**Revue Française d'Economie et de Gestion**
ISSN : 2728- 0128
Volume 6 : Numéro 7

# Quel Management De La Cybersécurité Pour Favoriser La Performance Digitale Des Entreprises Marocaines ?

# How Can Cybersecurity Be Managed to Boost the Digital Performance of Moroccan Companies?

**Dr CHAGAR Hassan**
Enseignant chercheur
Rabat Business School, Université Internationale de Rabat

**BOUCHFAR Zakaria**
Executive MBA
Rabat Business School, Université Internationale de Rabat

**Date de soumission** : 15/05/2025

**Date d'acceptation** : 07/07/2025

**Pour citer cet article** :

CHAGAR. H. & BOUCHFAR. Z. (2025) « Quel Management De La Cybersécurité Pour Favoriser La Performance Digitale Des Entreprises Marocaines ? », Revue Française d'Économie et de Gestion « Volume 6 : Numéro 7 » pp : 647- 673.



**Résumé**

Dans un contexte global caractérisé par une digitalisation rapide et une augmentation constante des cybermenaces, cette recherche évalue la maturité managériale des entreprises marocaines en matière de cybersécurité. Basée sur une méthodologie quantitative enrichie d'éléments qualitatifs, l'étude interroge un échantillon diversifié de 122 cadres et managers issus d'organisations marocaines et internationales. Les principaux défis identifiés incluent l'insuffisance de sensibilisation et de formation, une gouvernance trop centrée sur les départements IT, ainsi qu'un investissement limité dans les technologies innovantes. Sur la base d'une analyse comparative internationale (France, Estonie, Kenya), cette étude propose des recommandations stratégiques ciblées, ainsi qu'un projet intégré « Cybersecurity Excellence Program » visant à positionner durablement le Maroc comme un acteur régional majeur en cybersécurité.

**Mots clés :** Cybersécurité ; Digital Morocco 2030 ; Maturité managériale ; ISO 27001 ; NIST CSF ; Gouvernance stratégique.

**Abstract**

In a global context characterized by rapid digitalization and a continuous rise in cyber threats, this research assesses the managerial maturity of Moroccan companies in cybersecurity. Based on a quantitative methodology enriched with qualitative elements, the study surveys a diverse sample of 122 executives and managers from Moroccan and international organizations. The main identified challenges include insufficient awareness and training, governance overly centered on IT departments, and limited investment in innovative technologies. Drawing from an international comparative analysis (France, Estonia, Kenya), the study proposes targeted strategic recommendations as well as an integrated "Cybersecurity Excellence Program" aimed at sustainably positioning Morocco as a leading regional actor in cybersecurity.

**Keywords:** Cybersecurity; Digital Morocco 2030; Managerial maturity; ISO 27001; NIST CSF; Strategic governance.

## Introduction

Le cyberespace, devenu un domaine stratégique majeur, conditionne désormais la souveraineté étatique et la compétitivité des entreprises. Sa protection, à travers une cybersécurité efficace, est comparable à la préservation de la santé mentale d'un individu, car les cyberattaques peuvent fragiliser les systèmes décisionnels et économiques.

Le Maroc, conscient de ces enjeux, a adopté la loi 43-20 sur la cybersécurité et s'aligne progressivement sur les standards internationaux (ISO 27001, NIST CSF). La Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) a élaboré une Stratégie Nationale de Cybersécurité 2030, visant à créer un environnement numérique sécurisé par la protection des infrastructures critiques, le renforcement de la gouvernance et un cadre juridique adapté. Par ailleurs, la stratégie Maroc Digital 2030 accélère la transformation numérique, ce qui accroît toutefois les risques cybernétiques.

Or, un récent incident impliquant un grand groupe marocain victime d'une cyberattaque ayant entraîné une rançon de 500 000 dollars souligne l'urgence d'une gouvernance intégrée et non exclusivement technique. Une étude de l'AUSIM révèle que 78% des dirigeants jugent insuffisants leurs investissements en cybersécurité, et 84% craignent des atteintes à leur réputation et à la confidentialité des données.

Dans un contexte de transformation numérique accélérée, les organisations marocaines doivent élever leur maturité managériale en cybersécurité afin de la positionner non plus comme un simple impératif technique, mais comme un levier stratégique durable. Cette élévation de maturité vise à garantir à la fois une résilience opérationnelle face aux menaces cyber et une conformité rigoureuse aux exigences de la Loi 43-20.

La question clé qui en découle est la suivante :

**Quel management de la cybersécurité pour favoriser la performance digitale des entreprises marocaines ?**

L'étude vise, à titre principal, à évaluer la maturité et les pratiques en cybersécurité des organisations marocaines afin de :

- Évaluer la culture organisationnelle en cybersécurité au sein des entreprises marocaines en mesurant les perceptions des acteurs internes (cadres IT et non IT) sur les notions et enjeux de cybersécurité.
- Identifier la perception des solutions techniques actuellement en place dans les organisations marocaines et évaluer leur alignement avec les tendances mondiales et leur efficacité perçue, en comparaison avec les meilleures pratiques internationales.

- Examiner précisément l'organisation du management cyber afin de comprendre si elle est structurée comme une fonction purement IT ou intégrée dans les processus décisionnels stratégiques.
- Analyser la perception individuelle des décideurs sur la cybersécurité en tant qu'investissement stratégique de compétitivité et d'opportunités économiques (business, réputation, confiance) ou une contrainte économique.

Ces volets permettront de dresser un panorama précis de l'état du dispositif cyber au Maroc et d'orienter des recommandations opérationnelles et stratégiques adaptées.

La suite de l'article s'articule comme suit : après une revue de littérature qui établit le cadre théorique (section 1), nous présentons la méthodologie de l'étude (section 2), puis analysons les résultats et leur discussion (section 3). Enfin, la conclusion (section 4) expose les apports, limites et perspectives.

## 1. Fondements théoriques

### 1.1. Les cadres normatifs en cybersécurité

Face à la digitalisation accrue et aux menaces croissantes, deux modèles internationaux sont particulièrement pertinents pour le contexte marocain et essentiels pour structurer une gouvernance efficace :

- CMMI-S (Capability Maturity Model Integration for Security) : propose cinq niveaux de maturité, allant de chaotique à optimiser, adaptés aux organisations cherchant une démarche structurée rigoureuse.
- NIST Cybersecurity Framework : privilégie une approche flexible, applicable aux PME comme aux grandes entreprises, structuré autour de cinq piliers clés (identifier, protéger, détecter, répondre, récupérer). La stratégie marocaine met particulièrement l'accent sur ce modèle pour sa flexibilité.

