

Jean Marie VIGNEAUD

Responsabilité Sociale des Entreprises :
quand le bien être au travail
participe à une meilleure
réactivité des parties prenantes internes
face au risque cyber



Promotion 2024-2025

Résumé

À l'ère de la transformation numérique, les entreprises sont de plus en plus exposées aux risques cybernétiques. Le rapport Hiscox 2023 indique que 53 % des entreprises ont été victimes d'une cyberattaque, soulignant l'ampleur croissante de la menace. Dans ce contexte, la cybersécurité ne peut plus être pensée uniquement en termes techniques : elle doit s'inscrire dans une approche globale, intégrant les dimensions humaines et organisationnelles.

Cette étude explore le lien entre les politiques de Responsabilité Sociétale des Entreprises (RSE) et la sécurité des systèmes d'information, en mettant l'accent sur le rôle du bien-être au travail dans la prévention des cyberattaques, en particulier le phishing. S'appuyant sur des recherches récentes montrant que 95 % des incidents de cybersécurité impliquent un facteur humain, nous émettons l'idée que la réduction du stress, de la charge mentale et de l'anxiété favorisée par une politique RSE, engendre une meilleure disponibilité cognitive et une vigilance accrue chez les collaborateurs.

Deux hypothèses structurent notre réflexion :

H1 : Le bien-être psychologique des employés renforce leur capacité à détecter et prévenir les cybermenaces.
H2 : Des employés épanouis grâce à un environnement de travail soutenant, favorisé par une stratégie RSE, développe une coopération et une résilience collective face aux risques numériques.

La première partie de l'article analyse les leviers psychologiques exploités dans les attaques de phishing. La seconde propose une revue de littérature sur les effets de la RSE sur la santé mentale au travail et le développement d'un comportement coopératif. Enfin, la dernière partie examine en quoi ces dynamiques favorisent une meilleure réactivité et une gestion plus efficace du risque cyber.

1 - INTRODUCTION

À l'ère du numérique, les entreprises sont de plus en plus dépendantes des technologies de l'information pour assurer leur fonctionnement, leur compétitivité et leur croissance. Cette transformation numérique, bien qu'elle offre de nombreuses opportunités, s'accompagne d'un accroissement considérable des risques liés à la sécurité des systèmes d'information [1].

Selon le rapport Hiscox 2023 [2], 53 % des entreprises ont subi une attaque, comparativement à 48 % en 2022.

Face à la multiplication de ces cyberattaques, des fuites de données sensibles et des actes de cyber espionnage, les entreprises doivent adopter une approche proactive et globale de la cybersécurité, non seulement pour protéger leurs actifs numériques, mais également pour conforter la confiance des parties prenantes, clients comme partenaires.

En intégrant la cybersécurité dans leur stratégie RSE, les entreprises ne se contentent plus de protéger leurs systèmes d'information : elles affirment également leur engagement envers l'éthique, la transparence et la durabilité numérique [3]. La protection des données personnelles, la contribution à un espace numérique plus sûr et la prévention des risques pour les employés deviennent alors des dimensions clés de leur responsabilité sociétale.

Un article d'IS Partners indique que 95 % des incidents de cybersécurité comportent un facteur humain [4]. La surcharge cognitive, le stress et la fatigue sont des éléments cruciaux qui influencent directement la capacité des collaborateurs à détecter et à réagir face aux menaces cybernétiques [5].

Dans ce contexte, cet article se propose d'explorer les interconnexions entre la RSE et la cybersécurité, en soulignant particulièrement comment, dans une approche holistique, une attention portée sur le bien-être au travail et la diminution du stress peut améliorer la disponibilité cognitive des employés, favorisant ainsi une meilleure gestion des enjeux de cybersécurité.

Nous ferons ici deux hypothèses qui guideront notre réflexion tout au long de cet article :

H1 : La promotion du bien-être psychologique et de la disponibilité cognitive des employés permet d'améliorer l'efficacité des dispositifs de cybersécurité en renforçant l'adhésion aux bonnes pratiques et la capacité de détection des menaces,

H2 : Des employés épanouis, soutenus par une démarche RSE, sont plus enclins à développer une approche collaborative, qui optimise la vigilance et la capacité collective à anticiper et neutraliser ces cybermenaces.

