Vers des environnements capacitants pour la cybersécurité : Proposition d'un cadre de recherche adapté

Ayoub Bourhim, Laurent Guillet, Julie Lassalle, Christine Petr

Bourhim A. Petr C., Guillet L. et Lassalle J. (2023), Vers des environnements capacitants pour la cybersécurité : Proposition d'un cadre de recherche adapté, 12ième Colloque EPIQUE-ARPEGE (Association pour la Recherche en Psychologie Ergonomique et Ergonomie), Ecole du Val de Grâce - Paris (75), 4-7 Juillet.

ÉPIQUE 2023

Vers des environnements capacitants pour la cybersécurité : Proposition d'un cadre de recherche adapté.

Ayoub Bourhim, Laurent Guillet, Julie Lassalle, Christine Petr

Laboratoire des sciences et techniques de l'information, de la communication et de la connaissance ;

Laboratoire d'Économie et de Gestion de l'Ouest ;

Université Bretagne Sud ;

ayoub.bourhim@univ-ubs.fr

laurent.guillet@univ-ubs.fr

julie.lassalle@univ-ubs.fr

christine.petr@univ-ubs.fr

Catégorie de soumission : communication affichée (poster)

RÉSUMÉ

La cybersécurité est un des défis de l'industrie moderne avec le développement de la technologie et d'internet au cours des dernières années. L'humain est souvent caractérisé par les experts de la cybersécurité comme le « maillon faible » de la chaîne de la cybersécurité. Ce postulat se base sur le paradigme de « L'erreur humaine » qui suppose que les failles de sécurité seraient principalement dues aux facteurs individuels. Cependant la littérature montre que les contraintes liées au travail ainsi que la nature de l'environnement ont un poids important sur l'individu et les risques cyber, remettant en cause le paradigme de « l'erreur humaine ». Afin de pallier aux risques cyber, les organisations ont tendance à investir dans des solutions techniques ou à mettre en place des politiques visant à contrôler l'individu. Ce papier propose une approche systémique et dynamique de la cybersécurité dans l'objectif d'amener à un questionnement sur les éléments permettant la mise en place d'environnement capacitants pour la cybersécurité.

MOTS-CLÉS

Cybersécurité, Environnements capacitants, Risque, Acteurs, Organisation

---

1. INTRODUCTION

Avec la démocratisation d'internet au cours des dernières années, la question de la cybersécurité est devenue primordiale dans le domaine de l'industrie, dans notre vie professionnelle et privée. La cybersécurité peut être définie comme « l'ensemble des processus, capacités ou états par lesquels les systèmes d'information et de communication ainsi que les informations qu'ils contiennent sont protégés et/ou défendus contre les dommages et les exploitations et modifications non autorisées. » (Notre traduction de la définition du NICCS, 2022). Alors que le monde économique et industriel est en pleine transition vers un modèle connecté avec l'industrie 4.0 (Lezzi et al., 2018), le nombre d'entreprises en France ayant subi au moins une cyber-attaque s'élève à 45% (rapport de 2023 du CESIN). De plus, un rapport publié par McAfee (Smith et al., 2020) estime le coût global de la

cybercriminalité entre 2018 et 2020 à 1 trillion de dollars. Cependant, afin de mieux gérer les risques cyber, la plupart des organisations favorisent des solutions techniques plutôt que d'investir dans le développement des compétences humaines. Les individus utilisateurs sont souvent considérés comme « le maillon faible » de la chaîne de la cybersécurité (Mouchoux, 2021). L'objectif de cette recherche est de contribuer à la mise en place d'environnement capacitant pour la cybersécurité. Le but est de faire de l'humain un atout pour l'organisation dans la gestion des risques cyber plutôt qu'un potentiel de dysfonctionnements au vu de ses usages effectifs du numérique.

Pour préciser les cadres analytiques à considérer, dans un premier temps, les facteurs individuels à l'origine de la prise de risque chez les personnes utilisatrices seront détaillés. Dans un second temps, les déterminants contextuels et situationnels des risques cyber au sein de l'organisation seront abordés. Enfin, dans un troisième temps, l'approche envisagée pour la recherche sera développée.