Le Maroc adopte progressivement ces standards à travers la Loi 43-20 et la Stratégie Nationale de Cybersécurité 2030, axée sur la protection des infrastructures critiques et la gouvernance intégrée. La combinaison de ces normes internationales et de ce référentiel national fournit aux organisations marocaines une architecture normative complète, indispensable pour atteindre une maturité cybernétique élevée, assurer la conformité légale et bâtir une résilience pérenne face aux menaces numériques.

La DGSSI recommande prioritairement le NIST CSF pour sa flexibilité et sa facilité d'adoption, tandis que le CMMI-S peut être préconisé par les entités souhaitant une standardisation plus stricte, au prix d'un effort de mise en œuvre plus conséquent. Cette dualité offre aux

organisations marocaines le choix entre agilité opérationnelle et rigueur structurelle pour progresser vers une maturité cybernétique optimale.

### 1.2. La cybersécurité comme levier stratégique

Traditionnellement considérée comme une contrainte technique ou un centre de coût, la cybersécurité est aujourd'hui devenue un véritable facteur de compétitivité et de résilience organisationnelle. Les entreprises matures ont pleinement intégré la cybersécurité dans leur stratégie globale, reconnaissant sa capacité à protéger durablement leurs actifs critiques, renforcer leur réputation et créer un avantage concurrentiel décisif.

Plusieurs avantages stratégiques majeurs découlent directement d'une maturité élevée en cybersécurité :

- Confiance client et avantage concurrentiel : L'adoption de standards élevés de cybersécurité (ISO 27001, RGPD, NIST CSF, etc.) permet aux organisations de se démarquer de leurs concurrents en garantissant un niveau de protection avancé des données et des infrastructures critiques. Elle permet aussi d'améliorer la réputation des entreprises et de faciliter significativement l'accès à des marchés internationaux très régulés, notamment en Europe (RGPD) ou aux États-Unis (CCPA).
- Réduction des risques et coûts opérationnels : Une cybersécurité efficace limite les conséquences financières majeures des cyberattaques (estimées mondialement à 4,88 millions USD par incident), assure la continuité d'activité (PCA/PRA) et réduit les coûts d'assurance cyber.
- Cybersécurité et transformation digitale : La cybersécurité n'entrave pas l'innovation, elle en constitue le catalyseur. À travers une gouvernance agile et collaborative, l'intégration précoce de la sécurité (Security by Design) dans les projets numériques permet de tirer pleinement parti des technologies émergentes (IA, cloud, IoT) tout en préservant la souveraineté, la confidentialité des données et la compétitivité des entreprises marocaines sur la scène internationale.
- Gouvernance transversale des risques cybernétiques : La cybersécurité doit être intégrée comme une responsabilité partagée à tous les niveaux de l'organisation, et non cantonnée au seul département IT. Cela nécessite l'implication active du top management, une sensibilisation continue des employés, et des rôles clairement définis (RSSI, DPO, analystes SOC). En adoptant cette approche transversale, l'organisation consolide sa résilience face aux menaces, améliore la réactivité opérationnelle et renforce la culture de sécurité à tous les échelons.

- Conformité réglementaire : La prolifération des régulations en matière de sécurité et de protection des données (RGPD, Loi 43-20) impose aux entreprises une conformité impérative pour se prémunir de sanctions et préserver leur réputation.

Ainsi, l'adhésion rigoureuse à ces exigences légales et normatives apparaît comme un axe prioritaire pour toute organisation souhaitant consolider sa posture de cybersécurité, limiter ses risques juridiques et renforcer sa crédibilité opérationnelle, tant sur le plan national qu'international.

### 1.3. Benchmark international et enseignements clés

L'analyse comparative internationale met en avant les meilleures pratiques mondiales et offre des enseignements concrets pour le Maroc :

- Gartner (2023) souligne l'importance d'une gouvernance transversale portée par le top management et l'intégration précoce de la cybersécurité dans le cycle de vie des projets (Security by Design) pour réduire significativement les incidents. Cette double orientation constitue le socle d'une posture cyber résiliente et garante d'une compétitivité durable.
- CIGREF (2023) met en exergue la dimension humaine et managériale de la cybersécurité, en insistant sur la nécessité de campagnes internes régulières de sensibilisation et de formation continue, avec une forte implication du top management. C'est ce qui constitue la pierre angulaire d'une gouvernance cyber efficace, capable d'insuffler une responsabilité partagée et de solidifier l'adoption des bonnes pratiques à tous les étages de l'entreprise.
- CESIN et Tikehau Capital (2024) mettent en évidence une augmentation mondiale des budgets cybersécurité dans les secteurs régulés (finance, santé, énergie), contrastant avec des investissements marocains encore insuffisants.

Afin d'enrichir le benchmark comparatif et d'extraire des pratiques transférables au Maroc, trois pays illustrent des écosystèmes numériques matures et des stratégies cohérentes :

- France : Écosystème mature (ANSSI, Cyber Campus) avec forte coopération public-privé (Orange Cyberdefense, Thales, Capgemini, Atos) et formation spécialisée garantissant un vivier de compétences qualifiées.
- Kenya : Gouvernance agile intégrant l'IA et cybersécurité (Kenya National AI Strategy 2025-2030), et favorisant les partenariats internationaux pour codévelopper des solutions innovantes.

- Estonie : Leader mondial avec son modèle e-Estonia (infrastructure numérique nationale sécurisée, inscrite dans la Constitution) et le « NATO Cyber Security Centre », intégrant pleinement le « Security by Design ».

Ces benchmarks recommandent pour le Maroc une stratégie nationale proactive, une coopération public-privé renforcée, et le développement prioritaire de compétences spécialisées en réponse aux incidents, audit forensique, cloud sécurité et MSSP.

Ces retours d'expérience soulignent l'importance d'une approche intégrée, multisectorielle et orientée innovation pour propulser le Maroc vers une maturité cybernétique comparable aux leaders mondiaux.

Parallèlement à l'analyse de ces benchmarks internationaux pertinents, il est essentiel de synthétiser clairement les principaux enseignements des recherches antérieures afin d'identifier explicitement le gap à combler pour le Maroc.

