

# Cybersécurité : Développer un Etat D'esprit Digital : Cas de la Société Philips Healthcare

## Cybersecurity: Developing a digital mindset: Philips healthcare

**Travail à faire:** Etablir l'étude financière relative au business plan "Bilan prévisionnel" : Tableau des investissements, Plan de financement initial, CPC « prévisionnel », Tableaux des Flux de Trésorerie « CAF et variation du BFR », Tableau de l'ESG, Bilan prévisionnel simplifié.

Sara OUASSOU, (Maitre de conférences chercheur)

*Laboratoire : LURIGOR*

*Université Mohammed Premier : FSJES-OUJDA, Morocco*

[ouassou.sara@ump.ac.ma](mailto:ouassou.sara@ump.ac.ma)

### Résumé

La cybersécurité est l'application de technologies, de processus et de mesures de contrôle visant à protéger les systèmes, les réseaux, les programmes, les dispositifs et les données contre les cyberattaques. Selon [13] son objectif est celui de protéger les réseaux et les systèmes informatiques connectés contre les événements compromettant leur intégrité et interférant avec les droits de propriété, entraînant ainsi une certaine forme de perte.

Cependant, la cybersécurité n'est pas uniquement une affaire d'experts techniques, mais une composante intégrée de l'état d'esprit digital collectif, essentiel pour bâtir une entreprise agile, innovante et sécurisée. Cela dit, l'état d'esprit digital est un ensemble d'attitudes et de comportements qui permettent de percevoir comment les données, les algorithmes et l'IA ouvrent de nouvelles perspectives.

Cette étude vise à explorer comment, l'état d'esprit digital impacte les structures organisationnelles, les rôles professionnels, les compétences des individus et les besoins des clients qui évoluent en permanence, en prenant comme exemple la société de services de santé Philips qui a récemment fait évoluer sa compétence principale, passant de la fourniture de produits de santé à la proposition de solutions numériques. Pour accompagner ses employés dans cette transition, elle a dû créer un environnement d'apprentissage continu.

Cette étude a démontré que la réussite d'une transformation digitale repose sur la capacité de l'organisation à fusionner la vision stratégique, l'accompagnement humain et la culture de l'adaptabilité.

**Mots clés :** Cybersécurité, Etat d'esprit Digital, intelligence artificielle, Technologie.

### *Abstract*

Cybersecurity is the application of technologies, processes, and control measures aimed at protecting systems, networks, programs, devices, and data from cyberattacks. According to [13], its objective is to protect connected IT systems and networks from events that compromise their integrity and interfere with property rights, thus leading to various forms of loss.

However, cybersecurity is not solely the responsibility of technical experts; it is an integral part of the collective digital mindset, which is essential to building an agile, innovative, and secure company. That said, the digital mindset refers to a set of attitudes and behaviors that allow individuals to perceive how data, algorithms, and AI open up new opportunities. This study aims to explore how the digital mindset impacts organizational structures, job roles, individual competencies, and customer needs, all of which are constantly evolving. It takes as a case study the health services company Philips, which recently shifted its core competency from providing health products to delivering digital solutions.

To support its employees through this transition, Philips had to create a continuous learning environment.

This study has shown that the success of a digital transformation relies on the organization's ability to merge strategic vision, human support, and a culture of adaptability.

**Keywords:** Cybersecurity, Digital Mindset, Artificial Intelligence, Technology

### I. INTRODUCTION

À l'ère de la transformation digitale, la dépendance graduelle des entreprises aux technologies connectées les expose davantage aux risques liés aux cyberattaques. Selon [15], La cybersécurité ne se limite plus à une approche purement technologique, elle est devenue un enjeu stratégique transversal exigeant une gouvernance intégrée, une approche participative et une culture de sécurité partagée. En effet, les cyberattaques ciblent non seulement les infrastructures techniques, mais également les facteurs humains et les failles organisationnels, notamment le manque de formation et les déficits de sensibilisation au sein des organisations. [11]

