Lara MARTIN

Cybermenaces par ingénierie sociale affectant les entreprises : dépistage des risques par un modèle préventif de santé publique appliqué à la cybersécurité ?

Université BORDEAUX MONTAIGNE | Cyber criminalités

Promotion 2024-2025

Résumé : Le facteur humain représente un enjeu et un défi majeur pour la cybersécurité des entreprises en France, notamment sur le cas spécifique des cybermenaces et cyberattaques utilisant l'ingénierie sociale. Chaque année, ce fléau engendre des dommages colossaux, malgré de nombreuses actions préventives pour y faire face. Cette étude cherche une approche différente en tentant de dépister cette forme de cybermenaces, par le biais d'un modèle préventif de santé publique *(Janz & Becker, 1984)* appliqué à la cybersécurité (sur des fondements psychologiques). L'approche méthodologique est exploratoire, mixte à dominance quantitative et elle s'articule en plusieurs étapes dont, la déclinaison du concept, l'élaboration d'un questionnaire, la définition d'échelles de risque, et des indicateurs permettant une vision rapide d'un niveau de vulnérabilité de l'entreprise sur ce type de risque et un profil traçable d'individus (dans l'entreprise) représentants un danger important. Bien que la taille de l'échantillon ne soit pas représentative, les résultats sont très encourageants et laissent envisager d'utiliser ce modèle comme un indicateur évaluant les vulnérabilités des entreprises sur ce type de menace.

Mots-clés : Cybersécurité – Ingénierie sociale – Cybermenaces – Cybercriminalité – Modèle des croyances de santé – Gestion des risques -

Abstract: The human factor represents a major issue and challenge for cybersecurity in France, particularly on the specific case of cyber threats and cyber-attacks using social engineering. Every year, this scourge causes colossal damage, despite numerous preventive actions to deal with it. This study seeks a different approach by attempting to detect this form of cyber-threat, through a preventive public health model (Janz & Becker, 1984) applied to cybersecurity (on psychological foundations). The methodological approach is exploratory, mixed with quantitative dominance and is structured in several stages including the development of the concept, the elaboration of a questionnaire, the definition of risk scales, and indicators allowing a rapid vision of the company's vulnerability to this type of risk and a traceable profile of individuals (in the company) representing a significant danger. Although the sample size is not representative, the results are very encouraging and suggest that this model could be used as an indicator to assess companies' vulnerabilities to this type of threat.

Keywords: Cybersecurity – Social engineering – Cyber threats – Cybercrime – Health beliefs model Risk management

INTRODUCTION & PROBLEMATIQUE

Les failles humaines représentent un enjeu et un défi majeur dans la protection et la résilience des entreprises face aux cyberattaques utilisant l'ingénierie sociale. Chaque année, les dommages nationaux et internationaux, qu'ils soient économiques, financiers, informatiques et sociaux sont colossaux. Malgré de nombreuses actions pour se prémunir, le fléau persiste et les résultats restent globalement très mitigés. Nombreuses de ces approches reposent majoritairement sur le postulat de départ : la victime potentielle a une connaissance du risque encouru, de ces répercussions, et une motivation pour y faire face. Cependant, une approche très différente se basant sur « *Modèle de croyances relatives à la santé* », Health Beliefs Model (Janz & Becker, 1984) mérite d'être approfondie. Ce modèle issu de la psychologie de la santé, est élaboré dans un premier temps, dans les années 1950 et enrichi plus tard par de nombreux chercheurs. Il a été développé dans le cadre de la prévention des risques en santé publique liée aux infections ou aux maladies de types asymptomatiques. Il permettait d'analyser la perception de ces risques par leurs potentielles victimes, afin qu'elles puissent prendre conscience des dangers encourus, de les encourager à limiter les comportements à risques, et d'adopter des comportements de protection. Ce modèle décliné dans le domaine de la cybersécurité, a permis de révéler que le risque perçu, la vulnérabilité perçue, les bénéfices perçus et l'auto-capacité à se protéger sont des facteurs déterminants du comportement des utilisateurs pour se prémunir contre les menaces cyber (Ng & Xu, 2007).

Au regard, de ces résultats, du manque d'indicateurs préventifs sur ce type de vulnérabilités (cybermenaces utilisant l'ingénierie sociale) et de la prolifération virale de cette cybercriminalité touchant les entreprises en France et notamment les TPE-PME, cette recherche se penche sur la possibilité d'utiliser ce modèle pour permettre aux entreprises d'identifier ce type de vulnérabilités, afin qu'elles puissent les intégrer dans leurs approches préventives, pour davantage d'efficacité. La question de recherche se résumant à *« Est-ce que le Modèle des croyances relatives de santé (Janz & Becker, 1984) appliqué à la cybersécurité permet d'identifier des vulnérabilités liées aux cybermenaces utilisant l'ingénierie sociale, touchant les entreprises en France ? »*

Cette étude repose sur certains concepts et théories issus des sciences sociales, de psychologie sociale, psychologie du comportement, de la criminologie, de la cyber-criminologie, de la cybersécurité et du management du risque. Elle examine entre autres, les diverses composantes du *Modèle des croyances relatives de santé* (Janz & Becker, 1984), l'étude « *Etude du comportement des utilisateurs en matière de sécurité informatique à l'aide du modèle des croyances relatives à la santé* » (Ng & Xu, 2007), les diverses méthodes de cybercriminels utilisant l'ingénierie sociale, et l'élaboration d'un indicateur pour dépister ce type de risque.

Le plan de cette étude sera le suivant : la première partie aborde le positionnement théorique et conceptuel employé pour l'étude, suivie d'une partie sur la méthodologie employée pour cette recherche,

puis de la présentation des résultats. La troisième partie examine et analyse les résultats de l'étude, permettant ensuite une discussion et une mise en perspectives des résultats trouvées. Il s'en suit la conclusion, les remerciements, les références bibliographiques et les annexes.

I. POSITIONNEMENT THEORIQUE ET CONCEPTUEL

Cette première partie présente les principaux axes théoriques et conceptuels utilisés pour tenter de répondre à la problématique.

Avant tout, il est utile de préciser « *qu'il n'existe pas de définition universelle acceptée de la cybercriminalité, il s'agit essentiellement d'un acte utilisant les technologies de l'information pour commettre ou faciliter un crime. » (*Service de recherche du Parlement européen, 2024)**.** Cependant, malgré cette définition couvrant un large champ, Europol distingue les cybercrimes dépendants, « *tout crime qui ne peut être commis qu'à l'aide d'ordinateurs, de réseaux informatiques ou d'autres formes de technologies de l'information et de la communication* » et les cybercrimes facilités, « *les crimes traditionnels facilités par Internet, les technologies numériques* » (Service de recherche du Parlement européen, 2024). Cette distinction complexifie les définitions et les classifications des cybermenaces utilisant l'ingénierie sociale (« *une manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes. Remarque : Il s'agit, pour les personnes malveillantes usant de ces méthodes, d'exploiter le facteur humain, qui peut être considéré dans certains cas comme un maillon faible de la sécurité du système d'information* » (ANSSI, 2024), car ce type de cybercriminalité peut en fonction du mode opératoire, jouer sur les deux tableaux. Toutefois, la définition de l'ingénierie sociale de Borkovich et Skovira (2019) est intéressante et elle est privilégiée dans le cadre de cette étude, car même si elle ne mentionne pas les termes « cyber*attaques, cybermenaces utilisant l'ingénierie sociale* », elle intègre le facteur humain, la manipulation psychologique, la sécurité, la cybersécurité et l'infraction à la loi. Cette définition est la suivante « *un vecteur d'attaque qui repose sur l'interaction humaine en manipulant les personnes pour qu'elles enfreignent les protocoles de sécurité normaux et les meilleures pratiques, permettant aux acteurs d'accéder à des systèmes informatiques, des réseaux ou des emplacements physiques à des fins frauduleuses* ».

Après, cet éclaircissement sur les définitions, il est utile d'avoir une vision du panel d'options (non exhaustives) d'attaques qui s'offre aux cybercriminels, des différents leviers psychologiques utilisés par ces acteurs et les différentes méthodes d'influences mobilisées ou mobilisables pour arriver à leurs fins. Le schéma ci-dessous composé des travaux de Siddiqi (2022) et de Jain, Tailang,, Goswami, Dutta, Sankhla, Kumar (2016) permet d'avoir une vision synthétique de la complexité, de la diversité, de l'interconnexion, de la quantité des options d'attaques et des méthodes d'influence pour ce type

d'attaques. Ce schéma témoigne également de l'importance du facteur humain et du facteur cyber dans ces modes opératoires.

EXEMPLES DE TYPES D'ATTAQUES - LEVIERS PSYCHOLOGIQUES UTILISES - METHODES D'INFLUENCES

Exemples de types d'attaques en Ingénierie Sociale et leviers psychologiques utilisés

Phishing : inciter les victimes à divulguer des informations sensibles ou à télécharger des fichiers malveillants par e-mail ou message imitant des entités légitimes. Exemple : hameçonnage ciblé, vocal, par sms, Usurpation d'identité / compromission de messagerie professionnelle

↓

Peur, Urgence, Soumission à l'autorité, curiosité, cupidité, empathie, mémoire associative, faible effort perçu

Scareware : diffuser des messages alarmant incitant à agir dans la précipitation.

↓

Peur, urgence, soumission à l'autorité, ignorance technique, soulagement, biais de confirmation, conformité sociale

Baiting: offrir une récompense pour inciter à agir.

↓

Curiosité, appat du gain, conformité sociale, urgence, envie, faible effort perçu

Quid Pro Quo : promettre une récompense ou un service en échange d'une action ou information.

↓

Réciprocité, conformité sociale, besoin d'aide, empathie, confiance, gratification faible effort perçu,

Pretexting : creation d'un prétexte pour manipuler quelqu'un.

↓

Confiance, soumission à l'autorité, pression sociale, besoin d'aide, effort faible perçu, urgence, légitimité apparente

Tailgating / Piggybacking : suivre une personne autorisée pour accéder à des zones sécurisées.

↓

Politesse, désir de coopérer, conformité sociale, pression du groupe social, conformité à la règle

Reverse Social Engineering : manipuler une victime en créant un problème, puis en offrant une solution.

↓

Besoin d'aide ou vulnérabilité, confiance, autorité, urgence, conformité à la norme sociale

Water Hole : infecter des sites web de confiance pour cibler un groupe spécifique.

↓

Confiance, curiosité, ouverture, curiosité, urgence, normalisation de l'accès à des ressources, conformité sociale

Deepfake : média très réaliste généré par l'IA pour manipuler.

↓

Crédibilité, confiance, autorité perçue, perception de légitimité, effet visuel, normalisation de l'information numérique, influence sociale

Dumpster Diving : chercher des informations dans les poubelles.

↓

Négligence, confiance, routine, non vigilance

Shoulder surfing : lire par dessus l'épaule pour voler de l'information

↓

Négligence, manque de vigilance, confiance, comportement automatique, pression sociale

Méthodes d'Influences

Influence Sociale : groupe d'influence - influence Informative/Influence normative - théorie de l'échange social/ la réciprocité des normes – influence morale/ responsabilité sociale – révélation de soi / création de lien

Persuasion : similarité distraction/Manipulation – curiosité – persuasion par l'autorité/crédibilité

Attitude & Comportement : impression/engagement – théorie de dissonance cognitive – comportement conditionnant une attitude – effet du témoin – rareté / urgence

Confiance et Déception (Trahison) : confiance/relation – trahison/fraude

Langage and Raisonnement : effet de cadre / biais cognitif – complication du processus de pensée

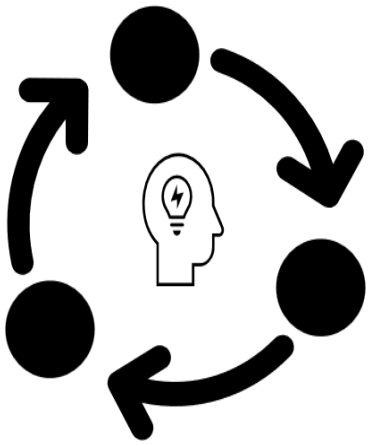
De plus, pour comprendre cette forme de cybermenace, il est nécessaire de comprendre l'humain en tant que système évoluant dans un système en mouvement, interconnecté, où la rationalité et la tangibilité ne sont pas toujours de mises. Le schéma ci-dessous développé pour cette étude permet de visualiser une partie des composantes importantes impliquées dans ces processus, telles que le facteur humain, l'humain connecté, l'environnement de travail et la gestion de la cybersécurité de l'entreprise.

COMPLEXITE DU FACTEUR HUMAIN DANS LES ATTAQUES CYBER UTILISANT L'INGENIERIE SOCIALE TOUCHANT LES ENTREPRISES

Facteur Humain

- Perception
- Attention
- Mémoire
- Emotion
- Langage
- Raisonnement
- Rationalité/Irrationalité
- Décision
- Imagination
- Apprentissage
- Motivation

- Métacognition
- Culture
- Personnalité
- Conditionnement
- Automatisme
- Vicariance
- Comportement à risque
- Variables socio-démographiques
- Etc.