Dans un premier temps, nous reviendrons sur les leviers psychologiques utilisés par les hackers pour mener à bien leurs opérations de phishing. Puis nous ferons une revue de la littérature sur les apports de la RSE, notamment en matière de bien-être au travail, réduisant ainsi le stress, l'anxiété et la charge mentale, terreau des opérations de phishing. Nous verrons également comment la RSE peut développer un fort sentiment d'appartenance à l'entreprise, favorisant une prise de conscience collective des risques environnants. Enfin, nous étudierons comment ces éléments inhérents à la mise en place de la RSE, peuvent favoriser une meilleure réactivité et prise en compte du risque cyber au sein de l'organisation.

2 - LE PHISHING : UNE ATTAQUE PSYCHOLOGIQUE

Le phishing est une forme de cybercriminalité où les attaquants exploitent principalement les vulnérabilités psychologiques des individus, afin de les tromper pour qu'ils révèlent des informations personnelles ou financières sensibles [6]. Les hackers ne se contentent pas de tromper les victimes avec des messages frauduleux, ils manipulent également des facteurs psychologiques tels que le stress, l'anxiété, la charge mentale ou l'effet tunnel pour favoriser leurs attaques.

Comme le souligne Bruno Teboul [7], « 87 % des sondés déclarent gérer souvent plusieurs tâches simultanément et 78 % disent avoir une charge de travail élevée. Ceci a des conséquences cognitives : augmentation du niveau de stress (57 % des répondants se disent stressés) et génération de cortisol par le cerveau. Si le stress est prolongé, cela se traduira par une baisse de la vigilance – et donc par une plus grande vulnérabilité aux cyberattaques ».

Ces facteurs influencent fortement la capacité des individus à analyser rationnellement une situation, les rendant plus susceptibles de céder aux demandes des cybercriminels.

En étudiant ces leviers psychologiques, il devient possible de mieux comprendre les mécanismes de manipulation employés par les hackers et de mettre en place des mesures pour réduire la vulnérabilité des victimes face à de telles attaques.

2.1 Le stress : un moteur de réactions impulsives

Le stress est un facteur psychologique majeur dans la réussite des attaques de phishing. En créant un sentiment d'urgence et de pression, les hackers incitent leurs victimes à agir rapidement, sans prendre le temps de réfléchir à la véracité du message reçu [8].

Le stress engendré par un message urgent du type "Votre compte sera suspendu dans 24 heures" ou "Votre paiement a échoué, veuillez le régulariser immédiatement" active une réponse émotionnelle qui inhibe la réflexion rationnelle. Le cortisol, hormone liée au stress, peut altérer les capacités cognitives de la victime [9], réduisant sa capacité à analyser de manière critique le message et à remettre en question son authenticité. Dans ce contexte, les victimes sont plus enclines à cliquer sur un lien malveillant ou à fournir des informations personnelles, simplement pour se débarrasser de la source de stress.

Sijie Zhuo & al. ont montré que, sous une charge de travail élevée, les participants étaient plus enclins à cliquer sur des e-mails de phishing pertinents pour leurs tâches, indiquant que le stress et la surcharge cognitive peuvent compromettre la vigilance [10].

Le stress n'est pas seulement une réponse émotionnelle; il modifie également le traitement de l'information. Selon une étude menée par Sapolsky [11], sous stress, le cerveau humain privilégie les solutions rapides et immédiates au détriment de la prise de décision réfléchie, ce qui explique pourquoi les victimes de phishing prennent souvent des décisions impulsives.

Dans le contexte de la cybersécurité, les employés stressés peuvent également considérer les pratiques de sécurité comme des tâches supplémentaires exigeantes en ressources plutôt que comme des mesures de protection essentielles [12]. Cette attitude défensive peut entraîner des raccourcis dans les procédures de sécurité, des retards dans les mises à jour des systèmes ou des avertissements de sécurité ignorés, les employés tentant de préserver les ressources restantes pour gérer les exigences immédiates de leur travail.

2.2 L'effet Tunnel : réduction de la vision critique

L'effet tunnel est un phénomène psychologique où, sous l'influence de facteurs externes (comme une pression ou une émotion intense), une personne réduit sa capacité à percevoir une situation dans son ensemble et se concentre uniquement sur un détail particulier [13]. Les hackers utilisent ce phénomène pour concentrer l'attention de leurs victimes sur un aspect du message qui semble critique, tout en masquant les signes de fraude.