### 1.4. Synthèse des travaux antérieurs et gap identifie

La revue des travaux antérieurs permet d'identifier clairement un ensemble de constats clés sur la maturité cybernétique des entreprises marocaines comparée aux meilleures pratiques internationales.

Ces travaux convergent vers une maturité cybernétique faible à intermédiaire au sein des entreprises marocaines, sous l'effet de trois principales carences : sensibilisation interne insuffisante, gouvernance peu structurée, et investissements jugés insuffisants (l'AUSIM, en 2025, révèle que les décideurs considèrent leurs budgets cybersécurité comme trop faibles).

À cela s'ajoutent des obstacles à l'adoption des standards internationaux (ISO 27001, NIST CSF) : le déficit de compétences qualifiées en interne et la vision centrée sur l'aspect technique, au détriment d'une démarche globale et stratégique de la cybersécurité.

### 1.5. Gap clairement identifie pour le Maroc

Les entreprises marocaines doivent impérativement évoluer d'une posture technique et réactive vers une approche à la fois stratégique, proactive et intégrée (non seulement à l'IT, mais également aux départements Finance, RH, Marketing, etc.) de la cybersécurité, impliquant davantage le top management, renforçant les formations internes et augmentant stratégiquement les investissements technologiques (Cloud, IA, Zero Trust).

Ce constat fonde le cadre théorique de l'étude : déterminer les leviers stratégiques, managériaux et économiques permettant aux organisations marocaines de combler cet écart, d'atteindre une maturité cybernétique conforme aux meilleures pratiques internationales et de saisir des opportunités économiques majeures (Incident Response, Cloud Cybersecurity, forensique…).

## 2. Méthodologie

Cette partie détaille la démarche méthodologique adoptée pour mener cette recherche. Elle présente les approches méthodologiques utilisées, les choix réalisés en matière d'échantillonnage, le processus rigoureux de collecte des données ainsi que les techniques d'analyse employées pour traiter et interpréter les résultats obtenus.

### 2.1. Délimitation du problème de recherche

L'étude vise à déterminer quel type de management de la cybersécurité favorise la performance digitale des entreprises marocaines. Elle s'articule autour de la question centrale :

**« Quel management de la cybersécurité pour favoriser la performance digitale des entreprises marocaines ? »**

Pour structurer l'analyse et orienter la méthodologie, cette problématique est déclinée en quatre dimensions clés :

- Culture organisationnelle en cybersécurité.
- Connaissance des solutions techniques disponibles.
- Organisation et gouvernance stratégique de la cybersécurité.
- Perception individuelle et collective de la valeur stratégique de la cybersécurité.

Cette délimitation précise fournit le cadre conceptuel indispensable à la conception du questionnaire et à l'interprétation des résultats, assurant une étude ciblée.

#### 2.1.1. Questions de recherche

Pour répondre à la problématique, quatre questions de recherche ont été formulées :

- Comment les équipes IT et non IT perçoivent-elles et adoptent-elles la culture de cybersécurité ?
- Quel est le niveau de conscience des managers sur les solutions techniques existantes et leur alignement international ?
- Comment est structurée la gouvernance de la cybersécurité dans les entreprises marocaines ?
- Comment les répondants perçoivent-ils la valeur ajoutée de la cybersécurité dans leur environnement professionnel et organisationnel ?

#### 2.1.2. Typologie de l'étude

L'étude adopte une approche mixte, principalement quantitative (questionnaire structuré électronique), enrichie d'éléments qualitatifs (questions ouvertes), afin d'offrir une vision réaliste et représentative de la maturité cybersécurité des entreprises. Un benchmark qualitatif international complète l'analyse pour situer le Maroc dans un contexte global.

### 2.2. Échantillon et population cible

- Population cible : Cadres et managers IT et non IT d'organisations marocaines variées (public, privé, semi-public).
- Échantillon final : 122 répondants, dont 105 marocains et 17 internationaux.
- Critères d'inclusion larges : Sans exigence de responsabilité directe en cybersécurité, afin d'obtenir une diversité maximale des perspectives.

### 2.3. Structure et organisation du questionnaire

Le questionnaire a été structuré en six grandes sections :

- Profil du répondant : Secteur d'activité, taille, type d'organisation et fonction du répondant (IT vs non IT). Ces éléments de profilage permettent de contextualiser les réponses et d'effectuer des comparaisons pertinentes entre les groupes de répondants.
- Culture de la cybersécurité : Définition claire, campagnes de sensibilisation, compréhension du rôle des employés, sensibilisation aux menaces émergentes, implication de la direction. L'évaluation de ces éléments permet de mesurer la maturité de la culture cybersécurité au sein de l'organisation et de comprendre l'ampleur de l'engagement à tous les niveaux de l'entreprise.
- Connaissance des solutions techniques : Utilisation de référentiels (ISO 27001, NIST CSF), maturité RGPD, existence d'un SOC actif, sécurisation du cloud, exploration des technologies innovantes (IA, blockchain, Zero Trust). Cette dimension évalue la présence et l'efficacité perçue des solutions techniques en cybersécurité déployées au sein des entreprises.
- Organisation et gouvernance cybersécurité : Structure organisationnelle, supervision par la direction, intégration transversale avec d'autres départements, politique formelle de gestion des incidents, collaboration avec partenaires externes (CERT, fournisseurs). L'analyse de ces points permet de dresser un portrait précis de la gouvernance cybersécurité au sein des organisations et d'évaluer leur capacité à gérer les risques de manière intégrée et stratégique.
- Perception de la valeur ajoutée stratégique : Cybersécurité perçue comme investissement ou contrainte, satisfaction des solutions, perception de l'investissement en cybersécurité, contribution aux résultats financiers, mesure du ROI. Cette dimension explore la manière dont la cybersécurité est perçue au sein de l'organisation, tant sur le plan stratégique qu'économique.

- Conclusion (questions ouvertes) : Cette section permet de recueillir des avis qualitatifs sur les défis rencontrés par les entreprises et leurs besoins futurs.

### 2.4. Collecte et traitement des données

Cette section décrit les méthodes utilisées pour la collecte et l'analyse des données :

- Mode de collecte : Questionnaire électronique diffusé via LinkedIn et des groupes WhatsApp professionnels, assurant ainsi une large participation des cadres et managers dans divers secteurs.
- Période de collecte : Premier trimestre de l'année 2025.
- Analyse des données : Traitement statistique quantitatif (Excel, Power BI) et analyse qualitative approfondie des réponses ouvertes. Benchmark comparatif international pour situer les résultats dans un contexte global et renforcer la validité des recommandations.