2. LES FACTEURS INDIVIDUELS CONDUISANT À UN RISQUE CYBER

Il existe plusieurs facteurs pouvant favoriser la prise de risque à un niveau individuel :

- Le biais de surconfiance se caractérise par un niveau de confiance inadapté envers ses propres compétences et les capacités de la structure d'appartenance en matière de cybersécurité (Cain et al., 2018; De La Garza et al., 2022);
- La dilution de la responsabilité concerne le fait de ne pas intervenir lorsqu'un événement négatif survient en considérant qu'il n'est pas de notre responsabilité d'agir ou qu'une autre personne va intervenir. Dans le cadre de la cybersécurité, cela peut être par exemple une personne employée qui ne signale pas la réception d'un mail frauduleux estimant que cette action n'est pas de son ressort ;
- L'impression de crédibilité de l'émetteur et du message : des études ont montré que les êtres humains sont très sensibles à la crédibilité de l'émetteur (De La Garza et al., 2022) Ainsi, un hacker va chercher à exploiter cette sensibilité par une vigilance accrue au niveau de crédibilité de son attaque, par exemple, via des mails imitant ceux d'organisations connues pour inciter l'individu à cliquer sur un lien frauduleux.

Pour une revue exhaustive des relations entre biais cognitifs et cybersécurité, voir Wang et al., 2021.

Ces différents biais et heuristiques ne doivent toutefois pas être considérés comme des problèmes en soi. En effet, ces stratégies existent dans le but d'alléger la charge mentale des individus afin qu'ils puissent fonctionner de façon optimale et contribuent ainsi à notre bien-être Dans le cadre de la cybersécurité, ce sont précisément ces moments de surcharge cognitive, pendant lesquels les biais mentionnés s'activent pour la réduire, que les attaquants vont exploiter pour mener à bien leurs actions malveillantes. Par exemple, les attaquants visent les heures de pointe pour envoyer des mails frauduleux (De La Garza et al., 2022). Ce type de techniques de manipulation est répandu.

3. LES DÉTERMINANTS CONTEXTUELS ET SITUATIONNELS DES RISQUES CYBER

L'environnement et les conditions de travail ont également un impact important sur les ressources cognitives des individus pour prendre des décisions adaptées et sur leur perception des risques. La surcharge de travail chez les personnes employées peut entraîner une surcharge cognitive et donc favoriser les comportements à risques (Kadena & Gupi, 2021). De la Garza et al. (2022) mettent en avant l'effet de la pression temporelle sur les pratiques en cybersécurité. Cette pression est à l'origine d'émotions négatives chez les personnes employées et génère du stress, de l'anxiété et une peur de l'échec. Les personnes employées sont donc plus susceptibles d'être moins vigilantes et de contourner les politiques de sécurité afin d'atteindre leurs objectifs. Triplett (2022) montre que la charge de travail non planifiée (c'est-à-dire celle qui se rajoute au plan de travail déjà établi) est un facteur de risques en matière de cybersécurité. Cette littérature sur le poids de l'organisation et des contraintes de travail remet en cause le paradigme de l'erreur humaine comme variable clef du risque cyber où l'humain est considéré comme la source principale des brèches de sécurité en cybersécurité.

Bourhim A. Petr C., Guillet L. et Lassalle J. (2023), Vers des environnements capacitants pour la cybersécurité : Proposition d'un cadre de recherche adapté, 12ième Colloque EPIQUE-ARPEGE (Association pour la Recherche en Psychologie Ergonomique et Ergonomie), Ecole du Val de Grâce - Paris (75), 4-7 Juillet.

En plus des contraintes liées à l'environnement et aux conditions de travail, l'organisation de l'entreprise, sa méthode de communication sur la gestion des risques, et la communication entre les différents groupes d'acteurs sont des éléments qui peuvent fragiliser la sécurité numérique de l'entreprise. La façon dont l'organisation va communiquer sur la cybersécurité est aussi un facteur à prendre en compte. Beaucoup d'entreprises se reposent sur un système basé sur la sanction. Des études ont montré que cela pousse les personnes employées à cacher leurs erreurs plutôt qu'à les rapporter dans une visée d'amélioration collective (Danet, 2021). Pour rappel, il existe globalement un manque d'investissement de la part des entreprises dans la formation des individus utilisateurs (Triplett, 2022). Cela ne participe pas à créer des environnements de travail favorables au développement des connaissances des personnes employées et à des usages numériques adaptés du point de vue de la cybersécurité.