Facteur Humain Connecté

- Impact de l'IT & psychologique
- Impact de l'IT & cognition
- Impact de l'IT & comportement
- Impact de l'IT & neuroscience

- Impact de l'IT & surcharge mentale
- Impact de l'IT excessif des écrans
- Impact de l'IT sur l'Humain
- Impact de la cybersécurité sur l'Humain
- Etc.

Facteur Humain & Environnement de travail

- Culture d'entreprise
- Stress et pression
- Urgence
- Risque
- Niveau de l'utilisation de l'IT
- Données sensibles et gestions des accès
- Données intéressantes à revendre
- Poste occupé
- Culture d'entreprise sensibilisée aux risques cyber et ingénierie sociale
- Culture d'entreprise sensibilisée à la prévention des risques cyber dont ingénierie sociale
- Gestion de l'intangibilité
- Etc.

Facteur Humain & Gestion de la Cybersécurité

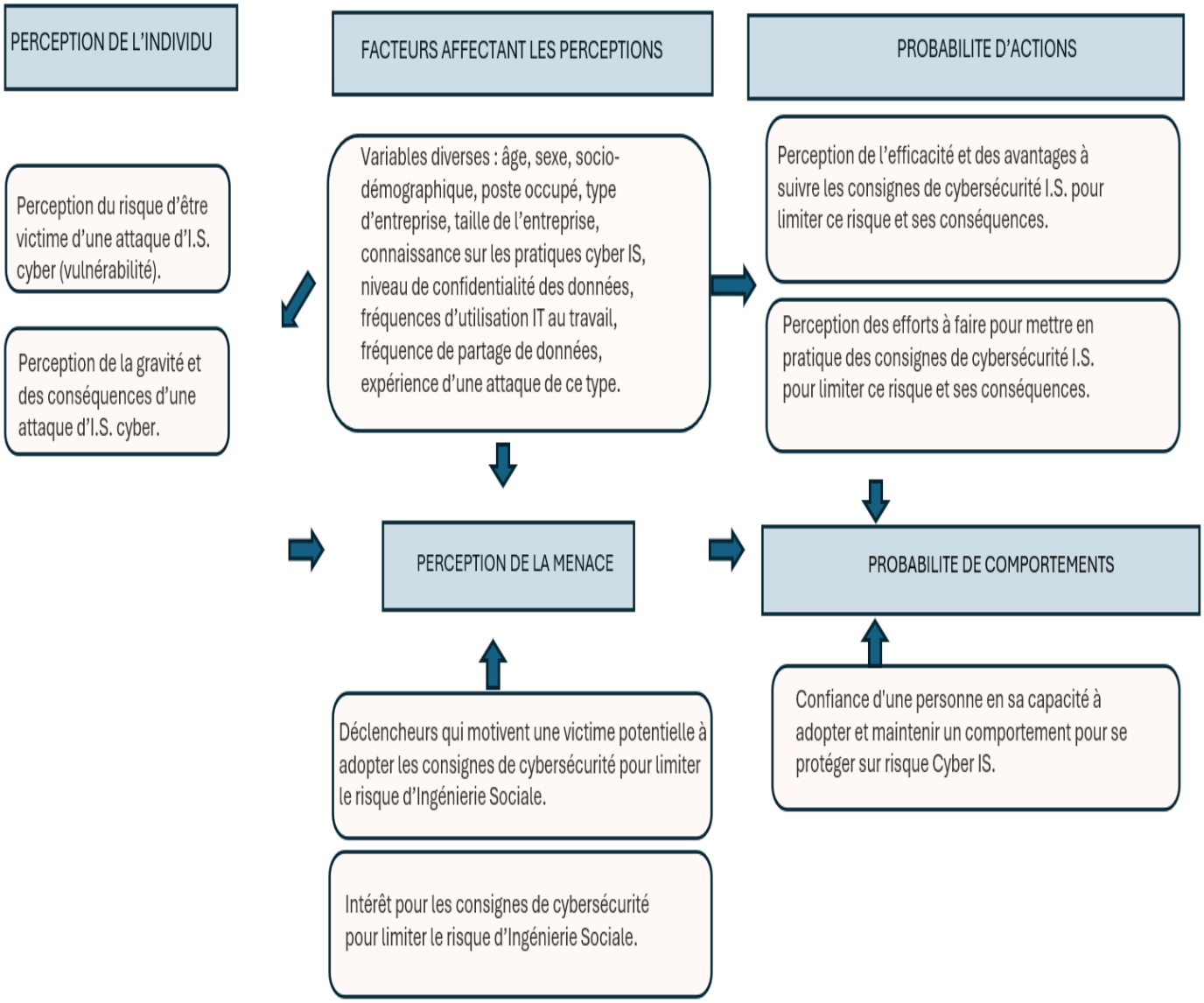
- Gestion de la cybersécurité
- Compétences en matière de cybersécurité
- Sensibilisation à l'ingénierie sociale par les gestionnaires de la cybersécurité
- Mise à niveau des systèmes informatiques
- Gestion du système d'information par des prestataires internes ou externes
- Etc.

Cependant, même si cette étude n'a pas pour vocation (à ce stade) de trouver une solution globale et systémique pour faire face à ce type de cybermenace, ce schéma permet également de comprendre plus facilement les composantes et les dynamiques du « *Modèle des croyances relatives de santé » (*Janz & Becker, 1984) décliné dans cette étude pour détecter les cybermenaces usant d'ingénierie sociale.

Présenté dans l'introduction, le modèle initial a été développé dans un premier temps par Rosenstock dans les années 1950 (Rosenstock, 1966) et complété plus tard par de nombreux chercheurs. Issu de la psychologie cognitive et sociale, il évolue et intègre peu à peu certaines théories motivationnelles, comme la théorie de l'action raisonnée (Fishbein et Ajzen, 1975) se résumant à « *Plus l'intention est grande, plus elle a de chances de se produire*. ». Ce modèle a pour objectif de comprendre pourquoi certains individus adoptent ou non des comportements préventifs, face aux risques de maladies asymptomatiques en fonction de la perception individuelle du risque et des bénéfices à agir. Cette approche se base sur cinq piliers : la perception de l'individu (incluant sa perception du risque, dont sa propre vulnérabilité, et la gravité perçue, dont les conséquences), les facteurs affectant ses perceptions (socio-démographie, etc.), sa perception de la menace (incluant les déclencheurs de motivation, et ses

intérêts pour les consignes pour limiter les risques), la probabilité d'actions de l'individu (au regard des éléments cités, et de sa perception des avantages et efforts à faire pour suivre les consignes pour réduire les risques et les conséquences) et sa probabilité de comportement (en fonction de sa confiance en ses propres capacités pour faire face à la menace). C'est sur ces mêmes piliers que s'est appuyée la recherche « *Etude du comportement des utilisateurs en matière de sécurité informatique à l'aide du modèle des croyances relatives à la santé* » Ng & Xu (2007) permettant de montrer que la vulnérabilité perçue, les bénéfices perçus et l'auto-efficacité sont des facteurs déterminants du comportement de sécurité informatique des utilisateurs.

MODÈLE DE CROYANCES RELATIVES À LA SANTÉ (Janz & Becker, 1984) **ADAPTÉ AUX RISQUES D'ATTAQUES CYBER UTILISANT L'INGENIERIE SOCIALE**



Après cette présentation des principaux axes théoriques et conceptuels, la prochaine partie est dédiée à la méthodologie utilisée pour tenter de répondre à la problématique.

II. METHODOLOGIE

Cette recherche s'inscrit dans une approche exploratoire, mixte à dominance quantitative. Elle s'articule en plusieurs phases.

Premièrement, une déclinaison du modèle *« Modèle des croyances relatives de santé* » (Janz & Becker, 1984) est élaborée pour ce type de cybermenace.

Deuxièmement, un questionnaire est construit pour permettre d'identifier les principales vulnérabilités liées aux cybermenaces utilisant l'ingénierie sociale, en respectant la segmentation des critères importants d*u « Modèle des croyances relatives de santé* » (Janz & Becker, 1984). L'objectif étant d'utiliser ces critères comme des référentiels de vulnérabilités. Le questionnaire est composé de 40 questions. Il est réalisé sur l'outil Microsoft Form. Il faut en moyenne 10 minutes pour répondre. Il est disponible en format papier et par e-mail. Il est destiné à des entreprises basées en France. Dans le cadre de cet article, le questionnaire est envoyé essentiellement à des TPE-PME, car n'ayant pas pour le moment de système d'automatisation de gestion des résultats, les analyses sont traitées via Excell, Microsoft Form, ChatGPT pour des analyses plus poussées.

Avant d'envoyer le premier questionnaire aux entreprises, une première vérification de la segmentation et du contenu du questionnaire est réalisée, en le présentant à des experts en cybersécurité pour avoir leurs commentaires et leurs éventuelles corrections.

Au total 5 entreprises ont répondu à cette étude, et au moment de la rédaction de cet article, le retour de plusieurs entreprises est en attente. Bien que cet échantillon ne soit pas représentatif, il permet de vérifier l'approche et l'élaboration et la mise en place des outils.

Le questionnaire est dans un premier temps envoyé aux dirigeants pour validation des questions et du processus de gestion du questionnaire et des réponses. Les dirigeants sont informés du respect de la confidentialité des données collectées.

Pour garantir une confidentialité des réponses, le nom de l'entreprise et le nom de la personne questionnée ne figurent pas sur le questionnaire. Les entreprises qui acceptent de tester ce questionnaire reçoivent des questionnaires avec un code dédié. Le questionnaire est ensuite envoyé avec un lien renvoyant sur Microsoft Form ou imprimé.

Une fois les réponses reçues, elles sont analysées. Elles sont comptées, puis intégrées dans des tableaux Excel avec différentes échelles évaluant les risques. Ces échelles ont été élaborées spécialement pour l'étude et varient en fonction des critères, ce qui explique qu'en fonction des échelles, les seuils de danger sont différents. Par exemple, pour le premier critère, les valeurs des actions aggravantes (valeurs positives), bénéfiques (valeurs négatives) et les neutres (valeur 0) sont additionnés, puis classés avec le

score total obtenu dans une échelle d'impact de gravité structurée en six niveaux, en fonction de plages de score clairement définies (par exemple : ≤ -1 = bénéfique, ≥ 15 = alarmant).

Ensuite, pour avoir une approche plus poussée et globale, les questions quantifiables sont ensuite rapportées dans un système de notation (voir dans les annexes). ChatGpt est utilisé principalement pour une visualisation et un classement de certaines données.

La segmentation prend en compte l'ensemble des secteurs et les postes occupés, notamment ceux « privilégiés » par les cybercriminels. La notion de fréquence d'utilisation d'internet et des ordinateurs est également un élément important, car cela entraîne une surexposition de la cible. Un autre point important pris en considération, est en relation à l'accès à des données sensibles, car ces données se négocient généralement mieux et les membres de ce type d'entreprise devraient être plus sensibilisés aux risques, à sa gravité, ses conséquences et à avoir des comportements de cybersécurité plus développés.

Pour les entreprises ayant plusieurs individus répondant au questionnaire, les profils les plus « dangereux » sont identifiés, afin d'avoir une vision plus précise des risques.

Une fois les informations recueillies, elles sont analysées, puis présentées aux personnes qui ont acceptée de tester l'étude, généralement les dirigeants et/ou les RSSI.

Le questionnaire et sa structure (accessible par lien https://forms.office.com/r/qt4KszhssQ) :

Présentation de l'étude

Vos activités professionnelles et la cybersécurité (AX00)

Bonjour, Ce questionnaire s'inscrit dans le cadre d'une étude universitaire portant sur les pratiques et comportements liés à cybersécurité dans les entreprises. Cette étude n'a pas pour objectif de mesurer vos connaissances techniques, vos réponses doivent simplement refléter vos expériences dans votre environnement professionnel. Les données collectées sont anonymes et confidentielles, elles ne seront utilisées qu'à des fins de recherche. Merci pour votre participation.