### 2.5. Justification du choix méthodologique

L'approche quantitative structurée retenue permet d'obtenir une analyse précise et comparative des perceptions et pratiques en cybersécurité au Maroc, par rapport aux standards internationaux, garantissant ainsi la pertinence et l'applicabilité des recommandations stratégiques proposées.

## 3. Analyse des résultats

Cette section présente les résultats (cf. détails en ANNEXE) issus du questionnaire structuré diffusé auprès d'un échantillon diversifié de cadres et managers marocains, issus à la fois du domaine IT et non IT, avec une comparaison internationale. Ces résultats sont exprimés en pourcentages, reflétant directement les réponses obtenues. Cela permet une lecture précise et une interprétation statistique des données.

### 3.1. Caractéristiques du profil des répondants

L'échantillon analysé se compose de 122 répondants, répartis comme suit :

- Maroc : 105 répondants (86 %)
- International : 17 répondants (14 %), incluant des participants provenant de pays comme Canada, France, Israël, Luxembourg et Turquie. Cette représentation internationale enrichit l'analyse en offrant un benchmark qualitatif pour une comparaison des pratiques à l'échelle mondiale.

L'analyse du profil des répondants montre une diversité significative en termes de secteurs d'activité, tailles d'entreprises, types d'organisations et fonctions occupées, assurant que les

résultats reflètent une large gamme de perspectives sur les enjeux de cybersécurité, en tenant compte des spécificités locales et internationales.

En résumé, les répondants proviennent principalement des secteurs de l'industrie, de la technologie et des services publics. Majoritairement issus d'organisations privées (75%), publiques (18%) et semi-publiques (7%), ils sont à 77% des cadres/managers non IT et à 23% des responsables IT. L'échantillon présente également une répartition équilibrée en matière de tailles d'organisation et de chiffres d'affaires, assurant ainsi une robustesse statistique et une diversité organisationnelle significative.

### 3.2. Culture organisationnelle en cybersécurité

Résultats clés :

- Niveau de maturité global jugé faible (45%) ou intermédiaire (38%). Seuls 17% déclarent une maturité avancée.
- Majorité avec définition claire de la cybersécurité, mais des lacunes persistent.
- Campagnes de sensibilisation irrégulières. Bonne compréhension générale du rôle des employés, mais nécessité d'amélioration continue.
- Implication notable des directions générales, mais sensibilisation insuffisante aux menaces émergentes (27% des répondants).
- Benchmark international : en France, 85 % des entreprises ont des campagnes régulières contre seulement 45 % au Maroc.

Malgré une prise de conscience croissante, l'analyse des réponses montre une perception globalement intermédiaire à faible de la maturité en cybersécurité des organisations marocaines. Les entreprises les plus avancées sont principalement celles qui ont adopté des référentiels internationaux, tandis que d'autres se contentent de mesures basiques, souvent perçues comme insuffisantes.

Les entreprises marocaines doivent encore renforcer significativement leurs efforts de sensibilisation régulière et leur gouvernance stratégique.

### 3.3. Connaissance et adoption des solutions techniques

Résultats clés :

- 57 % des entreprises suivent partiellement l'ISO 27001, 45 % le NIST CSF, avec un retard marqué des PME.
- Maturité moyenne sur la conformité RGPD. Présence limitée de SOC actif et solutions cloud sécurisées.

- Faible adoption des solutions avancées (Zero Trust, XDR) et technologies innovantes (IA, blockchain).
- Benchmark international : Selon Tikehau Capital (2024), 62% des entreprises mondiales augmentent leurs budgets cybersécurité, contre des investissements marocains encore limités.

Une majorité des entreprises interrogées affirme utiliser des standards internationaux, mais leur application concrète varie. Les grandes d'entre elles sont plus alignées sur ces standards, alors que les PME rencontrent des difficultés à implémenter une gouvernance cyber robuste.

Les entreprises marocaines adoptent progressivement les solutions techniques internationalement reconnues, mais doivent accélérer leur alignement avec les meilleures pratiques mondiales.

### 3.4. Organisation et gouvernance de la cybersécurité

Résultats clés :

- Gouvernance souvent centralisée au sein du département IT, avec peu de RSSI dédiés.
- Politiques de gestion des incidents faiblement formalisées et intégration transversale limitée avec d'autres départements.
- Faible mais croissante collaboration avec des partenaires externes spécialisés (CERT, fournisseurs spécialisés), indiquant un potentiel inexploité pour renforcer leur cybersécurité.
- Benchmark international : la présence systématique de RSSI, recommandée par Gartner, reste insuffisante au Maroc.

L'analyse révèle une gouvernance cybersécurité encore largement rattachée au département IT, avec une faible implication transversale des autres départements. Peu d'entreprises marocaines disposent d'un RSSI (Responsable Sécurité des Systèmes d'Information) entièrement dédié, et les politiques formalisées de gestion des incidents restent minoritaires. La collaboration avec des partenaires externes spécialisés (CERT, prestataires en cybersécurité) est en croissance mais reste limitée à une minorité d'entreprises.

Une meilleure intégration transversale et une gouvernance clarifiée permettraient aux entreprises marocaines d'améliorer significativement leur maturité cybernétique.

### 3.5. Perception de la valeur ajoutée de la cybersécurité

Résultats clés : La perception stratégique de la cybersécurité diffère sensiblement entre les répondants IT et non IT. Ainsi, 70% des répondants du domaine IT perçoivent clairement la cybersécurité comme un investissement stratégique nécessaire, contre seulement 55% des

cadres non IT, qui tendent à percevoir cette fonction davantage comme un coût ou une contrainte organisationnelle.

La mesure formelle du retour sur investissement (ROI) des dépenses cybersécurité reste exceptionnelle dans les entreprises marocaines, contrairement à 60% des entreprises internationales selon Tikehau Capital (2024).

Bien que la cybersécurité soit progressivement perçue comme stratégique, des efforts de sensibilisation sont nécessaires auprès des cadres non IT afin de faciliter l'intégration complète et transversale de la cybersécurité comme levier de création de valeur économique et concurrentielle.