Enfin, la cohésion au sein de l'organisation et la qualité des échanges entre les différents groupes d'acteurs à un impact sur le niveau de cybersécurité. Une communication et des politiques de cybersécurité émises par la gouvernance de l'organisation qui ne prennent pas en compte les besoins des personnes employées et ceux de leur activité peuvent être contraignantes du point de vue de la tâche à réaliser ou ne pas être acceptées. *In fine*, elles peuvent conduire à des comportements à risques (Moustafa et al., 2021) parce qu'elles vont potentiellement entraver le travail des personnes employées.

4. L 'APPROCHE DE LA RECHERCHE : MODÈLES STRUCTURANTS ET CONCEPTUALISATION POSITIVE DU FACTEUR HUMAIN

Pour répondre à la problématique du **développement des compétences en cybersécurité des individus et des organisations**, le choix se porte d'une part sur une approche systémique dans laquelle l'ensemble des parties prenantes de la cybersécurité d'une organisation sont intégrées, et d'autre part, sur le facteur humain envisagé de manière positive comme une ressource. Dans cette perspective, **l'humain n'est plus considéré comme un facteur, mais comme un acteur de son environnement et de son activité.**

Concernant l'humain, deux postulats se dégagent dans la littérature. Le premier postulat considère l'humain comme une source de défaillance et cherche à y remédier par des solutions techniques. Cette approche est réductrice car elle n'intègre pas le poids de l'organisation et des facteurs systémiques, est centrée sur la défaillance et passe par l'imposition de droits selon des niveaux de sécurité. Elle est très répandue chez les ingénieurs qui ont tendance à considérer l'individu utilisateur comme la principale source de problème, illustrée par l'adage « Le problème se trouve entre le clavier et la chaise. » (Dejours, 2022 ; Mouchoux, 2021). Le second postulat est celui qui adopte à l'inverse une vision du développement des compétences et des ressources des individus comme une solution aux problématiques de cybersécurité. **L'objectif est alors de développer la compétence et l'autonomie des individus par la proposition d'environnements** qui développent les possibilités d'action des individus dans le domaine plutôt que de sanctionner et contraindre. La sécurité dans ce modèle est une conséquence des conditions de réalisation de l'activité au sens où si un individu utilisateur à une meilleure maîtrise de l'outil et évolue dans un environnement lui permettant de faire usage de ses compétences, alors le risque d'incidents s'en trouve réduit (Dejours, 2022; Raspaud & Falzon, 2020).

Dans ce contexte, nous proposons de nous appuyer sur des modèles structurants de la sécurité. Il existe dans la littérature sur la sécurité un concept similaire au paradigme de l'erreur humaine, « l'attribution excessive de la cause des accidents aux opérateurs de première ligne » (Amalberti, 2013). Pour y pallier plusieurs modèles prenant en compte la « chaîne d'erreurs » ont été avancés notamment le modèle des dominos de Heinrich (1931) ou encore le « Swiss Cheese Model » de Reason (2000). Ces modèles présentent déjà une vision systémique de la sécurité, c'est-à-dire qui repose sur les différentes composantes de l'organisation. Cependant ils restent très linéaires et ne prennent pas

Bourhim A. Petr C., Guillet L. et Lassalle J. (2023), Vers des environnements capacitants pour la cybersécurité : Proposition d'un cadre de recherche adapté, 12ième Colloque EPIQUE-ARPEGE (Association pour la Recherche en Psychologie Ergonomique et Ergonomie), Ecole du Val de Grâce - Paris (75), 4-7 Juillet.

en compte les interactions que les différents éléments de la structure ont les uns sur les autres. Ces modèles se concentrent sur les failles de chacune des parties dans une approche « bottom up » de la sécurité, ce qui peut être considéré comme obsolète dans le cas de la cybersécurité qui est dynamique de nature. (Amalberti, 2013). Dans le cas de la cybersécurité on préfèrera un modèle comme celui de LeCoze (2013a, 2016) qui prend en compte les interactions entre les différentes parties prenantes de la structure (ainsi que les influences extérieures) à différents niveaux d'interactions.