Par exemple, un phishing par email peut contenir un message d'alerte, insistant sur l'urgence de réinitialiser un mot de passe pour éviter une "panne de sécurité", tandis que d'autres éléments suspects (comme des fautes d'orthographe, des adresses email douteuses ou des liens URL non sécurisés) sont relégués à l'arrière-plan, ne captant pas l'attention de la victime. L'effet tunnel est particulièrement efficace lorsque les victimes sont déjà en état de stress ou d'anxiété.

Elles ne parviennent plus à analyser l'ensemble du message et ne se concentrent que sur l'élément qui leur semble urgent, ce qui les rend vulnérables à des attaques ciblées.

L'effet tunnel peut également être exacerbé dans des situations où la victime a déjà un biais de conformité ou de confiance envers l'entité envoyant le message. En conséquence, la victime ignore ou minimise les incohérences, ce qui augmente les chances de réussite de l'attaque [14].

2.3 L'anxiété : une propension à éviter les pertes

L'anxiété, liée à la peur des conséquences négatives, joue un rôle central dans l'efficacité des attaques de phishing. Ce levier psychologique repose sur le biais de perte, selon lequel les individus ressentent la perte de quelque chose (comme l'accès à un compte en ligne ou des données personnelles) comme étant bien plus douloureuse que le gain d'un équivalent [15]. Les hackers exploitent cette émotion en présentant des scénarios qui incitent à une réaction immédiate.

Les e-mails de phishing créent un climat d'anxiété en incitant la victime à "agir maintenant" pour éviter une conséquence négative. Par exemple, un message prétendant qu'un compte bancaire va être suspendu si une action immédiate n'est pas effectuée génère une anxiété importante. Cette anxiété entraîne une peur de la perte, qui est souvent plus forte que la peur de l'inconnu. Cette pression émotionnelle empêche souvent la victime d'analyser le message de manière rationnelle et de rechercher des signes de fraude, ce qui renforce l'efficacité de l'attaque.

L'anxiété peut aussi réduire la capacité de la victime à utiliser des stratégies de coping appropriées [11]. Elle accentue la tendance à agir rapidement pour "réduire" la tension, sans prendre le temps d'évaluer les options ou de remettre en question la source du message. En conséquence, la victime est plus susceptible de divulguer des informations sensibles ou de cliquer sur des liens malveillants.

2.4 La charge mentale : limitation de la capacité de traitement cognitif

La surcharge cognitive joue un rôle clé dans la baisse de vigilance face aux attaques de phishing. Lorsque les individus sont confrontés à de multiples tâches ou à des informations complexes, leur capacité à analyser et à évaluer les messages devient limitée [16]. Ceci est encore plus flagrant lorsqu'un individu est déjà soumis à une forme de stress ou d'anxiété.

Cette surcharge conduit là encore à une prise de décision basée sur l'émotion et la rapidité plutôt que sur la réflexion logique. Les hackers tirent parti de ce phénomène en rendant leurs messages aussi simples et directs que possible, tout en évitant de surcharger la victime d'informations. Par exemple, un message de phishing demandant une simple "confirmation d'identité" semble plus facile à traiter qu'un message complexe demandant une vérification de sécurité détaillée, ce qui incite souvent la victime à agir sans réfléchir.

Ainsi, les hackers exploitent des failles qui ne relèvent pas uniquement de la technologie, mais aussi — et de plus en plus — de la psychologie humaine. Le stress chronique, la charge mentale excessive et l'anxiété sont autant de vulnérabilités invisibles que les cyberattaquants savent manipuler pour augmenter leurs chances de succès dans les campagnes de phishing. Ces états altèrent la vigilance, réduisent la capacité de discernement et favorisent des prises de décision impulsives, souvent au détriment de la sécurité.

Face à ce constat, il devient essentiel de ne pas cantonner la cybersécurité aux seules mesures techniques ou protocolaires. La responsabilité des entreprises s'étend désormais à la prise en compte des facteurs psychosociaux dans la prévention des risques cyber. En tant qu'acteurs sociaux, elles ont un rôle clé à jouer dans la réduction du stress au travail, l'optimisation de la charge cognitive des employés et la promotion d'un environnement professionnel sain. Non seulement ces actions contribuent au bien-être global des collaborateurs, mais elles renforcent également leur résilience face aux tentatives de

manipulation psychologique. La sécurité numérique rejoint alors une mission plus large : celle du bien-être au travail comme rempart contre les menaces contemporaines.