### 3.6. Défis majeurs identifiés

Les principaux défis selon les répondants sont variés, avec peu de répétitions exactes, mais voici quelques thèmes clés identifiés :

- Menaces cybernétiques avancées et évolutives **(36,4 %)**
- Insuffisance de sensibilisation et de formation interne **(21,8 %)**
- Budget limité et ressources insuffisantes **(5,5 %)**
- Protection des infrastructures critiques **(3,6 %)**
- Autres défis incluant l'insuffisance de soutien gouvernemental et d'outils avancés de détection **(32,7 %)**

Ces défis mettent en évidence des axes stratégiques essentiels à renforcer dans la maturité cybernétique des entreprises marocaines.

### 3.7. Soutiens externes souhaités

Les résultats montrent que les organisations marocaines expriment un besoin marqué de soutien externe pour améliorer leur cybersécurité. Les réponses les plus fréquemment citées sont :

- Formations spécialisées et régulières
- Meilleure réglementation et sanctions plus dissuasives
- Recours à des experts externes (consultants spécialisés, CERT…).
- Incitations financières ou fiscales spécifiques

Ces résultats soulignent que des soutiens externes ciblés pourraient jouer un rôle clé dans l'accélération du développement de la maturité cybernétique au Maroc, en facilitant l'accès aux ressources, formations et expertises nécessaires pour renforcer la cybersécurité des organisations.

Une proportion notable de réponses **"Je ne sais pas"** indique un manque de clarté ou de compréhension sur les types de soutiens externes nécessaires.

### 3.8. Analyse comparative internationale

L'analyse des réponses des 17 répondants internationaux met en lumière une maturité nettement supérieure dans la gestion de la cybersécurité :

- Définition claire de la cybersécurité plus répandue.
- Campagnes de sensibilisation régulières plus fréquentes.
- Forte implication des directions générales.
- Perception stratégique plus affirmée, avec une évaluation régulière du ROI cybersécurité (60% à l'international contre rareté au Maroc).
- Pratiques innovantes telles que l'utilisation avancée de l'IA et l'approche « Security by Design » bien intégrées à l'international.

### 3.9. Synthèse des résultats

L'analyse comparée montre que les entreprises marocaines sont encore loin de l'excellence en cybersécurité en comparaison avec les pratiques internationales. En particulier, des améliorations sont nécessaires dans la gouvernance stratégique, l'investissement en technologies avancées et la sensibilisation continue.

Les résultats suggèrent que pour atteindre une maturité comparable aux meilleures pratiques internationales, les entreprises marocaines devront investir davantage dans la formation, la gouvernance, et l'intégration des technologies avancées.

## 4. Discussion des résultats et recommandations stratégiques

### 4.1. Discussion des résultats

L'analyse des données révèle un ensemble de constats convergents quant à la maturité managériale de la cybersécurité au sein des organisations marocaines :

#### 4.1.1. Culture de la cybersécurité

Malgré une prise de conscience émergente, beaucoup d'entreprises marocaines manquent encore de définition claire de la cybersécurité et les campagnes de sensibilisation restent insuffisantes. Une implication accrue des directions générales est nécessaire pour en faire un enjeu stratégique majeur.

#### 4.1.2. Connaissance des solutions techniques

Bien que les organisations marocaines utilisent des outils fondamentaux (firewalls, MFA, SIEM), leur alignement avec les référentiels internationaux (ISO 27001, NIST CSF, PCI DSS) reste partiel. L'utilisation des technologies innovantes (IA, blockchain, Zero Trust) est faible, révélant une maturité limitée en cybersécurité.

#### 4.1.3. Organisation de la cybersécurité

La gouvernance reste majoritairement centralisée au département IT, avec peu d'intégration transversale avec d'autres départements. L'absence fréquente d'un RSSI dédié et le manque de politiques formalisées de gestion des incidents constituent des limites importantes.

#### 4.1.4. Perception de la valeur ajoutée

70 % des répondants IT perçoivent la cybersécurité comme stratégique, contre seulement 55 % des non-IT. Le retour sur investissement (ROI) de la cybersécurité est rarement mesuré, freinant ainsi son intégration complète comme levier stratégique.

#### 4.1.5. Défis majeurs

- Sophistication croissante des menaces **(36,4 %)**
- Compétences spécialisées et formations insuffisantes **(21,8 %)**
- Budgets et ressources limités **(5,5 %)**

#### 4.1.6. Soutiens externes nécessaires

- Formations spécialisées régulières
- Renforcement réglementaire et sanctions dissuasives
- Expertise externe (consultants, CERT)
- Incitations financières/fiscales claires

### 4.2. Recommandations stratégiques

Pour traduire en actions concrètes les enseignements issus de l'analyse, cinq axes stratégiques sont proposés afin de renforcer la maturité cybernétique des organisations marocaines et d'en maximiser les retombées économiques, concurrentielles et réputationnelles :

#### 4.2.1. Axe 1 : Instaurer une culture cyber stratégique

- Objectif : Ancrer la cybersécurité dans l'ADN de l'entreprise
- Actions clés :
  - Élaborer et diffuser une charte cybersécurité formalisée.
  - Mettre en place des campagnes régulières (ateliers, simulations de phishing).
  - Organiser des revues trimestrielles de la stratégie sécurité par le CODIR.

#### 4.2.2. Axe 2 : Accélérer l'innovation technologique

- Objectif : Renforcer la posture défensive et proactive
- Actions clés :
  - Piloter des projets IA & Machine Learning pour la détection des menaces.
  - Adopter le Zero Trust (micro-segmentation, authentification forte).
  - Formaliser une veille technologique et benchmarker les nouveaux outils.

#### 4.2.3. Axe 3 : Structurer la gouvernance transverse

- Objectif : Associer toutes les parties prenantes et optimiser la résilience
- Actions clés :
    - Constituer un Comité de gouvernance cyber réunissant IT, RH, Finance, Marketing.
    - Créer un poste de RSSI indépendant, rattaché à la DG.
    - Instaurer des protocoles d'escalade clairs et tester les procédures de gestion de crise (PCA/PRA).

#### 4.2.4. Axe 4 : Valoriser la cybersécurité comme levier économique

- Objectif : Mesurer, communiquer et optimiser l'investissement
- Actions clés :
    - Définir des indicateurs clés (KPI) : nombre d'incidents, temps de rétablissement, ROI estimé.
    - Réaliser un tableau de bord cybersécurité pour le CODIR.
    - Lancer des incitations internes (budget R&D, certifications) pour encourager les initiatives cyber.

#### 4.2.5. Axe 5 : Renforcer la coopération public-privé

- Objectif : Dynamiser l'investissement privé
- Action clé : Développer une plateforme nationale de partage d'informations cybernétiques, soutenue par des incitations publiques et des aides financières ciblées.

