cybersécurité. Le manque de sensibilisation et de formation, particulièrement dans les PME, rend difficile l'application des exigences. La limitation des ressources financières, surtout pour les PME, constitue également un frein majeur. De plus, la mise en place de processus de gouvernance adaptés et le suivi rigoureux des réglementations sont souvent insuffisants. Les entreprises doivent également garantir la protection des données sensibles, un enjeu crucial dans le cadre de la conformité. Pour réussir, il est essentiel d'investir dans des ressources spécialisées et des solutions adaptées tout en sensibilisant les collaborateurs.



**M. Nabil CHIADMI**
RSSI
CMR

Les évolutions réglementaires en matière de cybersécurité au Maroc, notamment la loi 05-20, la DNSSI v2 et la loi 09-08, représentent un défi majeur pour les entreprises marocaines. Elles les incitent à renforcer leurs pratiques de sécurité, mais plusieurs freins ou contraintes se dressent sur leur chemin :

- Dépendance au cloud et souveraineté numérique : L'utilisation massive de solutions de cybersécurité basées sur le cloud peut compromettre la souveraineté numérique du pays.
- Obsolescence des systèmes IT/OT : de nombreuses entreprises fonctionnent avec des systèmes IT/OT obsolètes, difficiles à sécuriser. En effet, elles sont confrontées à un dilemme entre maintenir la productivité et se conformer aux règlementations, car le remplacement de ces systèmes demande des investissements importants et peut s'étaler sur de longues périodes (délai d'amortissement entre 10 et 15 ans).
- Budget insuffisant : plusieurs entreprises marocaines manquent de ressources financières pour mettre en œuvre les mesures de cybersécurité nécessaires à la conformité légale.

En résumé, pour relever tous ces défis et assurer une conformité durable, il est essentiel d'asseoir une culture de sécurité robuste et une sensibilisation continue des employés.

# Passage à l'action : **Recommandations**

## Sécuriser l'avenir : vision & recommandations

### Anticiper, Investir et Converger

L'enquête AUSIM x PwC met en évidence une prise de conscience accrue des entreprises marocaines face aux enjeux de cybersécurité.

Cependant, malgré les efforts engagés, des défis majeurs subsistent : manque d'anticipation des risques, adaptation aux nouvelles réglementations, adoption des technologies émergentes et déficit de compétences internes.

Dans ce contexte, il est essentiel que les entreprises adoptent une approche proactive et structurée pour renforcer leur posture en matière de cybersécurité. Cela passe par trois axes stratégiques :

### Ce que les entreprises marocaines doivent mettre en place

#### Une cybersécurité intégrée à la stratégie globale

- Mettre en place une gouvernance claire et alignée avec la stratégie d'entreprise pour faire de la cybersécurité un levier de résilience et non une contrainte.
- Instaurer un suivi régulier des cybermenaces et évaluer en continu la maturité cyber de l'organisation.

#### Un investissement adapté aux menaces émergentes

- Prioriser les investissements dans la sécurité du Cloud, identifié comme un enjeu critique par 42% des entreprises interrogées.
- Déployer l'intelligence artificielle pour renforcer la détection des menaces, tout en s'assurant d'une gouvernance éthique et réglementaire conforme.
- Miser sur les services managés et les partenariats stratégiques pour pallier le manque de ressources internes et optimiser la réponse aux incidents.

#### Un alignement avec la réglementation et les bonnes pratiques

- Se conformer aux évolutions de la Loi 05-20 sur la cybersécurité et aux exigences de la DNSSI pour garantir la protection des infrastructures critiques.
- Adopter des standards internationaux (ISO 27001, NIST, CIS Controls) pour structurer les pratiques et assurer une résilience à long terme.
- Sensibiliser et former régulièrement les collaborateurs pour réduire les risques humains, qui restent un vecteur majeur de cyberattaques.

#### Une gestion de crise cyber efficace et adaptée

- S'assurer de l'existence d'un plan de continuité des activités robuste aux cyberattaques.
- Mettre en place les ressources nécessaires à la gestion de crise.
- S'entrainer pour pratiquer et s'améliorer.
- Tirer les leçons à chaque activation des plans de réponse et de reprise.

# Passage à l'action : **Introduction à la gestion de crise**

Introduction inspirée du guide ANSSI : Crise d'origine cyber – les clés d'une gestion opérationnelle et stratégique

## Comprendre la nature d'une crise d'origine cyber

Une crise cyber survient lorsqu'un incident informatique compromet gravement les activités d'une organisation. Elle se caractérise par sa soudaineté, son imprévisibilité et ses conséquences potentiellement majeures : interruption de services, atteinte à la réputation, perte de données sensibles ou exposition juridique.