La cybersécurité désigne l'ensemble des mesures techniques, organisationnelles et humaines mis en œuvre pour protéger les systèmes d'information et préserver leur confidentialité, intégrité et la disponibilité des données (ENISA, 2020). Elle implique une responsabilité collective qui engage l'ensemble des membres de l'organisation pour adopter des pratiques et des réflexes de cybersécurité. Dans cette perspective, selon Tsedal Neeley & Paul Leonardi (2023), un état d'esprit digital se traduit par un ensemble d'attitudes et de comportements qui permettent aux organisations et aux individus de percevoir comment les algorithmes, les données et l'intelligence artificielle ouvrent de nouvelles perspectives, et présentent une trajectoire de réussite dans un écosystème économique et professionnel de plus en plus façonné par des technologies intelligentes et intensives en données.

L'objectif de cet article est d'explorer et d'analyser comment la mise en place d'un état d'esprit digital peut consolider la posture de cybersécurité dans une organisation en plein processus de transformation. Cette étude s'attache plus particulièrement à présenter les mécanismes de mise en place d'un état d'esprit digital et son effet sur la structure interne, le développement des compétences des employés, la gestion des risques numériques et la relation client. Cette étude s'appuie sur la société Philips Healthcare, qui a opéré une transition stratégique d'un modèle orienté produits médicaux à une stratégie basée sur l'offre des solutions numériques intégrées. Cette

transition favorisée par la mise en place d'un environnement d'apprentissage continu, basé sur l'intelligence artificielle via la plateforme Cornerstone on demand.

## II. FONDEMENTS THÉORIQUES : CYBERSÉCURITÉ ET ÉTAT D'ESPRIT DIGITAL COMME LEVIERS DE TRANSFORMATION

La cybersécurité est l'application de technologies, de processus et de mesures de contrôle visant à protéger les systèmes, les réseaux, les programmes, les dispositifs et les données contre les cyberattaques. Cependant, avec l'accélération de la digitalisation des structures organisationnelles, La cybersécurité dépasse désormais le cadre purement technique pour devenir une composante stratégique intégrée aux dynamiques de gouvernance et d'innovation.

Dans ce contexte, Dans ce contexte, l'état d'esprit digital (ou digital mindset) émerge comme un levier essentiel favorisant l'apprentissage continu, l'agilité et l'appropriation des outils digitaux, le digital mindset contribue à renforcer la résilience organisationnelle face aux cyberattaques.

### A. Définition et Evolution de la Cybersécurité

À l'ère de la transformation numérique, la cybersécurité présente un enjeu stratégique majeur pour les organisations publiques et privées. Loin d'être un concept figé, elle a connu une transformation significative, tant sur le plan conceptuel qu'opérationnel. Son évolution témoigne de l'adaptation progressive des entreprises aux nouvelles formes de menaces, liées aux changements technologiques et à l'interconnexion croissante des systèmes d'information, exigeant la mise en place d'une approche de sécurité numérique.

Les premiers développements de l'informatique en réseau ont connu l'émergence de la cybersécurité. Dès les années 1970, les préoccupations sécuritaires se focalisent principalement sur la protection de la confidentialité, l'intégrité et la disponibilité des données [1]. À cette époque, la sécurité était alors envisagée comme une réponse technique aux tentatives d'intrusion, dans des environnements restreints tels que les réseaux militaires ou des systèmes fermés, sans réelle prise en compte des enjeux humains ou organisationnels.

L'essor des technologies de l'information et l'ouverture d'Internet au grand public dans les années 1990, ont révélé de nouvelles vulnérabilités dans les infrastructures numériques. Cela dit, les premières cyberattaques ont révélé les limites des approches traditionnelles de sécurité. À partir des années 2000, la multiplication des malwares, ransomwares et des failles logicielles a élargi le périmètre de la cybersécurité, qui ne se limite plus à la protection des machines mais qui s'étend à la protection des données personnelles, des processus métiers critiques et de l'image des organisations.

Dans le but de dépasser les approches classiques de la cybersécurité, [13] propose une définition intégrée qui articule dimensions technologiques, organisationnelles et humaines, il définit la cybersécurité comme : « l'ensemble des pratiques, politiques, outils technologiques, structures organisationnelles et comportements humains visant à prévenir, détecter, répondre et se remettre des incidents numériques. » Cette approche souligne l'importance de la responsabilité partagée au sein des organisations, où chaque membre de l'organisation, du décideur au collaborateur, joue un rôle essentiel dans la chaîne de sécurité.