1. Merci de saisir le code entreprise (si vous en avez reçu un) *

Merci de saisir le nom de votre entreprise (si vous n'avez pas reçu de code)

Entrez votre réponse

Critère 1 : Facteurs affectant les perceptions de l'individu – Exposition aux risques de l'individu et l'entreprise

2. Quelle est la structure de votre entreprise *

- ◯ Entreprise de 1 à 9 salariés ou collaborateurs
- ◯ Entreprise de 10 à 49 salariés ou collaborateurs
- ◯ Entreprise de 50 à 249 salariés ou collaborateurs
- ◯ Entreprise de + de 250 salariés ou collaborateurs

3. Dans quel secteur d'activité, exercez-vous la majeure partie de votre activité professionnelle ? *

- ◯ Banque, Finance, Assurance, Comptabilité
- ◯ Avocat, Juridique, Notaire
- ◯ Informatique, Cybersécurité, Numérique
- ◯ Santé, Pharmaceutique
- ◯ Tourisme, Luxe, Hôtellerie, Restauration
- ◯ Commerce, E-commerce
- ◯ Industrie, BTP
- ◯ Administration, Collectivité locale
- ◯ Education, Formation,
- ◯ Artisanat, Agriculture
- ◯ Autre

4. Quel poste occupé vous dans l'entreprise ? *

- ◯ Président, Dirigeant, Gérant
- ◯ Responsable financier, Comptable, RH
- ◯ Responsable informatique, Administrateur SI,
- ◯ Manager, Responsable de service
- ◯ Employé(e), salarié(e), opérationnelle
- ◯ Département juridique, Avocat, Juriste,
- ◯ Département financier, comptable
- ◯ Stagiaire, alternant

5. Quelle est la fréquence d'utilisation d'un ordinateur, smartphone, ou internet dans vos activités professionnelles ? *

- ◯ Toute la journée
- ◯ Entre 3h et 5h par jour
- ◯ Entre 1h à 3h par jour
- ◯ Très rarement

6. Est-ce que dans votre travail vous avez accès à des données confidentielles ou sensibles ? *

- ◯ Oui
- ◯ Non

7. Est-ce que dans vos activités professionnelles, vous avez des accès privilégiés à des systèmes ou données sensibles ou critiques ? *

- ◯ Oui
- ◯ Non

Critère 2 : Perception de l'individu | Perception du risque perçu (dont sa propre vulnérabilité)

8. Avez-vous déjà été victime d'une attaque cyber utilisant les techniques de manipulation psychologique sur votre lieu de travail ou dans le cadre de vos activités professionnelles ? *

- ◯ Oui
- ◯ Non
- ◯ Ne sait pas

9. Pensez-vous être susceptible d'être victime d'une attaque cyber utilisant des techniques de manipulation psychologique sur votre lieu de travail ou dans le cadre de vos activités professionnelles ? *

	Certainement pas	Très improbable	Improbable	Moyennement probable	Probable	Très probable	Certainement
Affirmation 1	◯	◯	◯	◯	◯	◯	◯

10. Pensez-vous être potentiellement victime d'une attaque cyber sur votre lieu de travail ou dans le cadre de vos activités professionnelles utilisant les aspects suivants ? (Question à choix multiples) *

- ☐ Votre curiosité
- ☐ La peur de quelque chose, de quelqu'un ou d'une situation
- ☐ Votre empathie
- ☐ D'utiliser une situation de crise
- ☐ D'utiliser une situation d'urgence
- ☐ Autres
- ☐ Je ne pense pas être potentiellement victime de ce type d'attaque.

12. Quelle est selon vous, la probabilité que vous soyez la cible d'une attaque cyber utilisant de la manipulation psychologique, sur votre lieu de travail ou dans le cadre de vos activités professionnelles ? *

	Certainement pas	très improbable	Improbable	Moyennement probable	Probable	Très probable	Cer
A court terme (dans les 6 prochains mois)	◯	◯	◯	◯	◯	◯	
A long terme (dans le courant de l'année prochaine)	◯	◯	◯	◯	◯	◯	

13. Est-ce que votre entreprise a été victime d'une attaque cyber utilisant les techniques de manipulation psychologique ? *

- ◯ Oui
- ◯ Non
- ◯ Ne sait pas

14. Pensez-vous que votre entreprise soit susceptible d'être victime d'une attaque cyber utilisant des techniques de manipulation psychologique ? *

	Certainement pas	Très improbable	Improbable	Moyennement probable	Probable	Très probable	Certainement
Affirmation 1	◯	◯	◯	◯	◯	◯	◯

Critère 3 : Perception de l'individu | Perception de la gravité du risque (dont les conséquences)

15. Pensez-vous qu'une attaque cyber utilisant des processus de manipulation psychologique ou reposant sur la manipulation des comportements humains, vous impliquant, pourrait avoir des conséquences graves pour vous ? *

- ◯ Oui
- ◯ Non
- ◯ Ne sait pas

16. Pensez-vous qu'une attaque cyber utilisant des processus de manipulation psychologique, vous impliquant, pourrait : *

- ☐ vous faire valoir un avertissement par votre employeur
- ☐ vous faire perdre votre emploi
- ☐ vous créer un dommage financier
- ☐ vous créer un dommage réputationnel
- ☐ vous créer un dommage professionnel
- ☐ vous créer un dommage psychologique
- ☐ vous créer un dommage corporel
- ☐ pas du tout d'effet pour moi

17. Pensez-vous qu'une attaque cyber reposant sur de la manipulation psychologique, ciblant votre entreprise pourrait avoir des conséquences graves pour votre entreprise ? *

- ◯ Oui
- ◯ Non
- ◯ Ne sait pas

18. Pensez-vous qu'une attaque cyber utilisant des processus de manipulation psychologique touchant votre entreprise, pourrait ? *

- ☐ Créer une perte financière importante pour votre entreprise
- ☐ Créer un dommage réputationnel à votre entreprise
- ☐ Créer une perte de confiance des clients
- ☐ Engendrer la faillite de votre entreprise
- ☐ Engendrer le licenciement de nombreux employés
- ☐ pas du tout d'effet pour l'entreprise

19. Pensez-vous qu'une attaque cyber reposant sur la manipulation psychologique ou visant à manipuler vos comportements, ciblant votre entreprise, pourrait avoir des conséquences graves pour l'un de vos collègues ? *

- ◯ Oui
- ◯ Non
- ◯ Ne sait pas

Critère 4 : Perception de la menace (incluant les déclencheurs de motivation pour limiter le risque)

20. Si vous aviez des consignes à suivre, pour limiter ce type de risque d'attaque cyber reposant sur de la manipulation psychologique, dans le cadre de vos activités professionnelles, est-ce que vous les appliqueriez ? *

- ◯ Oui
- ◯ Non
- ◯ Ne sait pas

21. Parmi les éléments suivants, lesquels vous motiveraient le plus à appliquer les consignes de cybersécurité face aux cyberattaques reposant sur de la manipulation psychologique, dans le cadre de vos activités professionnelles ? (Cochez ceux qui s'appliquent à vous, plusieurs choix possibles) *

- ☐ Être reconnu dans mon entreprise et par mes collègues comme une personne vigilante et professionnelle
- ☐ Me sentir plus serein(e)
- ☐ Avoir le sentiment d'avoir déjoué une tentative de cyberattaque
- ☐ Eviter des sanctions en cas de ce type d'incident
- ☐ Apprendre à identifier et contrôler mes émotions (curiosité, peur, urgence, pression sociale) face à une situation potentiellement frauduleuse
- ☐ Savoir quel comportement avoir face à une demande suspecte
- ☐ Développer des connaissances en cybersécurité sur ce type d'attaque pour augmenter la confiance en moi
- ☐ Apprendre à douter d'une personne qui se présente comme une figure d'autorité
- ☐ Autres
- ☐ Je ne suis pas du tout motivé(e) pour appliquer les consignes face aux cyberattaques reposant sur de la manipulation psychologique, dans le cadre de vos activités professionnelles.

22. Si vous avez répondu "Autres" à la question, merci d'expliquer :

Entrez votre réponse

23. Parmi les éléments suivants, lesquels seraient pour vous, les meilleurs moyens pour appliquer les consignes de cybersécurité face aux cyberattaques reposant sur de la manipulation psychologique, dans le cadre de vos activités professionnelles ou sur votre lieu de travail ? *

- ☐ Avoir des formations sur le sujet
- ☐ Avoir des partages d'expérience de personne qui ont été victimes
- ☐ Être encouragé(e) par son entreprise, avec une reconnaissance des bons comportements sur ce type de menaces
- ☐ Exercices pratiques et simulations d'attaques
- ☐ Avoir une valorisation de l'autoformation sur ce sujet
- ☐ Avoir un référent sur ce sujet « un modèle à imiter » dans l'entreprise
- ☐ Savoir que votre entreprise à une assurance cyber
- ☐ Que je puisse percevoir et comprendre les risques liés à ce type de menaces
- ☐ Que mon entreprise exprime clairement, que ça fait partie d'une de mes taches
- ☐ Percevoir que les actions pour lutter contre ce type de menace sont efficaces

24. Pensez-vous que la gestion sur ce type de menaces soit secondaire (pas une priorité) dans votre entreprise ? *

	Certainement pas	très improbable	Improbable	Moyennement probable	Probable	Très probable	Certainement
Affirmation 1	◯	◯	◯	◯	◯	◯	◯

Critère 5 : Perception de la menace (incluant les intérêts de l'individu pour les consignes pour limiter les risques)

25. Est-ce que les sujets liés à la cybersécurité vous intéressent ? *

- ◯ Oui
- ◯ Non
- ◯ Ne sait pas

26. Est-ce que les sujets liés à la cybersécurité pour se protéger des attaques utilisant de la manipulation psychologique vous intéressent ? *

- ◯ Oui
- ◯ Non
- ◯ Ne sait pas

27. Avez-vous suivi des formations sur ces sujets ? *

- ◯ Oui
- ◯ Non

28. Etes-vous intéressé(e) pour suivre des formations sur ce sujet ? *

- ◯ Oui
- ◯ Non

29. Etes-vous plutôt du style à suivre les consignes préventives ? *

- ◯ Oui
- ◯ Non

Critère 6 : Probabilité d'actions | Perception des avantages et efforts à faire pour suivre les consignes pour réduire les risques et les conséquences

30. Pensez-vous que de suivre des consignes sur ce type de menaces permet réellement de réduire les risques d'être victime ? *

	Certainement pas	Très improbable	Improbable	Moyennement Probable	Probable	Très probable	Certainement
Affirmation 1	◯	◯	◯	◯	◯	◯	◯

31. En suivant les consignes de cybersécurité sur ce type de menaces, pensez-vous que vous : (choix multiples) *

- ☐ Réduisez votre propre risque d'être victime
- ☐ protégez vos collègues
- ☐ Contribuez à la sécurité de votre entreprise
- ☐ Evitez des sanctions potentielles en cas d'incident
- ☐ Evitez des situations stressantes et culpabilisantes après une attaque réussie
- ☐ Gagnez en compétence et en confiance face aux menaces cyber
- ☐ Autres
- ☐ Ces consignes ne servent à rien

32. Pensez-vous que les consignes actuelles de cybersécurité sur ce type de menaces dans votre entreprise sont ? *

Sélectionnez au plus 3 options.

- [ ] Trop contraignantes
- [ ] Limitent l'efficacité au travail
- [ ] Nécessaires
- [ ] Bien adaptées
- [ ] Insuffisantes et mériteraient d'être renforcées
- [ ] Je ne sais pas / Je ne les connais pas

Critère 7 : Probabilité d'actions | Perception efforts à faire pour suivre les consignes pour réduire les risques et les conséquences

33. Avez-vous reçu ou recevez-vous des consignes de cybersécurité dans le cadre de votre activité professionnelle ? *

- ◯ Oui
- ◯ Non

34. Si vous répondu "Oui", selon vous, appliquer les consignes de cybersécurité c'est : *

	Extrêmement difficile	Très difficile	Difficile	Moyennement difficile	Facile	Très facile	Extrêmement facile
Affirmation 1	◯	◯	◯	◯	◯	◯	◯

35. Quels sont pour vous les obstacles principaux qui gênent l'application des consignes de cybersécurité ? *

Sélectionnez au plus 4 options.

- [ ] Manque de clarté dans les consignes
- [ ] Manque de temps
- [ ] Trop de notions à appliquer
- [ ] Manque de formation
- [ ] Automatismes de travail qui rendent difficiles des changements de comportement
- [ ] Pression hiérarchique qui pousse à traiter les urgences en premier
- [ ] Difficultés à identifier une attaque cyber avec manipulation psychologique
- [ ] Ce n'est pas une priorité
- [ ] Je ne me sens pas concerné
- [ ] Dans mon entreprise, ce sujet n'est pas évoqué

36. Avez-vous reçu ou recevez-vous des consignes de cybersécurité sur les attaques cyber utilisant la manipulation psychologique dans le cadre de votre activité professionnelle ? *

- ◯ Oui
- ◯ Non

37. Pensez-vous que les consignes de cybersécurité ralentissent votre travail ? *

	Extrêmement	Vraiment beaucoup	Beaucoup	Moyennement	Peu	Très peu	Extrêmement peu
Affirmation 1	◯	◯	◯	◯	◯	◯	◯

Critère 8 : Probabilité de comportements | En fonction sa confiance en ses propres capacités à faire face à la menace

38. Si vous étiez confronté à une tentative d'attaque cyber, est-ce que vous sentiriez capable d'avoir un comportement adapté pour y faire face ? *

	Pas du tout capable	Très peu capable	Peu capable	Moyennement capable	Capable	Très capable	Extrêmement capable
Affirmation 1	◯	◯	◯	◯	◯	◯	◯

39. Si vous étiez confronté à une tentative d'attaque cyber avec une manipulation psychologique, est-que vous sentiriez capable d'avoir un comportement adapté pour y faire face ? *

	Pas du tout capable	Très peu capable	Peu capable	Moyennement capable	Capable	Très capable	Extrêmement capable
Affirmation 1	◯	◯	◯	◯	◯	◯	◯

Critère 9 : Probabilité de comportements | En fonction de ses acquis

40. Parmi ces comportements quels sont ceux qui correspondent à de bonnes pratiques en cybersécurité ? *

- ☐ J'utilise un mot de passe unique, complexe et de + 14 caractères pour chaque site
- ☐ J'enregistre mes mots de passe dans les favoris de mon navigateur
- ☐ Je vérifie toujours l'expéditeur des e-mails avant de cliquer sur un lien ou d'ouvrir une pièce jointe
- ☐ En cas d'e-mail ou message suspect, je ne dérange pas le responsable informatique ou ma collègue, ils ont déjà beaucoup à faire.
- ☐ Mon ordinateur vient de se bloquer, il y a un message de Microsoft. Le technicien Microsoft m'appelle, je lui laisse régler le problème en prenant la main à distance.
- ☐ Je recois un sms, puis un message vocal de mon patron, il est bloqué à l'étranger. Il a besoin en urgence d'avoir un virement pour les frais d'hopital. Je préviens vite la comptable pour qu'elle fasse le virement en urgence. Efficacité avant tout !
- ☐ Vous venez de cliquer sur un lien et soudainement, votre écran annonce un message d'un cyberattaquant. Vous décidez de ne rien dire et vous faites semblant de travailler.
- ☐ Vous avez l'habitude des campagnes de phishing de votre entreprise et vous venez de recevoir un e-mail pour vous féliciter de vos compétences et pour vous offrir une "Prime". Vous attendez 24h et vous faîtes le processus expliqué pour recevoir votre "Prime".