3 - LA RESPONSABILITE SOCIALE DES ENTREPRISES (RSE)

La Responsabilité Sociale des Entreprises (RSE) traduit la volonté des entreprises d'intégrer, de manière volontaire, des enjeux sociaux, environnementaux et économiques dans l'ensemble de leurs activités. Positionnant les entreprises comme des contributeurs proactifs au bien-être sociétal et environnemental, cette approche remet en question la perception traditionnelle que l'on a de les considérer comme de simples entités à but lucratif [17].

Ainsi, une entreprise doit être consciente et responsable des conséquences environnementales et sociales de ses produits, de ses services et opérations. Elle doit également identifier et prendre en compte ses parties prenantes, c'est-à-dire l'ensemble des acteurs influencés par ses décisions et actions.

A ce titre, le pilier social, en particulier, met l'accent sur le respect des droits fondamentaux et l'égalité des chances. Il englobe des thématiques essentielles telles que la formation, l'inclusion, la diversité, ainsi que la santé, la sécurité et le bien-être des collaborateurs.

Au sein de la littérature, nombreux sont les auteurs qui se sont intéressés au bien-être au travail et ses enjeux. Une synthèse des articles de Daniel Kahneman [18], Tony Hsieh [19], Adam Grant [20], Matthew Kelly [21] permet de dégager les points suivants :

- La gestion de la charge de travail : s'assurer que les employés ont des charges de travail raisonnables et gérables,
- La santé mentale et physique : favoriser la santé mentale et physique des employés en offrant des programmes de soutien et des services de santé mentale, en créant un environnement de travail sain et en encourageant les employés à prendre soin d'eux-mêmes.
- La culture d'entreprise : s'assurer que la culture d'entreprise est positive, respectueuse et inclusive, et qu'elle encourage les employés à s'épanouir professionnellement.
- La communication : favoriser une communication ouverte et transparente entre les employés et la direction, et s'assurer que les employés se sentent entendus et pris en compte.
- Les relations de travail : encourager la collaboration et la coopération entre les employés, et s'assurer que les relations de travail sont respectueuses et professionnelles.

3.1 Le bien-être au travail, levier d'une meilleure performance individuelle.

Historiquement, la littérature a mis l'accent sur l'impact de la RSE sur la performance financière et la réputation des entreprises [22]. Plus récemment, l'attention s'est portée sur les micro-effets de la RSE, notamment sur la vigilance et les capacités cognitives des employés [23]. Dans un contexte où la surcharge informationnelle menace la qualité de l'attention, la RSE peut servir de levier de focalisation.

Des recherches mettent en évidence l'importance de la RSE en tant qu'outil stratégique pour améliorer le bien-être et la sécurité des employés. Il est suggéré que les organisations

devraient privilégier les initiatives RSE non seulement en raison de leur impact positif sur la société et l'environnement, mais aussi pour leur capacité à améliorer les performances des employés. En investissant dans des démarches RSE, les entreprises peuvent créer un environnement de travail propice qui réduit le stress, renforce l'engagement des employés envers l'organisation et encourage des comportements sûrs [24].

La littérature scientifique démontre de manière constante que l'implication de l'entreprise dans des initiatives responsables améliore la perception que les employés ont de leur environnement de travail. Glavas [25] explique que les salariés qui perçoivent leur entreprise comme engagée socialement ressentent un sens plus profond à leur travail, ce qui accroît leur satisfaction, leur motivation et leur loyauté.

Un environnement de travail socialement responsable :

- Favorise des valeurs de respect et de reconnaissance.
- Renforce l'identité professionnelle et le sentiment d'appartenance.
- Stimule l'engagement à travers des objectifs partagés et valorisants.

Dans ce cadre, la RSE devient un moteur de motivation intrinsèque, un concept clef en psychologie du travail, qui va bien au-delà des simples incitations financières.

Des entreprises telles que Patagonia ou Danone, connues pour leur forte politique RSE, affichent des taux de satisfaction et de fidélisation des employés bien supérieurs à la moyenne de leur secteur [26].

D'autres études ont montré que les programmes RSE contribuent de manière significative à la réduction de la fatigue mentale des employés. Ces initiatives favorisent des choix altruistes et diminuent l'égoïsme éthique, ce qui a pour effet de promouvoir une meilleure santé mentale en milieu professionnel [27].