Ce glissement sémantique illustre un changement de paradigme : la cybersécurité n'est plus uniquement l'affaire des services IT, mais s'impose désormais comme un enjeu transversal au centre de la gouvernance stratégique des organisations. Elle s'inscrit au croisement des dynamiques d'innovation, des impératifs de conformité réglementaire (notamment le Règlement général sur la protection des données – RGPD – en Europe), des dispositifs de continuité d'activité et des mécanismes de gestion des crises.

Comme l'indique l'International Journal of Information Security (2023), l'un des tournants majeurs observés au cours de la dernière décennie, concerne le passage du concept de cybersécurité à celui de cyber résilience. En effet, la cyber résilience se présente dans l'aptitude d'une entreprise à anticiper les menaces numériques, et à en limiter l'impact. Elle implique une posture proactive, fondée sur la culture de l'apprentissage continu, l'intelligence collective et l'intégration de technologies avancées comme l'intelligence artificielle et l'analyse comportementale.

Face à ces défis, de nouvelles tendances structurantes émergent : sécurité "by design", automatisation de la détection, l'intégration de la cybersécurité dans les modalités de travail à distance et la formation des employés comme première ligne de défense. Cette dernière mesure rejoint la nécessité de mise en place d'un état d'esprit digital, fondé sur l'agilité, la responsabilisation et la compréhension des enjeux numériques.

#### *B. Définition d'Etat d'Esprit Digital*

Le concept de mindset est apparu dans la psychologie positive, notamment chez Dweck (2017), qui le définit comme un ensemble de connaissances et de schémas cognitifs acquises par l'expérience et mobilisées lors d'un processus d'absorption, de traitement et d'interprétation de l'information.

En effet, dans des environnements organisationnels marqués par une évolution rapide, ces schémas mentaux influencent la perception et la capacité des individus à répondre à la transformation numérique. Ainsi, le digital mindset s'impose comme une posture cognitive essentielle pour accompagner la transformation digitale de l'entreprise. [2]

D'après [5], le digital mindset se présente comme un ensemble de dispositions personnelles et comportementale qui structurent la pensée, le ressenti et l'action dans des contextes de transformation numérique. Ces dispositions n'impliquent pas des réponses comportementales fixes, mais créent une prédisposition probable à agir face aux changements, selon les influences de l'environnement et les dynamiques d'apprentissage.

De surcroît, le digital mindset ne se réduit pas à une expertise technique, mais reflète un état mental dynamique, caractérisé par l'exposition à l'innovation et une démarche d'apprentissage continu. [17]

Ce développement s'inscrit dans un processus fluide et progressif, oscillant entre deux extrêmes : un état d'esprit analogique ou traditionnel, et un état d'esprit digital pleinement mature [8].

L'état d'esprit analogique est caractérisé par un attachement aux structures connues. Par ailleurs, les individus tentent à éviter ou limiter l'usage des technologies, ne manifestent pas un intérêt pour l'innovation, et adoptent les outils digitaux uniquement sous contrainte.

À l'opposé, l'état d'esprit digital mature se distingue par une envie proactive à explorer et intégrer les nouvelles technologies, appuyée par une volonté constante de mise à jour et de dépassement des défis technologiques.

Par ailleurs, afin d'opérationnaliser ce concept, la littérature récente propose de le structurer autour de trois profils comportementaux fondamentaux, tels que définis par l'échelle (Clave Digital Mindset Scale) :

Open Minded: caractérisé par une ouverture d'esprit, curiosité technologique, agilité analytique ainsi qu'une capacité d'apprentissage rapide. Les individus de ce profil font preuve d'adaptation rapide à un environnement numérique en constante évolution [3]

Transformer : défini par l'orientation vers l'innovation, la capacité à initier des changements, le pilotage des expériences ainsi que l'application des approches disruptives.

Entrepreneur : caractérisé par un esprit proactif, une orientation vers l'action, prise de risque calculée et la capacité à conduire des projets digitaux.