III. RESULTATS

Les résultats de cette étude sont encourageants et permettent de confirmer positivement la question de recherche. En effet, le Modèle des croyances relatives de santé (Janz & Becker, 1984) appliqué à la cybersécurité permet d'identifier des vulnérabilités importantes liées aux cybermenaces utilisant l'ingénierie sociale, touchant des entreprises en France. La nuance « *touchant des entreprises* » à la place « *touchant les entreprises* » est à souligner et s'explique pour les raisons suivantes *:* la taille de

l'échantillon est insuffisante, donc pas assez représentative et l'approche statistique nécessite d'être plus précise, davantage approfondie, et automatisée.

Cependant, l'étude permet d'avoir une vision synthétique des risques étudiés et d'identifier les critères dangereux pour l'entreprise et ceux qui peuvent jouer en sa faveur. De plus, l'étude permet d'identifier les éléments présentant des risques importants, comme des profils d'individus à risque, généralement difficilement identifiables. Ce dernier point permet aussi de relativiser des résultats globaux.

Pour comprendre les informations que peut produire la création et l'utilisation de cet indicateur (offrant un dépistage des cybermenaces utilisant l'ingénierie sociale affectant les entreprises), l'exemple des résultats d'un questionnaire envoyé à une entreprise est parlant. Le tableau présenté au début des résultats de l'entreprise X permet une première vision générale de la situation.

Pour des raisons de cybersécurité et de confidentialité, les résultats présentés ci-dessous sont anonymisés et partiels. Les autres résultats d'entreprises sont accessibles (avec une codification des noms des entreprises) aux seules personnes autorisées.

RESULTATS PARTIELS DE L'ENTREPRISE X (secteur juridique)

I. INDICATEUR GLOBAL DU RISQUE SUR LES CYBERMENACES UTILISANT L'INGENIERIE SOCIALE

Le tableau ci-dessous permet d'avoir une vue synthétique de la perception du risque, de ses conséquences et d'une prévision des comportements face aux cybermenaces utilisant l'ingénierie sociale.

CRITERES	DEGRES DE RISQUE					
	Bénéfique	Faible	Mineur	Elevé	Très élevé	Alarmant
1. Exposition aux risques						
2. Perception du risque d'être victime						
3. Perception de la gravité & conséquences						
4. Déclencheurs motivant à suivre les consignes						
5. Intérêt pour les consignes						
6. Perception des avantages à suivre les consignes						
7. Perception des efforts à faire pour appliquer les						
8. Confiance en ses propres capacité pour se protéger						
9. Acquis sur les comportements de base pour se protéger						

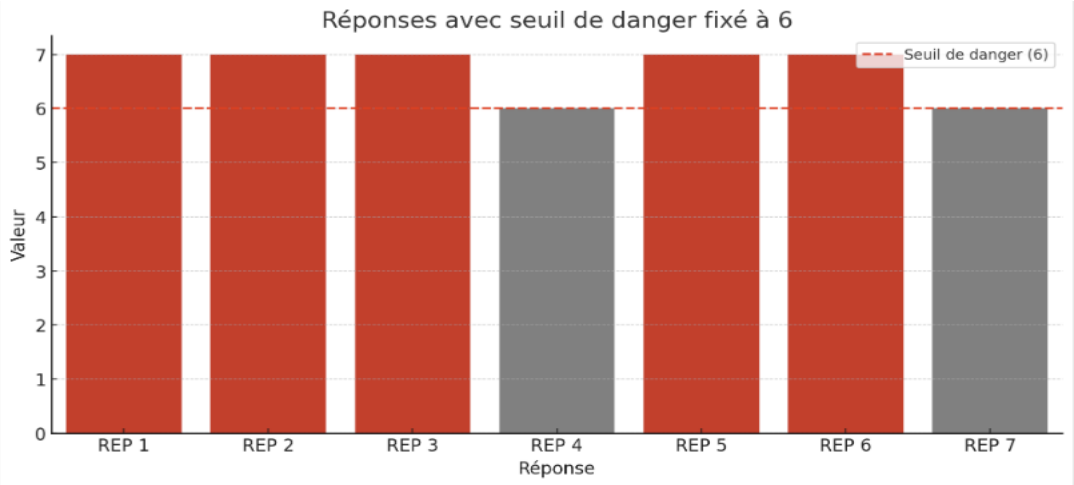
II. RESULTATS EN DETAIL PAR CRITERES ANALYSES

CRITERE 1 : Facteurs affectant les perceptions de l'individu | Exposition aux risques de l'individu et de l'entreprise

Les résultats montrent que l'exposition aux risques d'attaques cyber de cette entreprise est inquiétante et à surveiller avec attention. Cela s'explique en partie par le secteur d'activité de l'entreprise, l'accès à des données sensibles et du temps passés sur internet. Ce niveau d'exposition élevé a un impact amplificateur négatif sur les autres critères.

Degrés de risque	Score Ent	Echelle
Bénéfique		≤ -2 à 0
Facteur mineur – Faible		1 à 2
Facteur moyennement aggravant - Mineur		3 à 4
Facteur aggravant – Elevé		5 à 6
Facteur très aggravant - Très Elevé	7	7
Facteur extrêmement aggravant - Alarmant		8

Le schéma ci-dessous permet d'identifier les individus les plus exposés. L'accès aux résultats détaillés de l'étude permet d'identifier clairement les raisons des différences du niveau d'exposition.

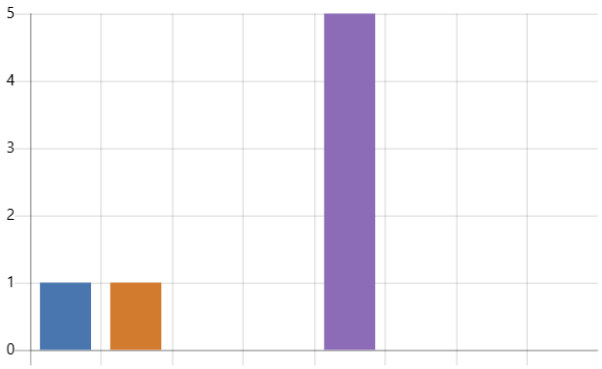


2. Quelle est la structure de votre entreprise

Entreprise de 1 à 9 salariés ou ...	0
Entreprise de 10 à 49 salariés ...	7
Entreprise de 50 à 249 salariés...	0
Entreprise de + de 250 salarié...	0

4. Quel poste occupé vous dans l'entreprise ?

Président, Dirigeant, Gérant	1
Responsable financier, Compt...	1
Responsable informatique, Ad...	0
Manager, Responsable de serv...	0
Employé(e), salarié(e), opérati...	5
Département juridique, Avoca...	0
Département financier, compt...	0
Stagiaire, alternant	0



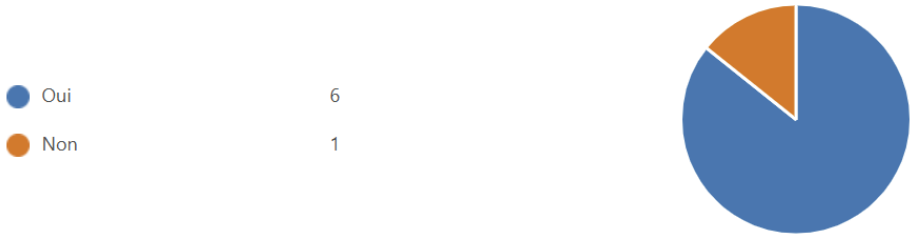
5. Quelle est la fréquence d'utilisation d'un ordinateur, smartphone, ou internet dans vos activités professionnelles ?

Toute la journée	7
Entre 3h et 5h par jour	0
Entre 1h à 3h par jour	0
Très rarement	0

6. Est-ce que dans votre travail vous avez accès à des données confidentielles ou sensibles ?

Oui	7
Non	0

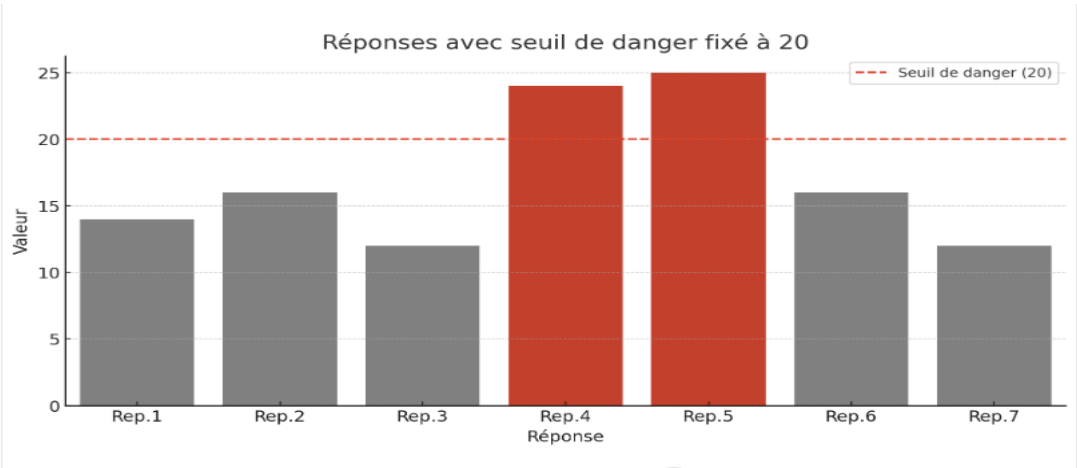
7. Est-ce que dans vos activités professionnelles, vous avez des accès privilégiés à des systèmes ou données sensibles ou critiques ?



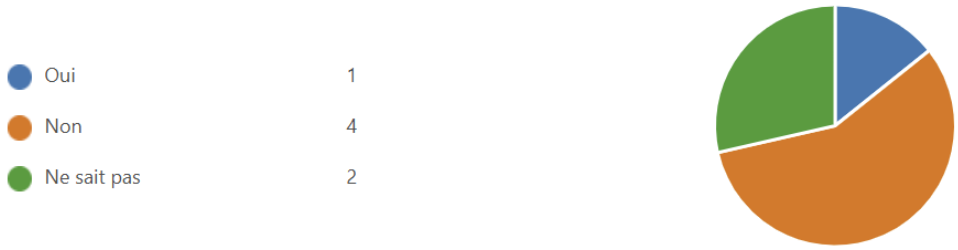
CRITERE 2 : Perception de l'individu | Perception du risque perçu (dont sa propre vulnérabilité)

Dans son ensemble les chiffres traduisant la perception des individus interrogés sur le risque qu'eux-mêmes ou l'entreprise soient victimes de ce type de cybermenace est élevé et à surveiller. En poussant l'analyse, il s'avère que deux individus influencent très négativement les résultats et le schéma ci-dessus témoigne que leurs expositions aux risques sont également élevées, ce qui est un amplificateur de risques. Les réponses de ces deux individus révèlent une minimisation claire de ce type de risque que ce soit pour eux-mêmes et pour l'entreprise.

