Développer des environnements de travail favorables à l'accroissement des compétences cyber des individus

Ayoub Bourhim, Julie Lassalle, Laurent Guillet, Christine Petr

Développer des environnements de travail favorables à l'accroissement des compétences cyber des individus

Auteurs : Ayoub Bourhim, Julie Lassalle, Laurent Guillet, Christine Petr

Un rapport publié par McAfee en 2020 estime le coût global de la cybercriminalité de 2018 à 2020 à 1 trillion de dollars. Alors que le monde économique et industriel est en pleine transition vers un modèle connecté avec l'industrie 4.0, la question de la cybersécurité est primordiale car elle touche tout autant les actifs stratégiques matériels et immatériels que la gestion des unités de production et de distribution (Lezzi et al., 2018). Afin de pallier les risques cyber, les organisations investissent souvent dans des solutions techniques plutôt que dans les acteurs humains (Bailey et al., 2018)

Ce choix s'explique par une position technicienne des enjeux de protection numérique dans laquelle l'humain est souvent caractérisé par les experts de la cybersécurité comme le « maillon faible » de la chaîne. Ce postulat est celui de « l'erreur humaine » qui suppose que les failles de sécurité seraient principalement dues aux facteurs individuels comme les biais cognitifs (Dejours, 2022 ; Mouchoux, 2021). Afin d'y faire face, les organisations ont recours à des politiques protectrices qui cherchent à contrôler les comportements des individus en s'appuyant sur l'application de sanctions (Mouchoux, 2021).

Bien que les caractères individuels soient un facteur important, la littérature a montré que des éléments contextuels liés à l'environnement de travail et à l'organisation ont un poids sur la perception du risque et la capacité des employés à prendre des décisions adaptées. Des facteurs, comme la pression temporelle qui va générer du stress chez les employés ce qui les rend plus susceptibles d'une perte de vigilance, permettent de questionner le paradigme de l'erreur humaine comme variable principale du risque cyber (De La Garza et al., 2022).

Basé sur ces éléments, une approche alternative consiste à considérer l'humain positivement. En effet, l'humain est une ressource et un acteur de son environnement (Dejours, 2022). L'objectif est alors la mise en place d'environnements de travail permettant de développer les compétences, les capacités d'actions et l'autonomie des employés, ce que l'on nomme les environnements capacitants. Dans ce modèle, on suppose que la sécurité est une conséquence de l'environnement. Si un individu se trouve dans un environnement de travail lui permettant de faire usage de ses compétences et d'avoir une meilleure maîtrise de son activité, alors le risque s'en trouve diminué. (Falzon, 2010 ; Raspaud & Falzon, 2020).

Dans cette perspective, nous engageons un projet de recherche combinant cette approche avec un modèle systémique de la sécurité basé sur les travaux de Reason (2000) et LeCoze (2016). Notre projet est de contribuer à la mise en place d'environnements capacitants permettant *in fine* l'amélioration de la cybersécurité dans les organisations. La mise en place de tels environnements impose un diagnostic de la structure et exige une conception impliquant les différents groupes d'acteurs pour s'assurer que les individus puissent effectivement développer leur pouvoir d'agir en matière de cybersécurité.

Dans notre présentation, nous développerons les principales étapes et les verrous tant conceptuels que méthodologiques et d'accès aux terrains empiriques que notre recherche devra lever.

Références :

Bailey, T., Kolo, B., Rajagopalan, K., & Ware, D. (2019). *Perspectives on transforming cybersecurity*

(Digital McKinsey and Global Risk Practice).

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.

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.

Mouchoux, R. (2021, septembre 17). The H-Factor : Turning Human Into The Strongest Link Of Your Cybersecurity Strategy. *Conquer Your Risk*. https://www.conquer-your-risk.com/2021/09/17/the-h-factor-turning-human-into-the-strongest-link-of-your-cybersecurity-strategy/

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., E. Lostri, and J. A. Lewis. 2021. The hidden costs of cybercrime. https://www.csis.org/analysis/hidden-costs-cybercrime.