Ces profils offrent un cadre d'analyse pour positionner les individus sur un continuum de maturité numérique, facilitant ainsi l'élaboration de stratégies pédagogiques ou de gestion des ressources humaines selon leur profil.

Selon [16] le digital mindset est considéré comme un levier intangible mais fondamental de la réussite organisationnelle. Même lors de la présence des ressources technologiques suffisantes, l'absence d'état d'esprit digital partagé entre dirigeants et employés, peut conduire à l'échec de la transformation digitale.

Un tel mindset s'avère essentiel à tous les niveaux de l'organisation, leadership compris, pour assurer la conduite efficace des initiatives de digitalisation durables. Il favorise l'intelligence collective, encourage la créativité, l'initiative entrepreneuriale, et renforce une culture d'apprentissage alignée sur les défis du numérique [12]

### III. L'ÉTAT D'ESPRIT DIGITAL COMME LEVIER ORGANISATIONNEL

Adopter un état d'esprit digital ne signifie pas devenir expert en technologie, mais plutôt saisir comment la technologie façonne le monde dans lequel nous vivons. Il s'agit de comprendre comment elle change les attentes des clients, et comment elle reconfigure les modèles d'affaires et redéfinit les modes de création de valeur au sein des entreprises.

L'adoption d'un état d'esprit digital exige que nous reconnaissons que nous évoluons dans un monde de plus en plus structuré par les données, les algorithmes et l'intelligence artificielle. Il ne s'agit pas seulement de maîtriser des outils numériques, mais de comprendre les capacités qu'ils rendent possibles, et d'identifier de nouvelles opportunités là où d'autres ne voient que des défis.

Adopter un tel état d'esprit revient à adopter une posture agile, fondée sur :

Une curiosité face aux nouvelles technologies.

Disposition à l'expérimentation et l'apprentissage par les erreurs.

L'ouverture aux changements dans les processus et dans les modèles économiques.

La vigilance éthique de l'utilisation des données et de l'IA.

Cela implique également l'adhésion à une culture d'apprentissage continu, l'acceptation de l'incertitude et la volonté de repenser les méthodes de travail traditionnelles.

Dans ce sens, développer un état d'esprit orienté IA ne signifie pas d'être data scientist ou ingénieur en apprentissage automatique (machine Learning). Il s'agit plutôt de comprendre ce que l'IA peut et ne peut pas faire, afin de pouvoir contribuer de manière informée aux décisions stratégiques liées à son utilisation.

Le développement d'un état d'esprit IA repose sur plusieurs principes fondamentaux :

Compréhension des capacités de l'IA : Il est primordial de savoir ce que les technologies d'IA permettent dans un contexte professionnel, comme l'automatisation des tâches répétitives, l'analyse d'énormes volumes de données, ou l'amélioration de la prise de décision.

Saisir les limites de l'IA : L'IA ne constitue ni un miracle ni un système infallible. Elle peut amplifier les biais, générer des résultats erronés ou difficilement interprétables, et doit toujours être utilisée avec un discernement rigoureux.

Collaborer avec l'IA : interagir efficacement avec des systèmes d'IA signifie une redéfinition des rôles humains, il s'agit de déléguer certaines tâches aux machines tout en valorisant la compétence humaine là où la créativité, le jugement ou l'intuition stratégique sont cruciaux.

Savoir poser les bonnes questions : Un état d'esprit orienté IA requiert la capacité d'interroger intelligemment les systèmes : quelles données ont été exploitées ? Quels sont les risques d'erreur ? Qui assume la responsabilité des résultats ?

Adopter une posture éthique : Il est essentiel d'être conscient des implications sociales, juridiques et éthiques liées à l'usage de l'IA, notamment en matière de vie privée, d'équité et de transparence.

En résumé, développer un état d'esprit IA revient à adopter une posture critique, responsable et collaborative, permettant de tirer profit de l'IA tout en maîtrisant les risques.

#### IV. ÉTUDE DE CAS : PHILIPS

L'acquisition de nouvelles compétences technologiques est indispensable à la transformation digitale, mais cela ne suffit pas si les employés ne sont pas assez motivés à mobiliser ces compétences pour créer de nouvelles opportunités. Cela exige le développement d'un état d'esprit digital.