Les situations de stress au travail sont souvent amplifiées par des perceptions d'injustice, d'insécurité ou de désalignement entre valeurs personnelles et professionnelles [28]. Le stress au travail, souvent lié à la charge mentale et émotionnelle, est un facteur clé de mal-être. Or, plusieurs études montrent que la RSE agit comme un modérateur de ce stress. D'autre part, la transparence des dispositifs de reconnaissance (retours réguliers, valorisation des initiatives internes) accroît la confiance organisationnelle et réduit l'incertitude, facteurs clés de stress psychologique [29].

Rupp et al. [30] démontrent que les employés évoluant dans un contexte RSE fort perçoivent leur environnement comme plus juste et soutenant, ce qui réduit significativement les niveaux de stress perçu. Cela contribue à instaurer un climat de justice organisationnelle, à améliorer la confiance dans l'organisation, à réduire l'ambiguïté des rôles et l'incertitude.

Selon Crawford & al. [31], la RSE contribue à réduire le stress au travail en fournissant des ressources qui amortissent les exigences du travail, permettant aux employés de maintenir les ressources cognitives et émotionnelles nécessaires à une activité professionnelle efficace.

Une autre étude menée par Great Place to Work [32] a révélé que les employés travaillant dans des entreprises fortement engagées en RSE rapportaient 37 % de stress perçu en moins que dans des entreprises peu engagées.

La charge mentale, définie comme l'ensemble des efforts cognitifs mobilisés pour accomplir une tâche, est diminuée lorsque l'environnement est plus soutenant et prévisible. Ainsi, dans une entreprise engagée en RSE, l'employé a moins à se soucier de luttes internes (manque de reconnaissance, conflits de valeurs etc.) et peut consacrer pleinement ses ressources cognitives à son activité principale [27].

3.2 La RSE renforce la collaboration

La mise en place de la RSE favorise non seulement l'épanouissement au travail, mais également une dynamique de collaboration renforcée et une plus grande implication des employés dans des enjeux cruciaux tels que la cybersécurité.

Les initiatives RSE, en visant à promouvoir un environnement de travail éthique, respectueux et inclusif, contribuent de manière significative à l'épanouissement des collaborateurs. En intégrant des valeurs de durabilité, d'équité et de responsabilité sociale, les entreprises favorisent un cadre propice à la motivation, à l'engagement et à la satisfaction au travail.

Une étude menée par le *Harvard Business Review* montre que les employés qui perçoivent leur entreprise comme étant socialement responsable sont plus satisfaits de leur travail et présentent un taux d'engagement plus élevé [33].

De plus, la RSE encourage la collaboration entre les différents départements et équipes au sein de l'entreprise. En mettant en œuvre des projets RSE, les employés sont amenés à travailler ensemble sur des objectifs communs qui vont au-delà de la simple performance économique. Cette coopération renforce la cohésion interne et crée un environnement de travail plus solidaire et plus harmonieux, comme le montre une étude de Gallup [34] sur l'impact de la collaboration interéquipes sur le bien-être au travail.

4 – RSE ET CYBERSECURITE

Une étude menée par *Deloitte* souligne que la cybersécurité est devenue une priorité pour les entreprises qui intègrent des programmes de RSE, car ces derniers permettent non seulement de sensibiliser les employés à la protection des données, mais aussi de les motiver à adopter des comportements sécuritaires au quotidien [35].

Ainsi, de nombreuses études suggèrent qu'une approche proactive (anticiper, former, impliquer) et inclusive (associer tous les niveaux hiérarchiques) favorise la vigilance collective. Lorsqu'elle s'inscrit dans une démarche RSE, la cybersécurité devient un enjeu éthique, augmentant ainsi l'adhésion des collaborateurs.

Weissbrod & Bocken [36] proposent par exemple une approche durable où la cybersécurité est vue comme un devoir éthique de protection des parties prenantes (clients, partenaires, salariés). L'intégration explicite de la sécurité des données dans les engagements RSE rend les enjeux numériques plus concrets et mobilisateurs pour les collaborateurs.

Le rapport EY [37] confirme quant à lui, que les organisations intégrant la cybersécurité dans leur stratégie RSE observent un engagement collaborateur supérieur. IBM, par exemple, a constaté une augmentation de 33 % des détections internes d'incidents après avoir déployé des ateliers collaboratifs autour de la cybersécurité dans son programme RSE.

4.1 Bien-être au travail et susceptibilité au phishing

Comme nous l'avons exposé précédemment, le phishing repose souvent sur l'exploitation d'états émotionnels tels que la fatigue mentale, l'anxiété ou l'urgence perçue [38]. La dégradation des performances humaines en matière de cybersécurité est un facteur de risque

critique qui nécessite une attention immédiate, car les cybercriminels continuent d'exploiter les faiblesses humaines pour accéder aux infrastructures sensibles et critiques [39].