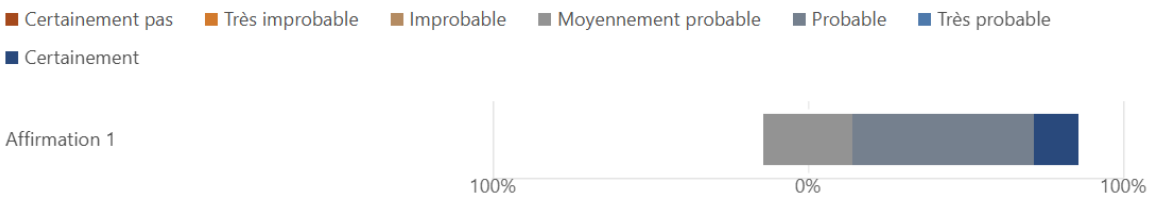
Degrés de risque	Score Ent.	Echelle
Bénéfique		≤ -1
Facteur mineur – Faible		0 à 6
Facteur moyennement aggravant - Mineur		7 à 13
Facteur aggravant – Elevé	17	14 à 20
Facteur très aggravant - Très Elevé		21 à 27
Facteur extrêmement aggravant - Alarmant		28 à 34



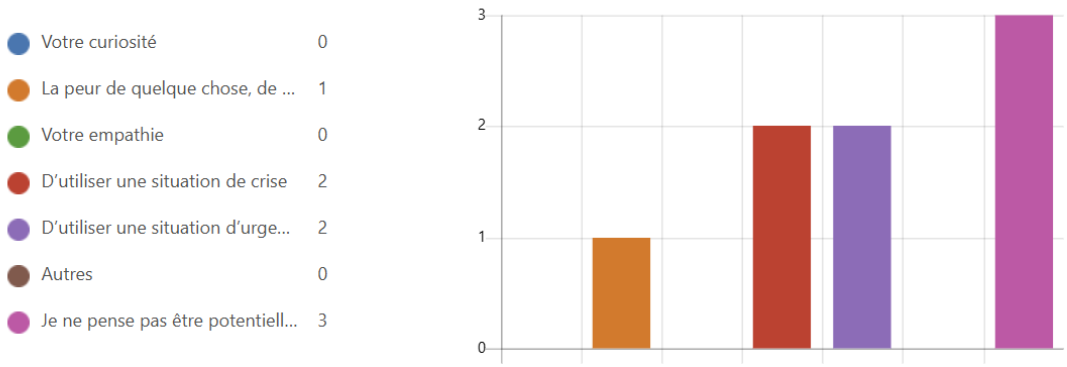
8. Avez-vous déjà été victime d'une attaque cyber utilisant les techniques de manipulation psychologique sur votre lieu de travail ou dans le cadre de vos activités professionnelles ?



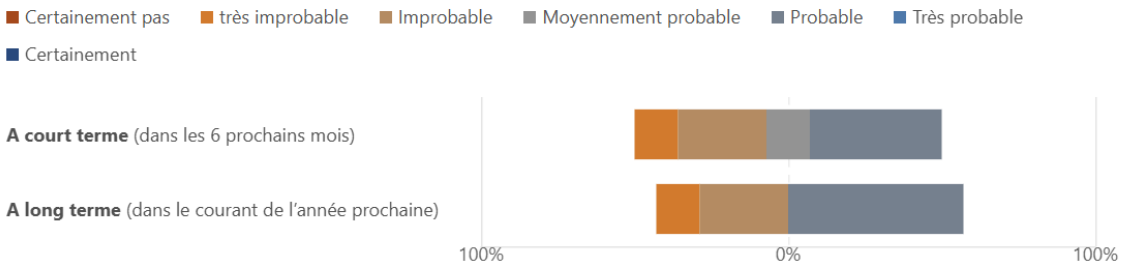
9. Pensez-vous être susceptible d'être victime d'une attaque cyber utilisant des techniques de manipulation psychologique sur votre lieu de travail ou dans le cadre de vos activités professionnelles ?



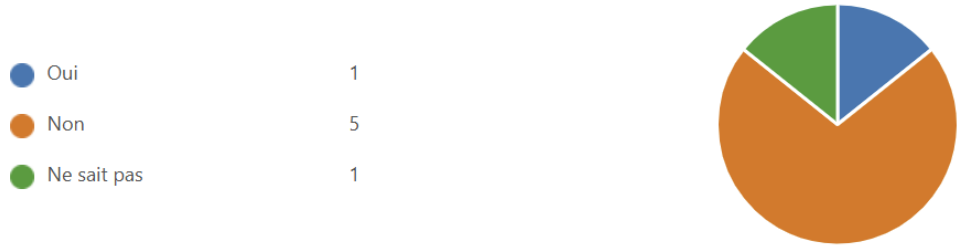
10. Pensez-vous être potentiellement victime d'une attaque cyber sur votre lieu de travail ou dans le cadre de vos activités professionnelles utilisant les aspects suivants ? (Question à choix multiples)



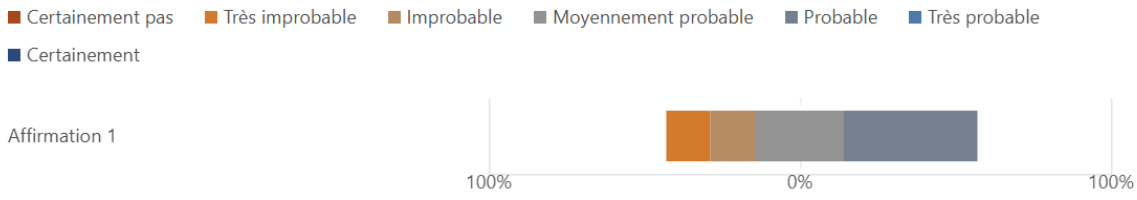
12. Quelle est selon vous, la probabilité que vous soyez la cible d'une attaque cyber utilisant de la manipulation psychologique, sur votre lieu de travail ou dans le cadre de vos activités professionnelles ?



13. Est-ce que votre entreprise a été victime d'une attaque cyber utilisant les techniques de manipulation psychologique ?



14. Pensez-vous que votre entreprise soit susceptible d'être victime d'une attaque cyber utilisant des techniques de manipulation psychologique ?

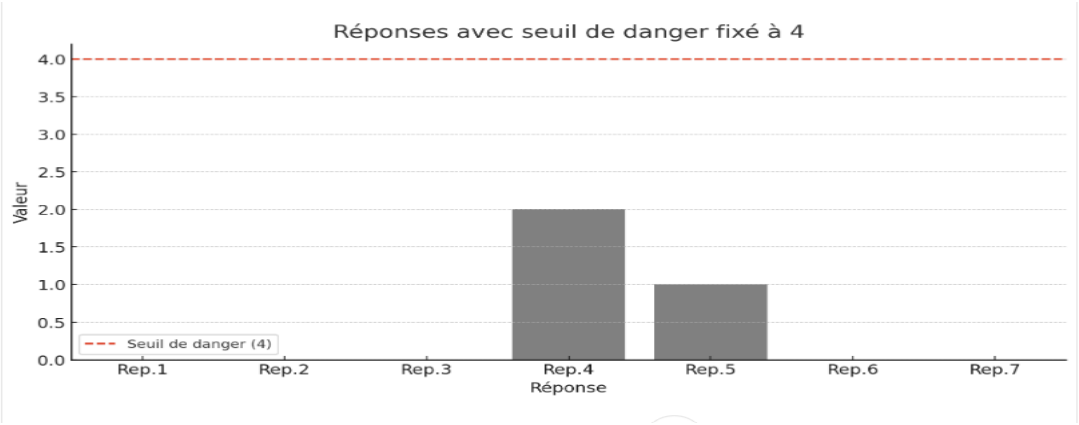


CRITERE 3 : Perception de l'individu | Perception de la gravité du risque et des conséquences

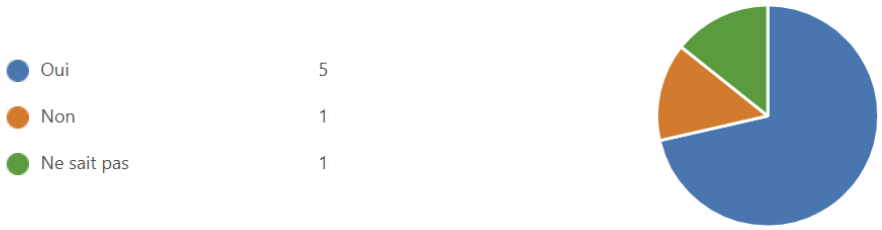
Les données collectées montrent que les individus de cette entreprise ont une assez bonne perception des gravités et des conséquences qu'engendre le risque de cyberattaques utilisant l'ingénierie sociale, ce qui est bénéfique en terme cybersécurité. Toutefois, les profils des questionnaires 4 et 5 se démarquent également négativement en répondant que ce type d'attaques ne pourrait avoir des conséquences graves pour eux ou en ne sachant pas si cela pourrait avoir des conséquences graves pour eux.

Les individus interrogés pointent en priorité comme conséquences : l'impact professionnel, l'impact psychologique et le risque d'avertissement.

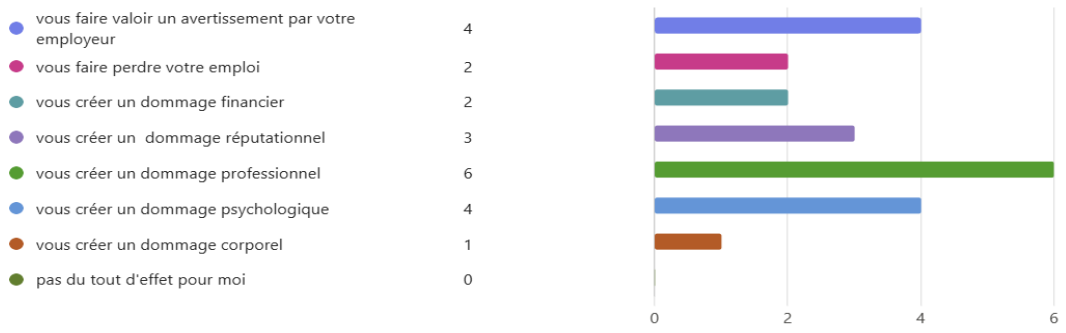
Degrés de risque	Score Ent.	Echelle
Bénéfique		0
Facteur mineur – Faible	1	1 à 2
Facteur moyennement aggravant – Mineur		3 à 4
Facteur aggravant – Elevé		5 à 6
Facteur très aggravant - Très Elevé		7 à 8
Facteur extrêmement aggravant – Alarmant		9 à 10



15. Pensez-vous qu'une attaque cyber utilisant des processus de manipulation psychologique ou reposant sur la manipulation des comportements humains, vous impliquant, pourrait avoir des conséquences graves pour vous ?



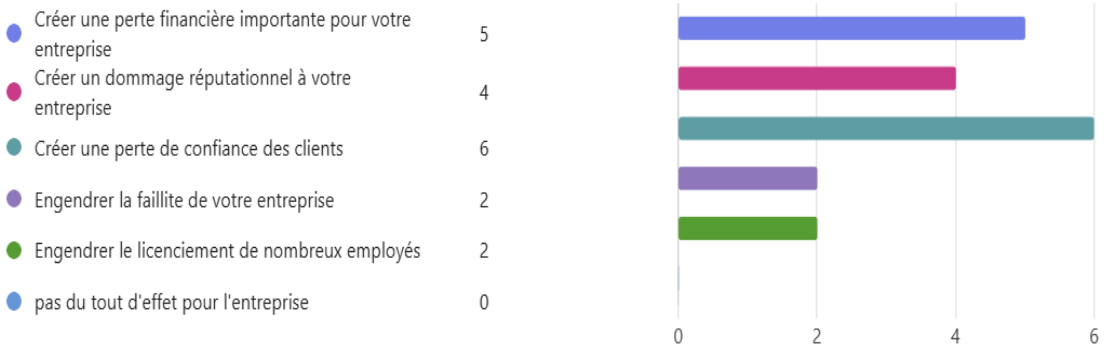
16. Pensez-vous qu'une attaque cyber utilisant des processus de manipulation psychologique, vous impliquant, pourrait : (0 point) En savoir plus



17. Pensez-vous qu'une attaque cyber reposant sur de la manipulation psychologique, ciblant votre entreprise pourrait avoir des conséquences graves pour votre entreprise ?

18. Pensez-vous qu'une attaque cyber utilisant des processus de manipulation psychologique touchant votre entreprise, pourrait ? (0 point)

En savoir plus



19. Pensez-vous qu'une attaque cyber reposant sur la manipulation psychologique ou visant à manipuler vos comportements, ciblant votre entreprise, pourrait avoir des conséquences graves pour l'un de vos collègues ?

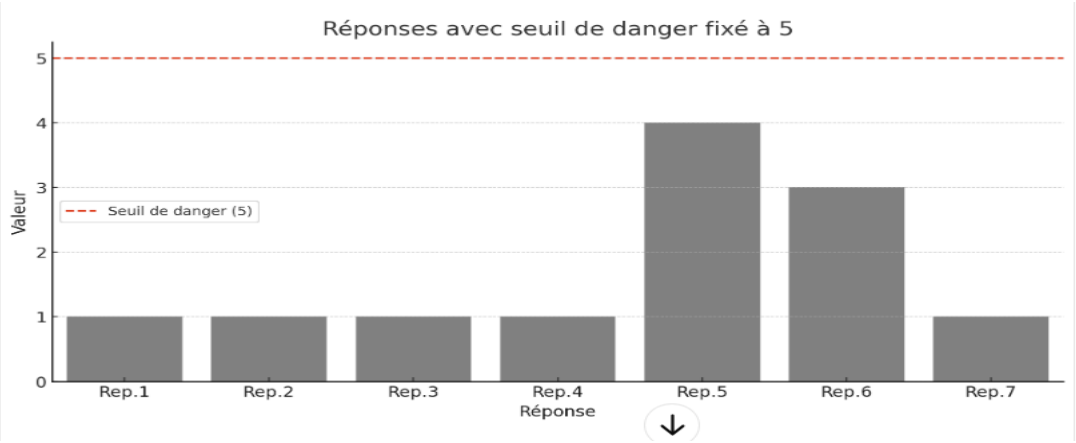
CRITERE 4 : Perception de la menace | Incluant les déclencheurs de motivation pour limiter le risque

Dans l'ensemble, les éléments déclencheurs de motivation pour limiter les risques sont des atouts pour l'entreprise. Toutefois, les profils des questionnaires 5 et 6 ne suivent pas du tout cette tendance et représentent une difficulté pour l'entreprise en termes de motivation pour réduire ce type de risque.