En effet, les psychologues définissent le mindset comme une manière de penser qui influence notre manière de percevoir, de ressentir et d'agir. Ainsi, l'état d'esprit digital correspond à un ensemble d'attitudes et de comportements qui permettent aux individus et aux organisations de percevoir, ressentir et agir face aux innovations technologiques, et comprendre également comment l'intelligence artificielle permet d'ouvrir de nouvelles perspectives et tracer une voie vers le succès dans un environnement économique de plus en plus dominé par les technologies intelligentes et les données massives. [14]

En vue de cela, développer un état d'esprit digital requiert des efforts significatifs, mais ceux-ci en valent la peine. L'expérience montre que les collaborateurs qui adoptent cette posture réussissent mieux dans leur travail, déclarent un niveau de satisfaction professionnelle plus élevé, sont plus susceptibles d'obtenir des promotions, et acquièrent des compétences transférables valorisées dans un contexte de mobilité professionnelle. Quant aux leaders dotés de cet état d'esprit, ils se révèlent plus aptes à orienter leur organisation vers la réussite et à contribuer à construire une main-

d'œuvre résiliente. Les entreprises qui en font un levier stratégique réagissent plus rapidement aux évolutions du marché et sont mieux positionnées pour exploiter de nouvelles opportunités.

À l'instar de toute démarche de changement, la transition digitale se heurte fréquemment à des résistances organisationnelles, et les erreurs de la première phase sont inévitables. Selon [14], L'expérience montre que les entreprises obtiennent de meilleurs résultats lorsqu'elles concentrent leurs efforts autour de deux leviers stratégiques essentiels:

La préparation des individus à une nouvelle culture organisationnelle digitale.

La conception et l'alignement des systèmes et processus avec cette dynamique.

Dans cette section, nous allons présenter les principes fondamentaux de cet ambitieux chantier, à partir de l'expérience tirée de cas concrets comme l'entreprise Philips healthcare. Cette entreprise qui a offert une feuille de route précieuse dans le but de développer un état d'esprit digital au sein des talents existants et assurer l'alignement des systèmes avec les compétences numériques digitales.

#### A. Mise en Place d'une Culture d'Apprentissage Continu

L'entreprise de services de Philips healthcare a récemment opéré une transition stratégique en faisant évoluer son cœur de métier : elle est passée de la fourniture de produits médicaux à l'offre de solutions numériques. Pour soutenir ses collaborateurs dans cette transformation, elle a instauré un environnement d'apprentissage continu.



Fig. 1 : Services offerts par Philips Healthcare :

Source : [18]

À cet effet, Philips a conclu un partenariat avec Cornerstone OnDemand, un fournisseur de solutions cloud spécialisé dans la formation et la gestion des ressources humaines, afin de mettre en place une infrastructure pilotée par l'intelligence artificielle, capable de s'ajuster aux besoins et au rythme d'apprentissage de chaque utilisateur. [14]

Les employés ont la possibilité de partager des « playlists » de modules de formation personnalisés avec leurs collègues, à l'image des listes de lecture sur les plateformes de streaming musical. De plus, la dimension sociale de la plateforme facilite la mise en relation entre les nouveaux arrivants et les collaborateurs expérimentés susceptibles de jouer un rôle de mentorat plus naturel et spontané que celui issu de programmes de jumelage formels.

Cela étant, les dirigeants de Philips, en tant que formateurs dans le programme d'apprentissage continu, mettent l'accent non seulement sur l'acquisition de nouvelles compétences, mais également sur un changement culturel



profond. Ils endossent la responsabilité de l'avenir de leurs équipes, dépassant la simple gestion des tâches, ils partagent également leur expertise, leurs connaissances et leur passion lors des sessions de formation.



Figure 2: Mise en place d'une culture d'apprentissage continu

L'entreprise recueille et exploite des données sur l'utilisation de la plateforme par les employés, procède à l'analyse la corrélation entre apprentissage continu et performance, et étudie comment les différents outils favorisent l'apprentissage, parfois de manière inattendue.