Li & al. [40] ont démontré que les entreprises qui mettent en place des programmes RSE efficaces offrent un soutien social aux employés, ce qui diminue le stress lié à des luttes internes telles que le manque de reconnaissance ou les conflits de valeurs. Un environnement de travail perçu comme juste et éthique permet aux employés de consacrer plus de ressources cognitives à leurs tâches principales. Cette diminution du stress et de la charge cognitive crée un environnement propice à la concentration, ce qui peut réduire la tendance à répondre impulsivement à des menaces telles que le phishing.

D'autre part, en améliorant le climat de confiance, on favorise la communication ouverte, ce qui permet aux employés de signaler rapidement des e-mails suspects ou des comportements inhabituels. Moody et al. [41] ont démontré que la conformité aux politiques de cybersécurité est nettement meilleure dans les entreprises où les salariés perçoivent un engagement sincère de leur organisation envers leur bien-être et leur développement personnel.

En renforçant la culture de vigilance : Les entreprises RSE mettent souvent en place des formations régulières en cybersécurité, intégrées à une culture d'entreprise éthique et respectueuse. [42]

Ces différentes études nous donnent à penser que l'instauration d'une démarche RSE centrée sur le bien-être des collaborateurs favorise un climat de travail plus apaisé et sécurisé, où le sentiment de reconnaissance et d'implication réduit significativement les niveaux de stress. En diminuant la tension quotidienne, les salariés pourraient gagner en vigilance et en lucidité face aux tentatives de phishing en prenant le temps de vérifier l'authenticité des messages, d'alerter leurs collègues ou leur service informatique, et d'adopter les bonnes pratiques de sécurité.

Notre première hypothèse qui prône que la promotion du bien-être psychologique et de la disponibilité cognitive des employés permet d'améliorer l'efficacité des dispositifs de cybersécurité semble donc trouver ici quelques arguments.

4.2 Adopter une approche proactive et inclusive en cybersécurité renforce la vigilance collective

La mobilisation collective des employés, via le partage d'informations et la mise en place de routines collaboratives, apparaît comme une stratégie complémentaire aux défenses techniques. Petrič et Roer [43] ont démontré au cours d'une vaste étude mobilisant plus de 83.300 employés, que les organisations qui instaurent des règles de sécurité claires, adoptées par l'ensemble des collaborateurs, voient une baisse significative du taux de clics sur les liens malveillants.

Bada & Sasse [44] expliquent que l'implication active des employés, plutôt qu'une approche descendante punitive, améliore la vigilance collective. Lorsqu'ils se sentent inclus dans la démarche de sécurité, les collaborateurs s'engagent plus volontiers dans des comportements sûrs. Une sensibilisation continue, contextualisée et valorisant la responsabilité individuelle dans un cadre collectif est bien plus efficace que des campagnes de peur. Dans ce cadre, plusieurs mécanismes rentrent en jeu :

- Sentiment de compétence : lorsque les collaborateurs sont invités à participer activement (par exemple via des ateliers collaboratifs de cybersécurité, des groupes de discussion, des jeux de simulation de phishing), ils développent des compétences concrètes et se sentent outillés pour réagir face aux risques numériques.

- Appropriation des règles : plutôt que de subir des normes de sécurité imposées, les salariés participent à leur co-construction (par exemple en adaptant les règles aux réalités de leur métier). Cette participation renforce leur adhésion émotionnelle aux bonnes pratiques.
- Renforcement de la vigilance collective : lorsque les individus collaborent pour identifier ensemble les menaces (exercices de reconnaissance de phishing, évaluations collectives de risques), ils intègrent progressivement des réflexes de vigilance mutuelle. Dans ces cas, la cybersécurité devient un sujet partagé et coopératif, et non une responsabilité individuelle isolée.

Hadlington [45] montre que l'amélioration des attitudes et perceptions de la cybersécurité chez les salariés, par une approche participative, réduit leur impulsivité face aux risques et augmente la vigilance.

On le voit ici, des employés épanouis, soutenus par une démarche RSE, semblent être plus enclins à développer une approche collaborative, qui optimise la vigilance et la capacité collective à anticiper et neutraliser ces cybermenaces, ce qui ferait écho à notre seconde hypothèse.