En suivant ces axes, les organisations marocaines pourront non seulement combler les écarts identifiés, mais aussi transformer la cybersécurité en un levier pérenne de performance digitale, d'innovation et de confiance pour l'ensemble de l'écosystème national.

### 4.3. « Cybersecurity Excellence Program »

Pour traduire en actions concrètes les recommandations précédentes et hisser rapidement le Maroc au rang de hub régional de cybersécurité d'ici à 2030, l'étude propose le « Cybersecurity Excellence Program », un projet national structurant articulé autour de trois volets :

#### 4.3.1. Objectifs stratégiques

- Renforcer les compétences cyber managériales et techniques
- Accroître la maturité organisationnelle selon standards internationaux
- Réduire les impacts économiques et réputationnels des cyberattaques
- Positionner le Maroc comme hub régional majeur en cybersécurité d'ici 2030

#### 4.3.2. Composantes du programme

- Cyber Leadership Academy : Formation certifiante ciblée pour décideurs et managers
- Cybersecurity Innovation Lab : Développement et expérimentation de solutions avancées (Zero Trust, IA)
- National Cybersecurity Maturity Index: Évaluation continue et benchmarking international
- Cyber Resilience Investment Fund : Financement d'initiatives innovantes en cybersécurité pour les PME

#### 4.3.3. Résultats attendus

- Capital humain renforcé : développement soutenu de compétences spécialisées répondant aux besoins du marché national et régional.
- Conformité et maturité accrues : progression mesurable des entreprises marocaines vers les meilleurs référentiels mondiaux.
- Résilience opérationnelle accrue : protection renforcée des actifs numériques et réduction tangible des pertes liées aux cyberattaques.
- Écosystème innovant : émergence d'un vivier de startups et d'acteurs locaux, créant un cercle vertueux d'investissement et de R&D.
- Positionnement stratégique : affirmation du rôle du Maroc comme hub régional de cybersécurité, en cohérence avec les stratégies nationales Maroc Digital 2030 et Stratégie Nationale Cybersécurité 2030.

### 4.4. Opportunités économiques et stratégiques

Le marché marocain de la cybersécurité, stimulé par la digitalisation rapide et un cadre réglementaire renforcé (Loi 43-20, Stratégie Nationale Cybersécurité 2030, Maroc Digital 2030), présente un ensemble d'opportunités concrètes pour les investisseurs.

#### 4.4.1. État actuel et perspectives

Marché marocain en forte croissance, avec une demande croissante en audit cybersécurité, services externalisés (MSSP), cybersécurité Cloud, mais encore insuffisamment exploité par des acteurs locaux et internationaux. En somme, il présente un terrain fertile pour les investisseurs désireux de se positionner sur des segments à forte valeur stratégique et encore peu couverts, garantissant ainsi un excellent potentiel de croissance et de différenciation.

#### 4.4.2. Clients potentiels identifiés

L'étude identifie quatre segments-clés offrant des opportunités de développement pour des offres spécialisées en cybersécurité au Maroc :

- Grandes entreprises industrielles, financières, télécoms et santé (audit sécurité, compliance)
- PME nécessitant des services externalisés accessibles (MSSP)
- Administrations publiques (audit approfondi, formation, conformité)
- Établissements de formation supérieure en cybersécurité (certifications spécialisées)
- En ciblant ces segments de manière précise, les investisseurs et prestataires peuvent élaborer des offres sur-mesure, maximisant ainsi leur impact et leur retour sur investissement sur un marché encore largement inexploré.

#### 4.4.3. Segments porteurs pour investissements

Le marché marocain de la cybersécurité offre plusieurs opportunités d'investissement à fort potentiel, avec des segments spécifiques à cibler :

- Création d'un centre spécialisé en Cyber Forensics & Incident Response
- Développement de services Cloud-first Security innovants
- Lancements de MSSP dédiés aux PME
- Création de centres certifiés en formation cybersécurité

Ces segments représentent des opportunités stratégiques pour les investisseurs désireux de se positionner sur des niches en forte demande, tout en contribuant à la compétitivité du secteur de la cybersécurité au Maroc.

#### 4.4.4. Facteurs favorisant l'investissement

Le secteur marocain de la cybersécurité présente plusieurs facteurs clés qui le rendent particulièrement attractif pour les investisseurs nationaux et internationaux :

- Soutien des autorités marocaines via la Stratégie Nationale Cybersécurité 2030
- Cadre réglementaire attractif (Loi 43-20)
- Incitations fiscales et subventions ciblées pour l'innovation technologique

Ces facteurs stratégiques créent un écosystème favorable à l'investissement dans la cybersécurité, stimulant à la fois l'innovation technologique, la compétitivité des entreprises locales et l'intégration du Maroc dans la dynamique régionale de cybersécurité.

#### 4.4.5. Benchmarks internationaux applicables

Pour illustrer l'attractivité stratégique et économique des investissements dans le secteur de la cybersécurité, trois modèles internationaux exemplaires sont présentés :

- France : écosystème mature, avec soutien gouvernemental (à travers des incubateurs spécialisés comme le Cyber campus à Paris), et collaboration public-privé efficace.

- Estonie : leader mondial en e-gouvernance et cybersécurité intégrée, en développant son programme e-Estonia et en investissant dans des infrastructures sécurisées (ex. NATO Cyber Security Centre) et des solutions innovantes.
- Kenya : gouvernance agile avec intégration IA et cybersécurité, facilitant l'arrivée d'investisseurs internationaux.

#### 4.4.6. Recommandations pour concrétiser ces opportunités

Pour tirer pleinement parti des opportunités économiques et stratégiques dans le secteur de la cybersécurité, plusieurs recommandations spécifiques sont proposées afin de dynamiser et consolider le marché marocain de la cybersécurité :

- Créer rapidement un cadre incitatif clair pour les investissements privés (avantages fiscaux, aides ciblées).
- Développer activement la coopération public-privé (clusters, incubateurs spécialisés).
- Investir massivement dans les compétences humaines via des formations spécialisées certifiantes.

## Conclusion

Cette étude a permis d'établir un état des lieux approfondi de la maturité managériale des organisations marocaines en matière de cybersécurité, dans un contexte marqué par l'accélération de la transformation numérique et la montée en puissance des menaces cybernétiques. Les résultats révèlent une prise de conscience encore embryonnaire du caractère stratégique de la cybersécurité, souvent cantonnée à une fonction technique, et une insuffisance notable en matière de conformité aux standards internationaux, de formation spécialisée et d'évaluation du retour sur investissement.