Dans cette optique, le développement d'un état d'esprit digital repose largement sur le degré d'appropriation de cette démarche par les collaborateurs. Réfléchir à la manière d'interagir avec ces nouveaux outils, à leur utilisation, et à la façon dont ils peuvent améliorer les performances est un élément clé pour réussir la transformation digitale.

#### B. *L'Accélération de l'Adoption*

La transformation digitale est souvent radicale et nécessite une remise en question des valeurs, des normes, des attitudes et des comportements collectifs. Face à l'ampleur de cette démarche, il est primordiale de l'amorcer par un geste fort : une initiative symbolique qui attire l'attention et fait comprendre à tous les collaborateurs de l'entreprise qu'un nouveau cap doit être engagé. Parmi ces actions marquantes, on peut citer une restructuration majeure, une acquisition, une réaffectation des ressources, la nomination d'un responsable de la transformation digitale rattaché directement à la direction générale, ou encore l'annonce du retrait progressif d'un système technologique obsolète.

Bien qu'un geste fort permette lancer une dynamique de changement, cela ne suffit pas. Cette initiative doit être suivi d'un travail de fond, qui commence par une évaluation du ressenti des employés face aux projets de transformation digitale de l'entreprise. Certains peuvent ressentir de l'appréhension face à l'inconnu ; d'autres s'inquiéteront de leur capacité à apprendre et à intégrer les nouvelles technologies dans leur quotidien professionnel. [14]

Ces inquiétudes peuvent concerner aussi bien les fonctions techniques que non techniques. Par ailleurs, certains collaborateurs peuvent également remettre en question cette transformation numérique, que ce soit pour l'entreprise ou pour leur propre poste.



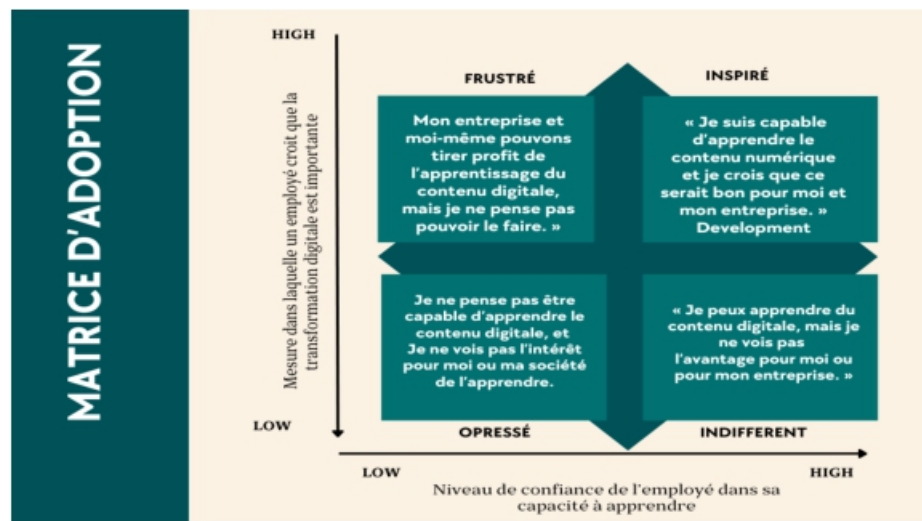


Figure 3 : Matrice d'adoption

Dans ce sens, les managers doivent prendre en compte deux dimensions fondamentales : l'adhésion : c'est-à-dire le degré auquel les individus croient que ce changement apportera des avantages pour eux-mêmes et pour l'organisation et la capacité d'apprentissage, autrement dit, la mesure dans laquelle les personnes se sentent capables et confiantes d'acquérir les nouvelles compétences requises pour répondre aux exigences. Les niveaux d'adoption les plus élevés sont atteints lorsque les employés sont motivés à développer leurs compétences parce qu'ils adhèrent pleinement à la stratégie de transformation et se sentent capables de contribuer activement à sa réalisation.

#### V. CONCLUSION

La transformation numérique ne se limite pas à l'adoption de technologies innovantes ; elle repose sur la réinvention des valeurs en profondeur, des comportements et des modes de collaboration. L'exemple de la société Philips Healthcare montre qu'une telle transformation nécessite bien plus qu'un simple virage technologique : elle repose sur la mise en place d'un environnement d'apprentissage continu, soutenu par un leadership engagé et une stratégie bien ficelée.