Les éléments importants favorables pour cette motivation sont : le besoin de sérénité, savoir quel comportement avoir face à une demande suspecte, développer des connaissances en cybersécurité sur ce type d'attaque pour augmenter la confiance en moi, avoir des formations sur le sujet, avoir des partages d'expérience de personne qui ont été victimes, et des exercices pratiques et simulations

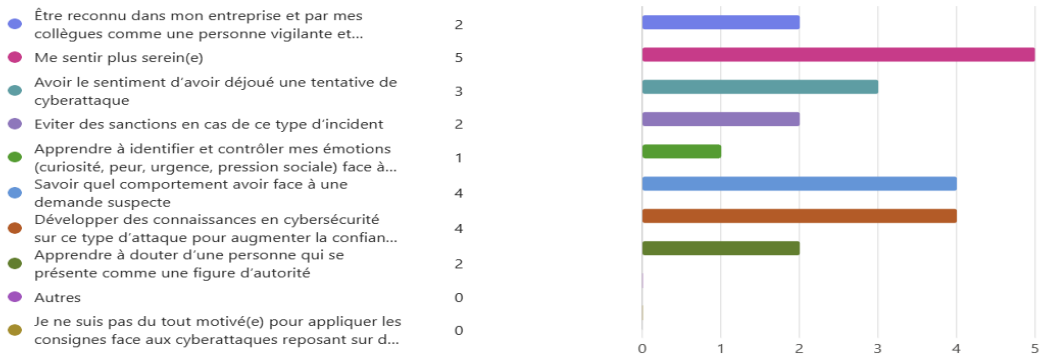
d'attaques. Concernant les profils des questionnaires 5 et 6, ils perçoivent comme secondaire, la gestion de ce type de menace par l'entreprise.

Degrés de risque	Score Ent.	Echelle
Bénéfique		1
Facteur mineur – Faible	2	2
Facteur moyennement aggravant – Mineur		3 à 5
Facteur aggravant – Elevé		6 à 8
Facteur très aggravant - Très Elevé		9 à 10
Facteur extrêmement aggravant - Alarmant		11



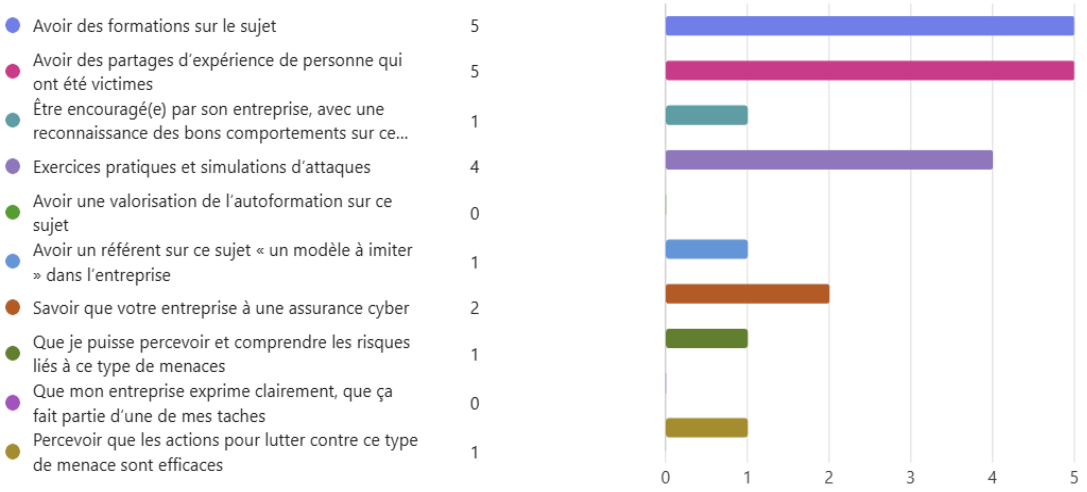
20. Si vous aviez des consignes à suivre, pour limiter ce type de risque d'attaque cyber reposant sur de la manipulation psychologique, dans le cadre de vos activités professionnelles, est-ce que vous les appliqueriez ?

21. Parmi les éléments suivants, lesquels vous motiveraient le plus à appliquer les consignes de cybersécurité face aux cyberattaques reposant sur de la manipulation psychologique, dans le cadre de vos activités professionnelles ? (Cochez ceux qui s'appliquent à vous, plusieurs choix possibles) (0 point) En savoir plus

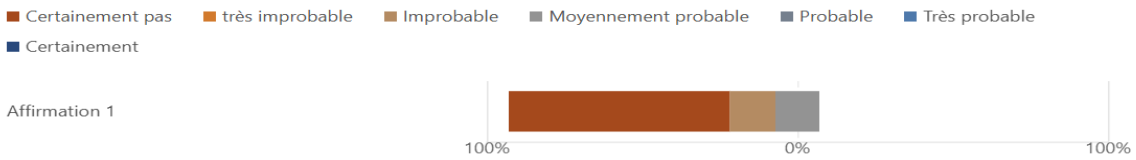


23. Parmi les éléments suivants, lesquels seraient pour vous, les meilleurs moyens pour appliquer les consignes de cybersécurité fac e aux cyberattaques reposant sur de la manipulation psychologique, dans le cadre de vos activités professionnelles ou sur votre lieu de travail ? (0 point)

En savoir plus



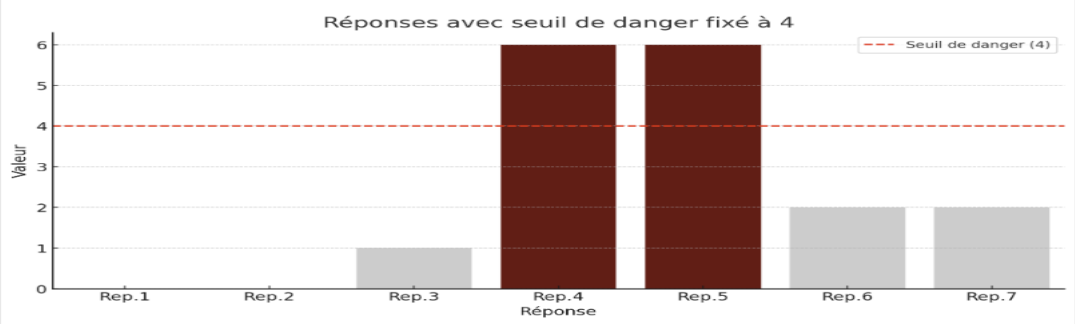
24. Pensez-vous que la gestion sur ce type de menaces soit secondaire (pas une priorité) dans votre entreprise ?



CRITERE 5 : Perception de la menace | Incluant les intérêts de l'individu pour les consignes limitant les risques

Les données recueillies traduisent un risque faible lié à la perception des consignes à suivre pour limiter les risques par les individus ayant répondu au questionnaire. Cependant, le schéma offrant une focale par questionnaire permet d'identifier deux profils présentant des risques importants, les questionnaires 4 et 5. Les sources de risques de ces profils deux profils sont liées aux points suivants : ils cumulent des intérêts défavorables, ou une absence d'intérêt sur ces sujets et sur de la formation concernant ces matières.

Degrés de risque	Score Ent.	Echelle
Bénéfique		0
Facteur mineur - Faible	2	1 à 2
Facteur moyennement aggravant - Mineur		3 à 4
Facteur aggravant - Elevé		5
Facteur très aggravant - Très Elevé		6
Facteur extrêmement aggravant - Alarmant		7



25. Est-ce que les sujets liés à la cybersécurité vous intéressent ?

Oui	5
Non	0
Ne sait pas	2

26. Est-ce que les sujets liés à la cybersécurité pour se protéger des attaques utilisant de la manipulation psychologique vous intéressent ?

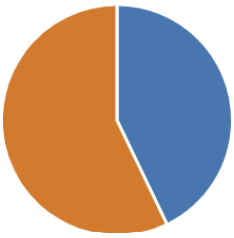
Oui	5
Non	0
Ne sait pas	2

27. Avez-vous suivi des formations sur ces sujets ?

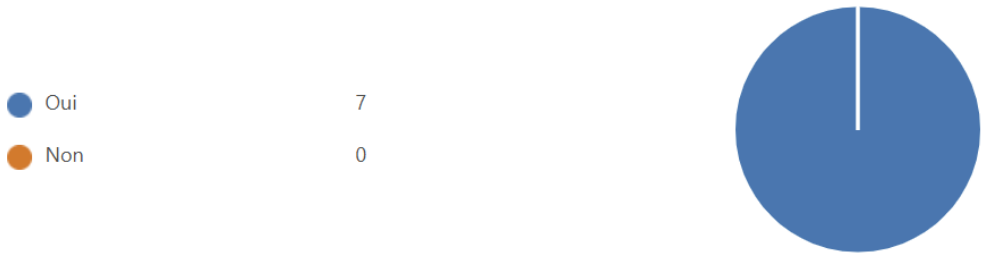
Oui	1
Non	6

28. Etes-vous intéressé(e) pour suivre des formations sur ce sujet ?

Oui	3
Non	4



29. Etes-vous plutôt du style à suivre les consignes préventives ?

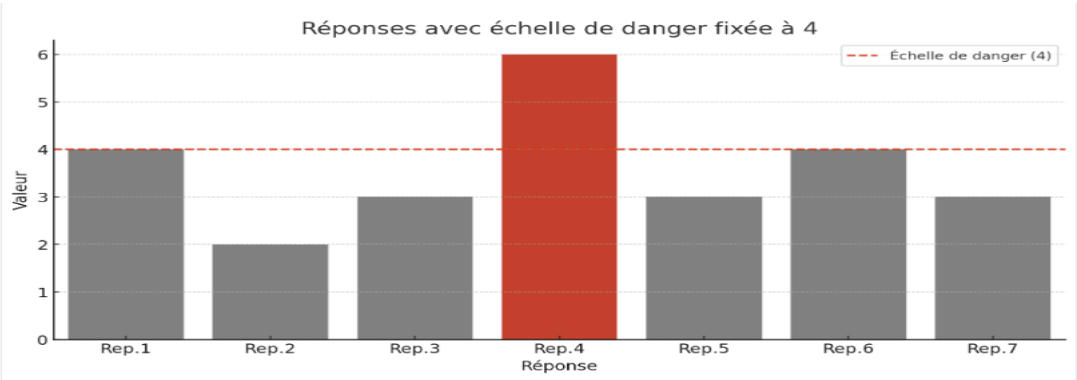


CRITERE 6 : Probabilité d'actions | Perception des avantages à faire pour suivre les consignes réduisant les risques et les conséquences

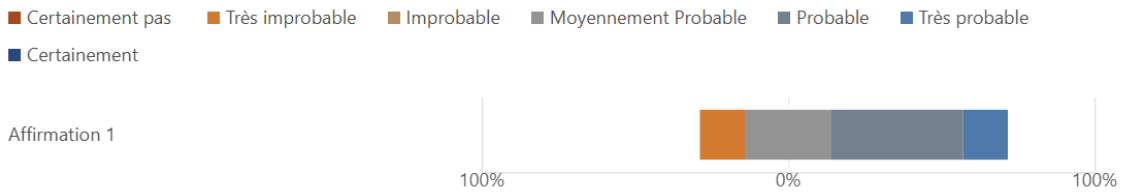
Dans l'ensemble l'entreprise présente des risques mineurs liés à la perception des avantages à suivre les consignes réduisant les risques et les conséquences sur ce type de cybermenaces. Cependant, le risque est amplifié par les réponses du profil du questionnaire 4 qui juge que le fait de suivre des consignes sur ce type de menaces réduit peu le risque.

Les leviers importants sont : contribuer à la sécurité de votre entreprise, réduire votre propre risque d'être victime, éviter des sanctions potentielles en cas d'incident, gagner en compétence et en confiance face aux menaces cyber. Les consignes actuelles de cybersécurité sur ce type de menaces dans l'entreprise sont perçues comme nécessaires.