Face à ce constat, l'étude émet un ensemble de recommandations structurantes visant à renforcer la posture cybersécuritaire du tissu économique marocain :

- La mise en place d'une gouvernance intégrée de la cybersécurité, impliquant les directions générales et favorisant une vision transversale des risques numériques.
- Le renforcement massif de la sensibilisation et de la formation continue, avec un accent sur la certification et le développement des compétences spécialisées.
- La généralisation des standards internationaux (ISO 27001, NIST CSF, etc.) pour améliorer la crédibilité et la résilience des entreprises.
- L'adoption de technologies innovantes, telles que le Zero Trust et l'IA appliquée à la cybersécurité, pour anticiper les menaces émergentes.

- Le développement actif de la coopération public-privé, notamment via des plateformes nationales de partage d'information et des incitations à l'investissement.

Par ailleurs, l'étude met en lumière des opportunités économiques concrètes pour le Royaume, à travers la création de services spécialisés en Forensic & Incident Response, de MSSP dédiés aux PME, de solutions Cloud sécurisées, ainsi que de centres de formation certifiés. Ces créneaux porteurs, soutenus par un cadre institutionnel en pleine structuration (Stratégie Nationale Cybersécurité 2030, Digital Morocco 2030), peuvent faire du Maroc un hub régional de cybersécurité à haute valeur ajoutée.

Enfin, la recherche se distingue par sa contribution originale, en dépassant les approches techniques traditionnelles pour proposer une lecture stratégique et managériale de la cybersécurité. Elle fournit un cadre conceptuel et opérationnel novateur, susceptible d'inspirer les politiques publiques, de guider les investisseurs et de structurer les démarches des entreprises marocaines vers une cybersécurité intégrée, résiliente et compétitive à l'horizon 2030.

## ANNEXE : PRINCIPALES CARACTERISTIQUES DE L'ECHANTILLON

### 1. Caractéristiques du profil des répondants

- Fonction du répondant :
  - Professionnel non-IT (Cadre, Manager, Directeur…) : **77%**
  - Professionnel IT (DSI, RSSI, Responsable IT, Consultant IT…) : **23%**
- Taille de l'organisation (effectif) :
  - Plus de 500 employés : **48%**
  - 50 à 200 employés : **21%**
  - 200 à 500 employés : **11%**
  - Moins de 50 employés : **20%**
- Chiffre d'affaires annuel estimé (en USD) :
  - Plus de 50 millions : **46%**
  - 100 000 à 1 million :**12%**
  - 10 à 50 millions : **17%**
  - Moins de 100 000 : **10%**
  - 1 à 10 millions : **15%**
- Type d'organisation :
  - Privée : **75%**
  - Publique : **18%**
  - Semi-Publique : **7%**
- Secteur d'activité :
  - Industrie : **24%**
  - Startup/PME : **7%**
  - Technologie/IT : **18%**
  - Construction : **5%**
  - Services Publiques : **15%**
  - Commerce/Retail : **4%**
  - Finance : **14%**
  - Autres : **12%**

### 2. Culture organisationnelle en cybersécurité

- Répartition des niveaux de maturité
  - Débutant : **45%**
  - Avancé :**17%**
  - Intermédiaire : **38%**
- Définition claire de la cybersécurité ?
  - Oui, elle est clairement définie et communiquée : **42%**
  - Oui, mais elle n'est pas formalisée : **25%**
  - Non, elle n'est pas clairement définie : **33%**
- Campagnes de sensibilisation ?
  - Oui : **56%**
  - Non : **43%**
  - Je ne sais pas : **1%**

- Compréhension du rôle des employés ?
  - Oui, pleinement : **22%**
  - Oui, partiellement : **51%**
  - Non : **27%**
- Implication de la direction Générale
  - Oui, très impliquée : **33%**
  - Modérément impliquée : **20%**
  - Peu ou pas impliquée : **27%**
  - Je ne sais pas : **20%**
- Sensibilisation aux menaces émergeantes
  - Oui, systématiquement : **38%**
  - Oui, mais de manière irrégulière : **35%**
  - Non : **27%**

**3. Connaissance et adoption des solutions techniques**

- Alignement des solutions :
  - SIEM (Security Information and Event Management) : **57%**
  - MFA (Authentification Multi-Facteurs) : **52%**
  - EDR (Endpoint Detection & Response) : **48%**
  - DLP (Data Loss Prevention) : **41%**
- Utilisation de cadres/normes en cybersécurité :
  - **57%** des entreprises déclarent suivre les recommandations de l'ISO 27001.
  - **45%** affirment être en alignement partiel avec le cadre NIST CSF.
  - Les PME semblent moins impliquées dans ces démarches par rapport aux grandes entreprises.
- Maturité par rapport au RGPD :
  - Très avancée : **3%**
  - Avancée : **22%**
  - Moyenne : **23%**
  - Faible : **23%**
  - Je ne sais pas : **29%**
- Présence de SOC :
  - Oui : **23%**
  - Non : **22%**
  - Je ne sais pas : **55%**

- Technologies innovantes :
    - Oui, activement : **12%**
    - Oui, mais de manière limitée : **9%**
    - Non, pas pour le moment : **31%**
    - Je ne sais pas : **48%**

**4. Organisation et gouvernance de la cybersécurité**

- Structuration organisationnelle :
    - Elle est gérée par le département IT : **33%**
    - Un département dédié existe : **23%**
    - Elle est externalisée : **3%**
    - Il n'y a pas de structure claire : **21%**
    - Je ne sais pas : **20%**
- Supervision par la direction générale :
    - Oui, directement : **31%**
    - Non, déléguée à un responsable spécifique : **24%**
    - Non, aucune supervision directe : **20%**
    - Je ne sais pas : **25%**
- Politiques de gestion des incidents :
    - Oui, elle est documentée et appliquée : **16%**
    - Oui, mais elle n'est pas strictement appliquée **: 9%**
    - Non, il n'y a pas de politique formalisée : **40%**
    - Je ne sais pas : **35%**
- Collaboration avec partenaires externes : Une tendance émergente au Maroc vers la collaboration accrue avec des partenaires spécialisés pour compenser le manque de compétences internes. Mais cela reste une minorité d'organisations qui collabore activement avec des partenaires externes (CERT, fournisseurs spécialisés), indiquant un potentiel inexploité pour renforcer leur cybersécurité.