Dans ce contexte, il est essentiel de considérer deux dimensions clés : l'adhésion des collaborateurs, c'est-à-dire leur conviction que la transformation leur sera bénéfique, et leur capacité à acquérir les compétences nécessaires pour y contribuer. Comme le montre la matrice d'adoption, c'est à la croisée de ces deux axes que naissent les comportements les plus constructifs. Le rôle des leaders est alors d'évaluer où se situent leurs équipes au sein de cette matrice d'adoption, entre frustration, inspiration, indifférence ou oppression et également d'accompagner chacun dans son développement vers un engagement actif et éclairé.

En somme, la réussite d'une transformation digitale repose sur la capacité de l'organisation à fusionner la vision stratégique, l'accompagnement humain et la culture de l'adaptabilité.

Enfin, il ne faut pas négliger l'une des dimensions les plus critiques de la transformation digitale qu'est la cybersécurité. Le plus petit des appareils connectés ou une simple erreur humaine peut suffire à paralyser tout un hôpital. Il est donc impératif de déployer une stratégie de cybersécurité globale comme l'offre l'entreprise Philips

healthcare grâce à sa transformation digitale, qui prenne en compte à la fois les dispositifs technologiques, les systèmes logiciels et, surtout, les comportements humains au sein des organisations.

#### VI. RÉFÉRENCES BIBLIOGRAPHIQUES :

- [1] Alam, S. (2022). Cybersecurity: Past, Present and Future.
- [2] Bai-Ngern, S., & Tubtiang, A. (2020). Digital Mindset and Organizational Readiness for Digital Transformation. *Revista de Administração Mackenzie*, 21(1).
- [3] Benke, I. (2013). Digitaler Mindset: Wie Unternehmen und Mitarbeiter den digitalen Wandel erfolgreich gestalten. *Zeitschrift für Organisationsentwicklung*, 2, 12–17.
- [4] Brown, M., & Grant, G. (2019). Digital Transformation and the New Challenges of Cybersecurity. *Journal of Information Systems*, 33(2), 15–30.
- [5] Bredendiek, A., & Knorr, J. (2020). What Is a Digital Mindset? 6 Dimensions That Define a Digital Mindset. *MoreThanDigital.info*.
- [6] Bughin, J., Catlin, T., Hirt, M., & Willmott, P. (2019). The Case for Digital Reinvention. McKinsey Global Institute.
- [7] Deloitte. (2021). Digital Mindset: How to Cultivate it Across the Organization. Deloitte Insights.
- [8] Dweck, C. S. (2007). *Mindset: The New Psychology of Success*. Random House.
- [9] Marinos, Louis & Lourenco, Marco. (2020). Main incidents in the EU and worldwide ENISA Threat Landscape.
- [10] Guenoun, A. (2020). *Cybersécurité et résilience numérique des entreprises*. Paris : Dunod.
- [11] Hadnagy, C. (2018) *Social Engineering: The Science of Human Hacking*. 2nd Edition, Wiley.
- [12] Kane, G. C., Palmer, D., Phillips, A. N., Kiron, D., & Buckley, N. (2017). Achieving Digital Maturity. MIT Sloan Management Review.
- [13] Schiliro, F. (2023). Towards a Contemporary Definition of Cybersecurity. arXiv preprint arXiv:2302.02274.
- [14] Tsedal Neeley & Paul Leonardi, enquête conduite par la Harvard Business Review (2023).
- [15] Von Solms, R. and Van Niekerk, J. (2013) From Information Security to Cyber Security. *Computers & Security*, 38, 97-102.
- [16] Westerman, G., Bonnet, D., & McAfee, A. (2014). *Leading Digital: Turning Technology into Business Transformation*. Harvard Business Review Press.
- [17] White, M. (2019). *The Digital Mindset: What It Really Takes to Thrive in the Age of Data, Algorithms, and AI*. McGraw-Hill.
- [18] [www.philips.fr/healthcare](http://www.philips.fr/healthcare).