5 - CONCLUSION

L'intégration de la RSE dans la stratégie d'entreprise ne se limite pas à un simple outil de gestion de l'image, mais devient un levier puissant pour favoriser l'épanouissement des employés, renforcer la collaboration au sein des équipes et encourager une implication accrue dans la cybersécurité. Ces initiatives participent à la création d'un environnement de travail où chaque collaborateur se sent valorisé et engagé, contribuant ainsi à une culture d'entreprise responsable et résiliente face aux défis numériques actuels.

En favorisant le bien-être au travail, en réduisant le stress et la charge mentale, elle contribue non seulement à une meilleure performance globale, mais aussi à la diminution des risques liés au comportement humain, notamment face au phishing.

Ce lien entre qualité de vie au travail et sécurité informatique est un champ encore peu exploré, mais de plus en plus crucial dans un monde hyperconnecté.

Il conviendrait de mener des études appropriées pour confirmer cette tendance, ce qui conforterait le sujet de la cybersécurité comme essentiel dans une démarche RSE.

Références

- [1] Rhéa E. (2020). Les entreprises à l'épreuve des cyberattaques. *Flux N°121*, pp 90-101
- [2] Rapport Hiscox 2023 sur la gestion des cyber-risques,
https://www.hiscox.fr/courtage/sites/courtage/files/documents/Rapport_Hiscox_sur_la_gestion_des_cyber-risques_2023.pdf
- [3] Meurant S., Cardon R. (2021). La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber-virus ? *Rapport d'information du Sénat n° 678*
- [4] Jones, A. (2024). Human Error Cybersecurity Statistics *Is partners*
<https://www.ispartnersllc.com/blog/human-error-cybersecurity-statistics/>
- [5] Dykstra, J. & Paul, C. L. (2018). Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations. *In 11th USENIX Workshop on Cyber Security Experimentation and Test (CSET 18)*, Baltimore, MD, USENIX Association.
- [6] Cybermailveillance (2023). L'hameçonnage ?
https://www.cybermailveillance.gouv.fr/medias/2022/12/230417_FicheReflexe_Hameconnage.pdf
- [7] Enquête OpinionWay pour Mailinblack (2022). Compétences cyber des salariés : une perception des risques bien différente de la réalité
- [8] Kavvadias, A. & Kotsilieris, T. (2025). Understanding the Role of Demographic and Psychological Factors in Users' Susceptibility to Phishing Emails: A Review. *Applied Sciences*. 15. 2236. 10.3390/app15042236.
- [9] Echouffo-Tcheugui J. B. & al. (2018). Circulating cortisol and cognitive and structural brain measures, The Framingham Heart Study, *Neurology*
- [10] Zhuo, S. (2024). The Impact of Workload on Phishing Susceptibility: An Experiment *NDSS symposium*
<https://www.ndss-symposium.org/wp-content/uploads/usec2024-24-paper.pdf>
- [11] Sapolsky, R. M. (2004). Why Zebras Don't Get Ulcers: The Acclaimed Guide to Stress, Stress-Related Diseases, and Coping. *Henry Holt and Company*.
- [12] Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, Volume 51, pp 69 - 79
- [13] Mather, M., Sutherland, M.R. (2011). Arousal-biased competition in perception and memory. *Perspectives on Psychological Science*, vol 6, 114–133, 10.1177/1745691611400234
- [14] Cialdini, R. B. (2007). Influence: The Psychology of Persuasion Harper Business. *Harper Business*
- [15] Kahneman, D., Tversky, A. (1979) Prospect Theory: An Analysis of Decision under Risk *The Econometric Society* Vol. 47, No. 2, pp. 263-292 <https://doi.org/10.2307/1914185>
- [16] Nasser, G. & al. (2020). The Role of Cue Utilization and Cognitive Load in the Recognition of Phishing Emails. *Frontiers in Big Data*, 3.
- [17] Aguinis H, Glavas A (2019). Sur la responsabilité sociale des entreprises, la création de sens et la recherche de sens au travail *J Manag* 45(3) : 1057–1086
- [18] Kahneman, D. (2011). Pensée lente, pensée rapide. *Sciences Humaines*, 246.
- [19] Hsieh, T. (2010). Delivering happiness: A path to profits, passion, and purpose. *Hachette UK*.