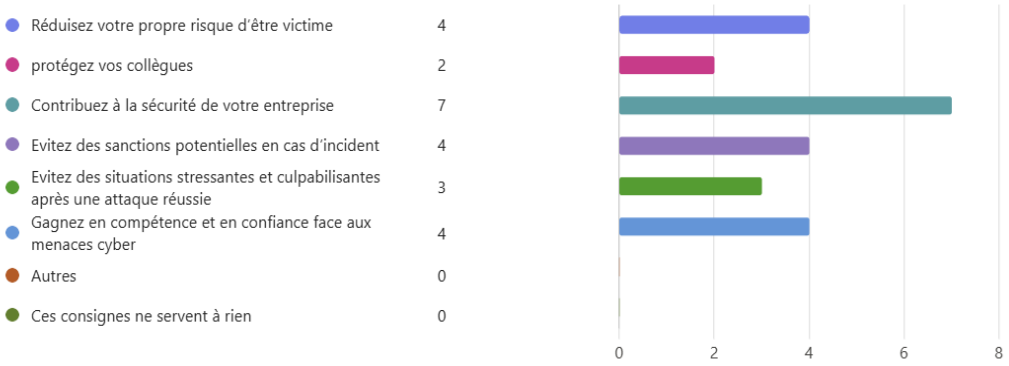
Degrés de risque	Score Ent.	Echelle
Bénéfique		1
Facteur mineur – Faible		2
Facteur moyennement aggravant – Mineur	4	3 à 4
Facteur aggravant – Elevé		5 à 6
Facteur très aggravant - Très Elevé		7 à 8
Facteur extrêmement aggravant – Alarmant		9



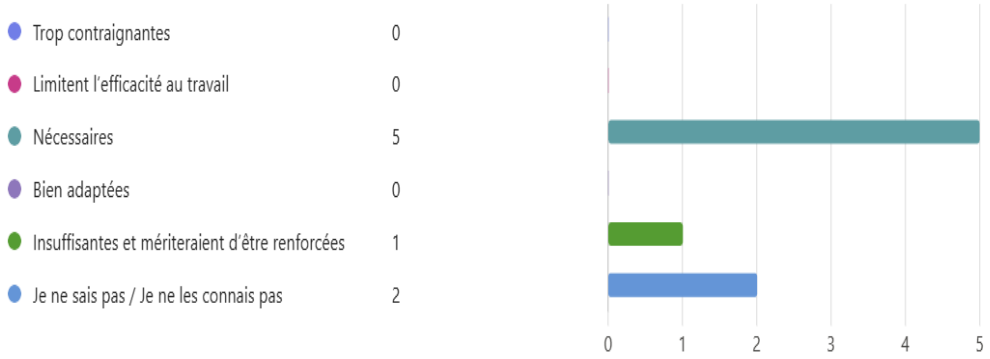
30. Pensez-vous que de suivre des consignes sur ce type de menaces permet réellement de réduire les risques d'être victime ?



31. En suivant les consignes de cybersécurité sur ce type de menaces, pensez-vous que vous : (choix multiples) (0 point) En savoir plus



32. Pensez-vous que les consignes actuelles de cybersécurité sur ce type de menaces dans votre entreprise sont ? (0 point) En savoir plus

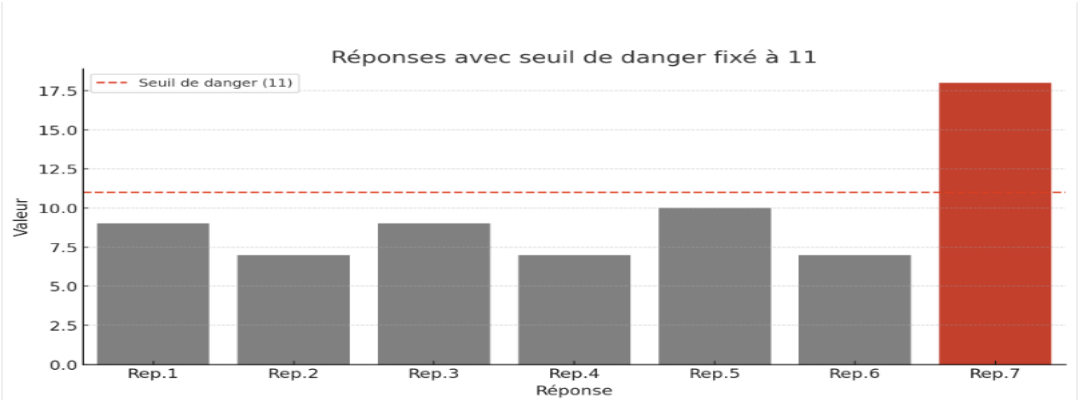


CRITERE 7 : Probabilité d'actions | Perception d'efforts à faire pour suivre les consignes pour réduire les risques et les conséquences

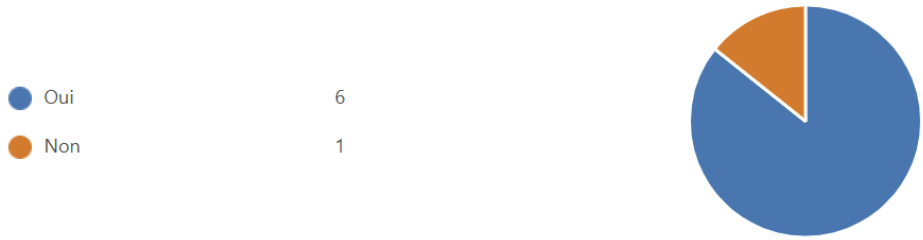
Globalement, la perception des efforts à faire pour suivre les consignes pour réduire ce type de risque et ses conséquences est à prendre en considération, car l'analyse identifie un danger moyen pour l'entreprise. Ce danger est lié à une perception d'une certaine difficulté à appliquer les consignes de cybersécurité et surtout à un individu qui signale ne pas avoir reçu de consignes sur le risque dans le

cadre professionnel. Les obstacles principaux identifiés sont : le manque de temps, la pression hiérarchique qui pousse à traiter les urgences en premier, les difficultés à identifier une attaque cyber avec manipulation psychologique.

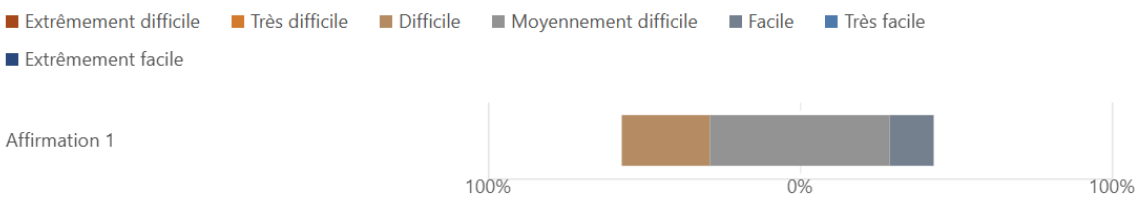
Degrés de risque	Score Ent.	Echelle
Bénéfique		2
Facteur mineur - Faible		3 à 5
Facteur moyennement aggravant - Mineur	10	6 à 11
Facteur aggravant - Elevé		12 à 17
Facteur très aggravant - Très Elevé		17 à 23
Facteur extrêmement aggravant - Alarmant		24 à 28



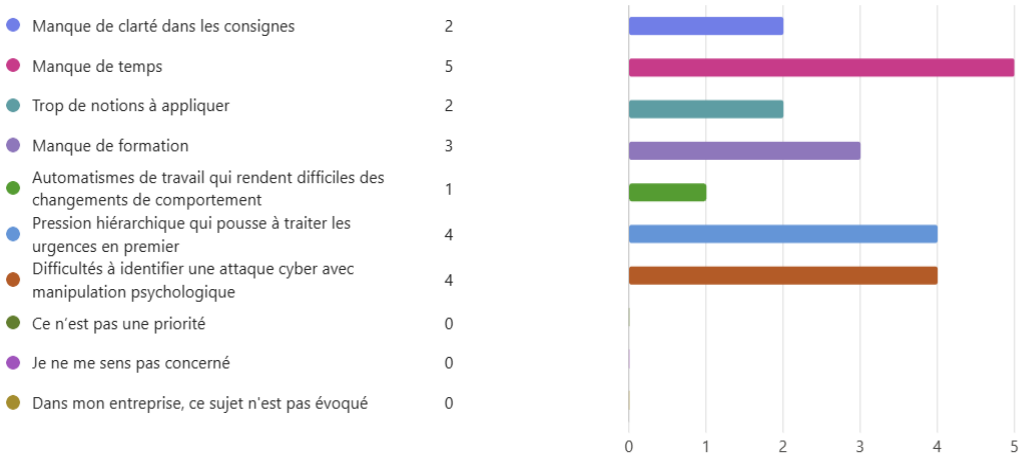
33. Avez-vous reçu ou recevez-vous des consignes de cybersécurité dans le cadre de votre activité professionnelle ?



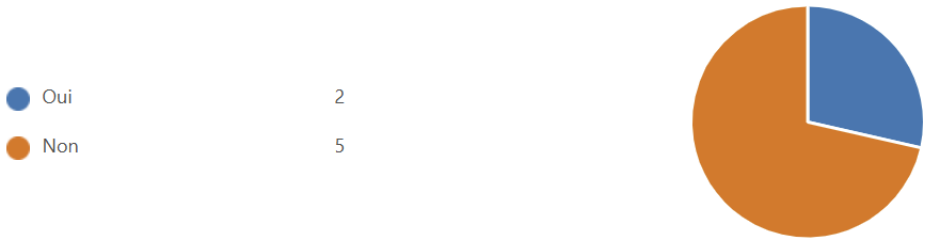
34. Si vous répondu "Oui", selon vous, appliquer les consignes de cybersécurité c'est :



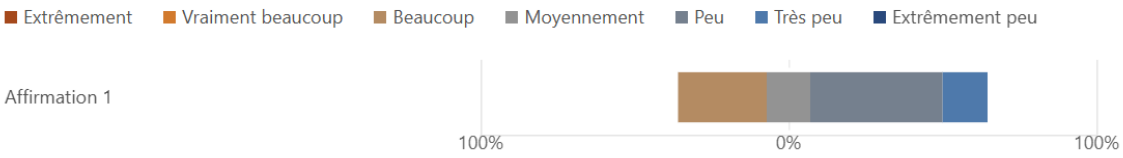
35. Quels sont pour vous les obstacles principaux qui gênent l'application des consignes de cybersécurité ? (0 point) En savoir plus



36. Avez-vous reçu ou recevez-vous des consignes de cybersécurité sur les attaques cyber utilisant la manipulation psychologique dans le cadre de votre activité professionnelle ?



37. Pensez-vous que les consignes de cybersécurité ralentissent votre travail ?

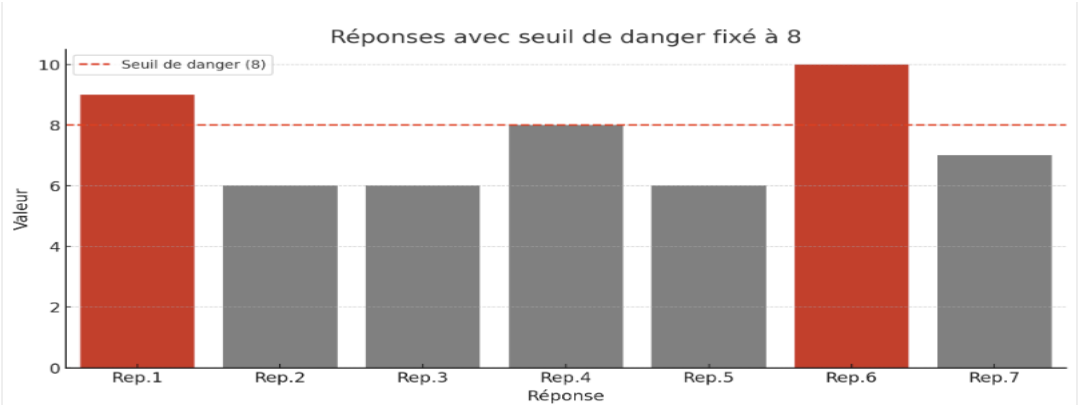


CRITERE 8 : Probabilité de comportements | En fonction de sa confiance en ses propres capacités à faire face à la menace

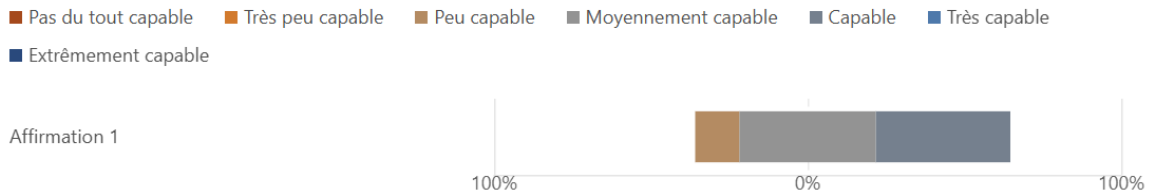
Dans l'ensemble, les résultats représentent un risque de danger moyen pour l'entreprise par rapport à la confiance qu'ont les individus en leurs propres capacités à gérer ce type de menace. Ces résultats sont négativement augmentés par les profils des questionnaires 1 et 6 qui manquent de confiance en eux sur ce type de menace.