## Se préparer efficacement à une crise cyber

La préparation en amont est déterminante pour limiter l'impact d'une crise. Elle repose sur sept leviers fondamentaux :

### 1. Connaître et maîtriser ses systèmes d'information

Cela passe par l'identification des actifs critiques, des dépendances numériques, et des scénarios d'attaque les plus plausibles. Cette cartographie permet d'orienter les décisions et les priorités en situation de crise.

### 2. Mettre en place un socle de capacités opérationnelles assurant la résilience numérique

Cela implique la mise en œuvre de dispositifs de surveillance, d'équipes spécialisées (SOC, CSIRT) et de procédures d'intervention adaptées aux différents types de menaces.

### 3. Formaliser une stratégie de communication de crise cyber

La communication en temps de crise doit être anticipée pour limiter les malentendus, rassurer les parties prenantes et protéger la réputation de l'organisation.

Une réponse efficace nécessite une gouvernance claire, des circuits décisionnels adaptés et une coordination fluide entre les métiers, les fonctions techniques et la direction.

### 4. Planifier et exécuter des exercices de gestion de crise

Les exercices réguliers permettent de tester les dispositifs, d'identifier les points de friction et de renforcer la réactivité des équipes.

### 5. Adapter les dispositifs de gestion de crise aux enjeux cyber

Les cellules de crise doivent être structurées pour intégrer les spécificités des incidents cyber. Cela suppose des rôles et responsabilités clairs ainsi qu'une coordination efficace entre les métiers et les techniques,

### 6. S'organiser pour bien gérer les preuves et porter plainte

En cas d'attaque, la conservation des preuves est essentielle pour permettre une analyse approfondie et, le cas échéant, engager des actions juridiques.

### 7. Gérer la sortie de crise et le retour à la normale

La phase de retour à la normale doit être progressive et sécurisée. Elle implique la vérification de l'état du SI, la remise en service maîtrisée des services, et un retour d'expérience structuré pour tirer les enseignements et renforcer les dispositifs existants.

# Passage à l'action : **Introduction à la gestion de crise**

Introduction inspirée du guide ANSSI : Crise d'origine cyber – les clés d'une gestion opérationnelle et stratégique

## Réagir efficacement en situation de crise en adoptant les bonnes pratiques

Lorsque la crise survient, la capacité à réagir rapidement et de manière structurée est déterminante pour en limiter les impacts. L'organisation doit pouvoir activer sans délai son dispositif de gestion de crise cyber.

Les premières actions consistent à :

- **Alerter, mobiliser et piloter la cellule de crise**, activer les mécanismes de soutien et coordonner l'ensemble des acteurs impliqués.
- **Maintenir la confiance des parties prenantes** en assurant une communication maîtrisée, cohérente et adaptée à la situation.
- **Conduire les investigations techniques** afin d'identifier l'origine et la portée de l'incident, tout en instaurant un mode de fonctionnement dégradé permettant la continuité des activités essentielles.
- **Relancer progressivement les activités critiques** et renforcer la sécurité des systèmes, en préparant les conditions d'un retour à un fonctionnement normalisé.
- **Tirer les enseignements de la crise**, capitaliser les retours d'expérience et consolider les dispositifs de gestion pour renforcer la résilience globale de l'organisation.

## Boîte à outils pour une gestion de crise structurée

Pour qu'une crise cyber soit gérée de manière rapide, coordonnée et efficace, l'organisation doit s'appuyer sur un socle d'outils préalablement définis et activables dès les premières alertes. Ces outils comprennent à la fois des **dispositifs généraux** – comme une cellule de crise physique ou virtuelle, un plan de communication de crise ou des fiches réflexes – et des **supports spécifiques** tels qu'un registre des risques et dérogations, une cartographie des systèmes critiques, un ordinateur hors réseau, ou encore un black-out outil de communication de secours.

## Boîte à outils pour une gestion de crise structurée

Au cœur de ce dispositif, trois outils structurants sont à activer en priorité :

### Le Plan de Continuité d'Activité (PCA)

Permet de maintenir les fonctions essentielles malgré une dégradation des conditions normales. Il s'appuie sur une organisation claire, une identification des activités critiques, une stratégie de continuité formalisée et des exercices réguliers.

### Le Plan de Continuité Informatique (PCI)

Assure la restauration des systèmes d'information indispensables à la continuité des services. Il repose sur l'anticipation des scénarios d'indisponibilité, la préparation des ressources techniques et la mise en œuvre de procédures de reprise.

### La cellule de crise cyber

Organe central de pilotage, réunissant les fonctions décisionnelles, techniques, métiers, communication et RH. Elle agit selon une gouvernance définie et coordonne l'ensemble des actions de gestion de crise, de l'investigation à la communication.

## Contact

**Jamal BASRIRE**
PwC
jamal.basrire@pwc.com

**Rachid BAARBI**
AUSIM
r.baarbi@lyazidi.co.ma