**5. Perception de la valeur ajoutée de la cybersécurité**

- Perception Générale :
    - Un investissement stratégique : **41%**
    - Une nécessité réglementaire : **21%**
    - Un coût inévitable : **26%**
    - Aucune idée : **12%**

- Satisfaction des solutions déployées :
  - Oui, j'en suis satisfait : **45%**
  - Oui, mais il manque des fonctionnalités : **20%**
  - Non, pas vraiment : **28%**
  - Je ne sais pas : **7%**
- Perception de l'investissement suffisant en cybersécurité :
  - Oui : **39%**
  - Non : **55%**
  - Je ne sais pas : **6%**
- Contribution aux résultats financiers :
  - Oui, de manière significative : **19%**
  - Oui, mais de manière limitée : **15%**
  - Non : **31%**
  - Je ne sais pas : **35%**
- Mesure du ROI :
  - Oui, de manière régulière : **6%**
  - Oui, mais de manière informelle : **4%**
  - Non : **41%**
  - Je ne sais pas : **49%**

## BIBLIOGRAPHIE


- **ANSSI. (2022).** Le Campus Cyber. https://cyber.gouv.fr/le-campus-cyber
- **AUSIM. (2024).** Ausimètre de la cybersécurité au Maroc (Version 1.5). https://ausimaroc.com/wp-content/uploads/2024/02/Version-1.5-Ausimetre-de-la-Cybersecurite-au-Maroc.pdf
- **Bennani, A.-E. (2025).** L'IA générative : entre domination américaine et alternatives européennes, une ouverture pour le Maroc grâce à DeepSeek. L'Opinion. https://www.lopinion.ma/L-IA-Generative-Entre-Domination-Americaine-et-Alternatives-Europeennes-une-Ouverture-pour-le-Maroc-grace-a-DeepSeek_a63199.html
- **CIGREF. (2023).** Rapport d'orientation stratégique 2023 : 10 ruptures à l'horizon 2030-2040. https://www.cigref.fr/wp/wp-content/uploads/2023/10/Rapport-dOrientation-Strategique-du-Cigref-CIGREF2023-WEB-FINAL.pdf
- **DGSSI. (2023).** Stratégie nationale de cybersécurité 2030. https://www.dgssi.gov.ma/sites/default/files/publications/pdf/2023-12/strategie_nationale_de_cybersecurite_2030.pdf
- **Gartner. (2023).** Gartner identifies the top cybersecurity trends for 2023. https://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023
- **IBM Security & Ponemon Institute. (2024).** Rapport 2024 sur le coût d'une violation de données. https://www.ibm.com/fr-fr/reports/data-breach
- **InCyber. (2024).** Baromètre de l'investissement en cybersécurité 2024 (5e éd.). https://incyber.org/article/barometre-de-linvestissement-2024/
- **Kenya Ministry of ICT. (2025).** Kenya National AI Strategy (draft). https://ict.go.ke/sites/default/files/2025-01/Kenya%20National%20AI%20Strategy%20%28Draft%29%20for%20Public%20Validatin%20%20%5B14-01-2025%5D.pdf
- **Ministère de la Transition Numérique et de la Réforme de l'Administration. (2024).** La vision éclairée de Sa Majesté le Roi Mohammed VI place le numérique au centre des priorités nationales. https://www.mmsp.gov.ma/fr/actualites/la-vision-%C3%A9clair%C3%A9e-de-sa-majest%C3%A9-le-roi-mohammed-vi-que-dieu-le-glorifie-plac%C3%A9-le-num%C3%A9rique-au-centre-des-priorit%C3%A9s-nationales

- **Ronzaud, L. (2020).** « E-Estonie » : le « nation-branding » numérique comme stratégie internationale d'influence et d'attractivité. Hérodote, 177-178(2), 267-280. https://shs.cairn.info/revue-herodote-2020-2-page-267
- **Senhaji, F. (2025).** Cybercriminalité : un grand groupe victime d'un vol de données sensibles. Le 360. https://fr.le360.ma/societe/cybercriminalite-un-grand-groupe-victime-dun-vol-de-donnees-sensibles_WZFCIPAMUJCXPG6CPZ5GYF3H7M/
- **UAE World Government Summit. (2023).** AI : A roadmap for governments. https://www.worldgovernmentssummit.org/observer/reports/detail/ai-a-roadmap-for-governments
- **U.S. NIST. (2016).** Baldrige Cybersecurity Excellence Program – Overview (presentation). https://csrc.nist.gov/Presentations/2016/Baldrige-Cybersecurity-Excellence-Program-Overview

## GLOSSAIRE

**ANSSI :** Agence Nationale de la Sécurité des Systèmes d'Information, autorité française chargée de la cybersécurité nationale.

**Audit Forensique (Cyber Forensics) :** Processus d'investigation numérique visant à identifier, préserver, analyser et présenter les preuves issues d'incidents de cybersécurité.

**AUSIM :** Association des Utilisateurs des Systèmes d'Information au Maroc.

**CERT :** Computer Emergency Response Team.

**CIGREF :** Club Informatique des Grandes Entreprises Françaises.

**CISO (RSSI) :** Chief Information Security Officer ou Responsable de la Sécurité des Systèmes d'Information.

**CMMI-S :** Capability Maturity Model Integration for Security.

**DGSSI :** Direction Générale de la Sécurité des Systèmes d'Information, entité marocaine chargée de coordonner les actions nationales en matière de cybersécurité.

**DLP :** Data Loss Prevention.

**ISO 27001 :** Norme internationale définissant les exigences d'un Système de Management de la Sécurité de l'Information (SMSI).

**MSSP :** Managed Security Service Provider, fournisseur externe proposant des services de cybersécurité gérés et externalisés pour les organisations.

**NIST CSF :** National Institute of Standards and Technology Cybersecurity Framework.

**PCA/PRA :** Plan de Continuité d'Activité / Plan de Reprise d'Activité.

**Phishing :** Technique frauduleuse visant à obtenir des informations sensibles (identifiants, mots de passe) par le biais de messages trompeurs.

**Ransomware :** Logiciel malveillant cryptant les données d'une victime et exigeant une rançon pour leur restitution.

**RGPD (GDPR) :** Règlement Général sur la Protection des Données.

**SOC :** Security Operations Center.

**Security by Design :** Intégration proactive de la cybersécurité dès la conception des produits, services ou systèmes informatiques.