Degrés de risque	Score Ent.	Echelle
Bénéfique		2
Facteur mineur – Faible		3 à 5

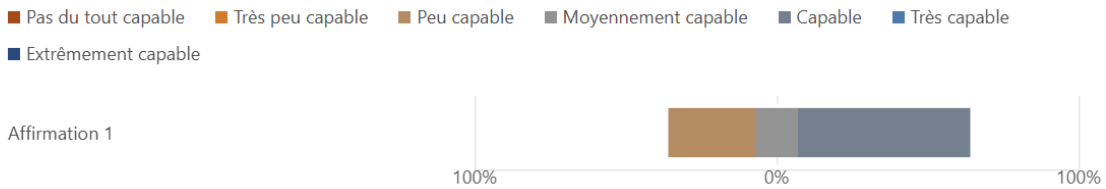
Facteur moyennement aggravant - Mineur	7	6 à 8
Facteur aggravant – Elevé		9 à 10
Facteur très aggravant - Très Elevé		11 à 12
Facteur extrêmement aggravant - Alarmant		13 à 14



38. Si vous étiez confronté à une tentative d'attaque cyber, est-ce que vous sentiriez capable d'avoir un comportement adapté pour y faire face ?



39. Si vous étiez confronté à une tentative d'attaque cyber avec une manipulation psychologique, est-que vous sentiriez capable d'avoir un comportement adapté pour y faire face ?

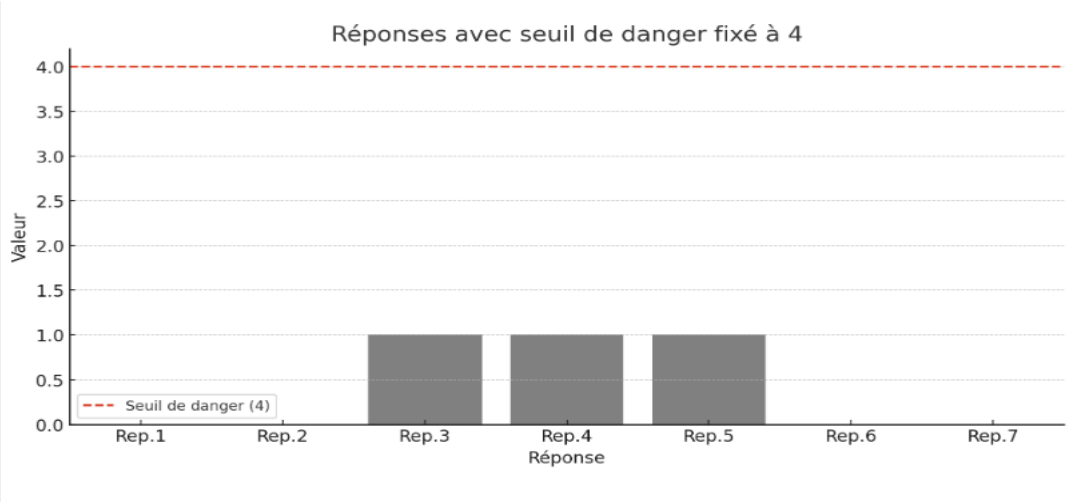


CRITERE 9 : Probabilité de comportements | En fonction de ses acquis

L'entreprise bénéficie d'atouts concernant les acquis en termes de comportements à suivre pour se protéger de ce type de cybermenace. Ils ont dans l'ensemble répondu correctement aux questions sur les comportements à avoir par rapport à ce type de menace.

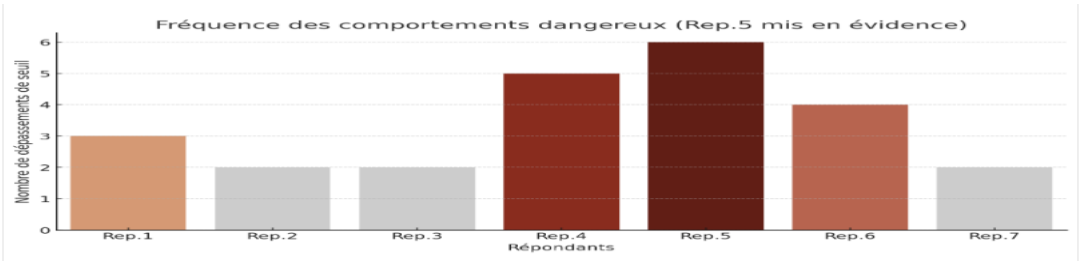
Degrés de risque	Score Ent.	Echelle
Bénéfique	0,4	0
Facteur mineur – Faible		1 à 2
Facteur moyennement aggravant - Mineur		3 à 4

Facteur aggravant - Elevé		5 à 6
Facteur très aggravant - Très Elevé		7
Facteur extrêmement aggravant - Alarmant		8

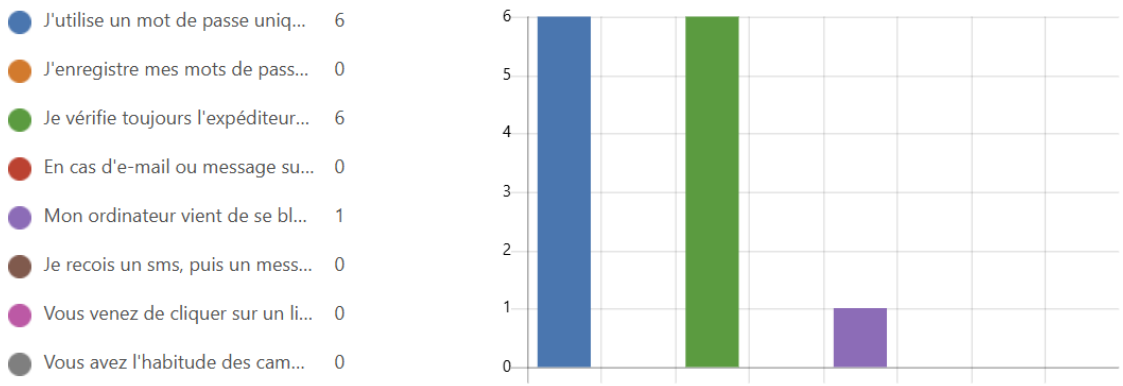


III. Identification des profils à risques

Ce schéma identifie des profils présentant des risques et ceux qui sont bénéfiques pour l'entreprise. Cela permet de pouvoir apporter des analyses plus précises sur la situation de cette entreprise sur les risques étudiés. Les profils 5, 4 sont à analyser en urgence.



40. Parmi ces comportements quels sont ceux qui correspondent à de bonnes pratiques en cybersécurité ?



IV. DISCUSSION DES RESULTATS & IMPLICATIONS

Les résultats de cette étude sont encourageants, car ils apportent des informations importantes concernant les facteurs humains qui interviennent, augmentent ou réduisent le risque de cybermenaces utilisant l'ingénierie sociale.

Bien que ces résultats ne soient pas complètement exploitables, ils permettent d'établir le cadre d'une approche de dépistage de ce type de risque, d'avoir un questionnaire permettant d'identifier des vulnérabilités importantes et des échelles de risque pouvant également être améliorées avec des méthodes statistiques plus précises et plus poussées. Par exemple, en utilisant des « HeatMap », des « boîtes à moustaches » et des traitements des données par intelligence artificielle automatisées utilisées en data science avec du Machine Learning supervisé ou non. Il est également important de prendre en considération l'approche déclarative de ces réponses, l'irrationalité potentielle de la victime pendant une phase d'attaque. En effet, le fait d'identifier la source du risque, le risque, ses conséquences et l'application des consignes ne garantit pas complètement le risque de faille humaine. Cependant, avec une préparation, une conscientisation du risque, l'individu sera davantage alerte pour se protéger et protéger l'entreprise.

En outre, pour avoir une vision plus précise, il serait utile de comparer le nombre d'individus sollicités dans l'entreprise, qui n'ont pas souhaité ou pu répondre au questionnaire, ce point serait un facteur aggravant. A ce stade, il n'est pas pris en considération (principalement pour des questions de gestion du temps).

Il est important d'appréhender cet indicateur comme un outil complémentaire d'aide à la gestion du risque cyber, sur un type de menace précise. Il n'a pas forcément vocation à long terme d'être utilisé seul, mais de permettre d'affiner des audits de cybersécurité, de proposer des solutions différentes, plus précises, et parfois plus pertinentes. Par exemple, dans le cadre des formations proposées par les pôles cyber de la gendarmerie, cet indicateur permettrait d'avoir une notion de la maturité de l'entreprise à former, et d'orienter la formation en fonction des faiblesses identifiées. Cet indicateur permet aussi des approches plus ad 'hoc pour la gestion du risque, dans la mesure où il pourrait identifier directement les individus d'une entreprise (en les prévenant), puis en combinant les résultats obtenus à des tests d'attaques pour évaluer, s'il y une meilleure perception du risque et d'établir une relation de cause à effet sur le respect des actions préventives.

Un autre avantage de cet indicateur, c'est qu'il permet de faire comprendre que parfois, ce n'est pas de la mauvaise volonté des individus dans l'entreprise, mais ce sont leurs perceptions du risque qui les limitent à suivre des consignes préventives. Cet indicateur pourrait être également combiné a des indicateurs plus poussés sur la motivation, pour avoir un impact plus important sur l'identification des personnes à risques avec pour objectifs primordiaux de les conduire à protéger l'entreprise contre ce type de cybermenace.

CONCLUSION

Pour conclure, cette recherche permet de répondre positivement à la question *« Est-ce que le Modèle des croyances relatives de santé (Janz & Becker, 1984) appliqué à la cybersécurité permet d'identifier des vulnérabilités liées aux cybermenaces utilisant l'ingénierie sociale, touchant des entreprises en France ? ».* Toutefois, le manque de représentativité de l'échantillon et d'éventuelles modifications (et même des corrections) sur les traitements statistiques empêchent d'affirmer que ce modèle peut être généralisé. Les limites de cette étude sont essentiellement liées à un manque de temps, ce qui pourrait être pallié facilement pour affiner l'approche et la tester à une plus grande échelle.

Pour autant, cette recherche a permis de poser ce concept, d'élaborer un questionnaire en fonction des critères du modèle, de développer des échelles offrant la possibilité de qualifier les risques pour les entreprises, d'identifier les individus à risque, et d'offrir un indicateur synthétique pour avoir une vision rapide. De plus, cette recherche permet d'avoir un outil supplémentaire pour accroitre l'efficience de campagnes préventives, de proposer des conseils en cybersécurité incluant le facteur humain exposé à ce type de cybermenace, de proposer des formations ciblées, d'intégrer cette approche dans des processus de gestion des ressources humaines et de créer des simulations d'attaques par de l'intelligence artificielle pour entraîner les individus de ces entreprises.

Les cinq piliers du modèle déclinés en neuf critères permettent d'avoir une compréhension des différents mécanismes qui affectent les diverses perceptions, les freins et les obstacles à la motivation et une projection probable des actions et comportements des individus. Dans l'exemple de présentation des résultats de la société X, ils sont traités de manière essentiellement individuelle, mais ils devraient également être traités en tenant compte de leurs interactions.

Bien que des études complémentaires sont nécessaires pour consolider, confirmer et généraliser ce concept de dépistage de cybermenaces utilisant l'ingénierie sociale, cette approche pourrait contribuer efficacement à la cybersécurité de nombreuses entreprises, dont des TPE-PME. Précisant que ce modèle peut être facilement combiné à d'autres approches, être mis en place sans trop de complexité et à des coûts très abordables.

REMERCIEMENTS

Je remercie Jean-Christophe FEDHERBE pour la qualité des échanges sur ce sujet et pour sa disponibilité, Marlène DULAURANS pour la qualité des cours du Diplôme Universitaire « Cybercriminalité, défis et enjeux humains (sciences sociales) » de l'IUT de BORDEAUX MONTAIGNE.

REFERENCES

Borkovich, D. J., & Skovira, R. J. (2019). Cybersecurity inertia and social engineering: who's worse, employees or hackers ?. *Issues in Information Systems*, *20*(3). P-139, P- 140 (a1)

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Janz, N. K., & Becker, M. H. (1984). The health belief model: A decade later. *Health education quarterly*, *11*(1), 1-47.

Jain, A., Tailang, H., Goswami, H., Dutta, S., Sankhla, M. S., & Kumar, R. (2016). Social engineering: Hacking a human being through technology. IOSR Journal of Computer Engineering, 18(5), 94-100.

Ng, B. Y., & Xu, Y. (2007). Studying users' computer security behavior using the Health Belief Model. *PACIS 2007 Proceedings*, 45. (a12)

Rosenstock, I. M. (1966). *Why people use health services*. Milbank Memorial Fund Quarterly, 44(3), 94–127. https://doi.org/10.2307/3348967

Rosenstock, I. M. (2005). Why people use health services. *The Milbank Quarterly*, *83*(4). Re-impression Milbank Memorial Fund Quarter- 44, ly 94-124, 1966.

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, *12*(12), 6042.

Site internet :

ANSSI. (2024). *Le CyberDico*. https://cyber.gouv.fr/le-cyberdico

Service de recherche du Parlement européen. (2024). *La cybersécurité dans l'UE : Menaces, défis et réponses politiques* (Briefing EPRS_BRI(2024)760356). Parlement européen. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf

ANNEXES

Annexe 1 : La matrice Excell pour évaluer le niveau de risque

Annexe 2 : Les résultats des entreprises sont joints dans le dossier « Confidentiel - Ne pas diffuser ».