- [20] Grant, A. M. (2013). *A Revolutionary Approach to Success: Give and Take* Viking
- [21] Kelly M. (2015). *The Dream Manager* Hyperion.
- [22] Chaudhary, R. (2018). Corporate social responsibility and employee performance: a study among Indian business executives, *The International Journal of Human Resource Management*, 31(2):1-24 DOI:[10.1080/09585192.2018.1469159](https://doi.org/10.1080/09585192.2018.1469159)
- [23] Aimin, Y. & al. (2020). Can Corporate Social Responsibility Promote Employees' Taking Charge? The Mediating Role of Thriving at Work and the Moderating Role of Task Significance ORIGINAL RESEARCH article *Frontiers Psychology*, Volume 11 <https://doi.org/10.3389/fpsyg.2020.613676>
- [24] Hong, Y., & Roh, T. (2024). The effect of corporate social responsibility on workplace safety: The significance of employees' moral identity. *Behavioral Sciences*, 14(6), 429. <https://doi.org/10.3390/bs14060429>
- [25] Glavas, A., (2016). Corporate Social Responsibility and Employee Engagement: Enabling Employees to Employ More of Their Whole Selves at Work, *Frontiers in Psychology*, doi: 10.3389/fpsyg.2016.00796
- [26] Harvard Business Review, 2019
- [27] Zheng, L., & al. (2022). Impacts of Corporate Social Responsibility on Employees' Mental Fatigue: Employees' Ethical Perspective. *Frontiers in psychology*, 13, 918106. <https://doi.org/10.3389/fpsyg.2022.918106>
- [28] Lazarus, R., & Folkman, S. (1984). *Stress, Appraisal, and Coping* New York Springer
- [29] Wilson, M. G. & al. (2004). Work characteristics and employee health and well-being: Test of a model of healthy work organization *Journal of Occupational and Organizational Psychology*, 77(4), 565–588. <https://doi.org/10.1348/0963179042596522>
- [30] Rupp, E. & al. (2013). Applicants' and Employees' Reactions to Corporate Social Responsibility: The Moderating Effects of First-Party Justice Perceptions and Moral Identity *Personnel Psychology*, vol 64, pp 895-933 <https://doi.org/10.1111/peps.12030>
- [31] Crawford, ER. & Al Linking job demands and resources to employee engagement and burnout: A theoretical extension and meta-analytic test (2010). *Journal of Applied Psychology*, Vol 95(5), pp 834-848
- [32] Great Place to Work (2021). <https://www.greatplacetowork.fr/>
- [33] Schwartz, M. S., & Carroll, A. B. (2003). Corporate social responsibility: A three-domain approach. *Business Ethics Quarterly*, 13(4), 503-530.
- [34] Gallup (2019). State of the Global Workplace Report.
- [35] Deloitte (2020). The 2020 Global Cybersecurity Survey.
- [36] Weissbrod, I., & Bocken, N. M. (2017). Developing sustainable business models: a capability approach. *Journal of Cleaner Production*, 140.
- [37] EY Global Information Security Survey (2020). How do you turn cybersecurity into a source of value? https://www.ey.com/en_hu/giss
- [38] Arevalo, D. & al. (2023). Human and Cognitive Factors involved in Phishing Detection A Literature Review *Congress in Computer Science (CSCE)*, pp. 608-614 doi 10.1109/CSCE60160.2023.00105.
- [39] Nobles, C. (2022). Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem *HOLISTICA – Journal of Business and Public Administration* 13(1):49-72 DOI:10.2478/hjbpa-2022-0003

- [40] Li, C., Lu, J., & Liu, Y. (2022). Corporate Social Responsibility and Employee Well-Being: A Moderated Mediation Model of Organizational Identification and Moral Identity *Behavioral Sciences*, 12(3), 57.
- [41] Moody, G. D., & Lowry, P. B. (2018). Information security policies compliance in a global setting. *Computers & Security*, 75, 1–21. <https://doi.org/10.1016/j.cose.2018.01.003>
- [42] Uchendu, B. (2011). Developing a cyber security culture: Current practices and future needs *Computers & Security*, Volume 109 <https://doi.org/10.1016/j.cose.2021.102387>
- [43] Petrič G., Roer K. (2021). The impact of formal and informal organizational norms on susceptibility to phishing: Combining survey and field experiment data *Telematics and Informatics* 67 DOI:[10.1016/j.tele.2021.101766](https://doi.org/10.1016/j.tele.2021.101766)
- [44] Bada, M., & Sasse, M. A. (2015). Cyber security awareness campaigns: why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society, University College London*.
- [45] Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7).