Combinant une approche systémique et dynamique du risque et de la sécurité et un postulat du facteur humain comme une ressource (acteur humain), l'ambition est ici **de déterminer comment contribuer à la conception d'environnements capacitants au service de l'amélioration de la cybersécurité** au sein des organisations. Les environnements capacitants peuvent être entendus comme des environnements de travail permettant au personnel de développer et d'exploiter leurs compétences (Raspaud & Falzon, 2020). Pour répondre cette problématique, nos premiers objectifs de recherche visent à **identifier les éléments favorisant** le développement d'environnements de travail favorables à l'accroissement des compétences cyber des individus, à savoir :

- **Au niveau des individus** : Quelles sont les caractéristiques de la perception du risque cyber et les stratégies individuelles de prise de décision qui expliquent l'acquisition de compétences cyber ?

- **Au niveau de l'organisation** : Quels sont les éléments organisationnels, qu'il s'agisse du fonctionnement et de la communication interne de l'employeur, qui contribuent à l'accroissement des compétences cyber de ses employés ?

- **Comment une coopération entre ses différents éléments peut favoriser le développement des compétences des individus en cybersécurité ?**

5. BIBLIOGRAPHIE

Amalberti, R. (2013). Piloter la sécurité. https://doi.org/10.1007/978-2-8178-0369-2

Bailey, T., Kolo, B., Rajagopalan, K., & Ware, D. (2019). *Perspectives on transforming cybersecurity* (Digital McKinsey and Global Risk Practice).

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36-45. https://doi.org/10.1016/j.jisa.2018.08.002

Danet, D. (2021). *Punish and Perish : The Human Factor in Cybersecurity*. 8.

De La Garza, C., Stoessel, C., & Oufi, N. (2022). *Prise en compte des Facteurs Organisationnels Humains en cybersécurité : Aller au-delà de l'erreur humaine*. 42ème Congrès Lambda Mu de l'IMdR, EDF Lab Paris Saclay.

Dejours, C. (2022). *Introduction: Vol. 8 éd.* (p. 6-22). Presses Universitaires de France.

Glossary | NICCS. Consulté 2 février 2023, à l'adresse https://niccs.cisa.gov/cybersecurity-career-resources/glossary

Kadena, E., & Gupi, M. (2021). HUMAN FACTORS IN CYBERSECURITY : RISKS AND IMPACTS. *Security Science Journal*, *2*(2), Art. 2.

Le Coze, J.-C. (2016). *Trente ans d'accidents : Le nouveau visage des risques sociotechnologiques*. Octarès éditions.

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature : A reference framework. *Computers in Industry*, *103*, 97-110. https://doi.org/10.1016/j.compind.2018.09.004

Mouchoux, R. (2021, septembre 17). The H-Factor : Turning Human Into The Strongest Link Of Your Cybersecurity Strategy. *Conquer Your Risk*.

Bourhim A. Petr C., Guillet L. et Lassalle J. (2023), Vers des environnements capacitants pour la cybersécurité : Proposition d'un cadre de recherche adapté, 12ième Colloque EPIQUE-ARPEGE (Association pour la Recherche en Psychologie Ergonomique et Ergonomie), Ecole du Val de Grâce - Paris (75), 4-7 Juillet.

Raspaud, A., & Falzon, P. (2020). De Sen à la pratique ergonomique : Conditions et moyens pour une intervention ergonomique capacitante. *Perspectives interdisciplinaires sur le travail et la santé*, *22-1*, Art. 22-1. https://doi.org/10.4000/pistes.6753

Reason, J. (2000). Human error : Models and management. *BMJ : British Medical Journal*, *320*(7237), 768-770.

Smith, Z. M., Lostri, E., & Lewis, J. A. (2020). *The Hidden Costs of Cybercrime*. 38.

Triplett, W. J. (2022). Addressing Human Factors in Cybersecurity Leadership. *Journal of Cybersecurity and Privacy*, *2*(3), Art. 3. https://doi.org/10.3390/jcp2030029

Wang, Z., Zhu, H., & Sun, L. (2021). Social Engineering in Cybersecurity : Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access*, *9*, 11895-11910. https://doi.org/10.1109/ACCESS.2021.3051633