Identifying Tensions Within Organizations: The Contribution of Engeström's Model to Cybersecurity

Identification des tensions au sein des organisations : Apport du modèle d'Engeström en cybersécurité.

Ayoub Bourhim [1-2-3], Julie Lassalle[1-3], Laurent Guillet[1-3]and Christine Petr[1-2]

[1] Université Bretagne Sud, France
[2] Laboratoire de Gestion de l'Ouest, Vannes, France
[3] Laboratoire des sciences et techniques de l'information, de la communication et de la connaissance, Lorient, France
ayoub.bourhim@univ-ubs.fr +33668794872
julie.lassalle@univ-ubs.fr +33689293679
laurent.guillet@univ-ubs.fr +33668402262
christine.petr@univ-us.fr +33641970959
17 Bd Flandres Dunkerque 1940, 56100 Lorient

Abstract. This study challenges the human error paradigm by highlighting the impact of organizational tensions on cybersecurity. By adopting a systemic perspective based on Engeström's model, we identify tensions in the form of contradictions within the model and propose solutions centered on collaboration among the organization's actors. This approach offers a better understanding of the system's internal dynamics, aiming to strengthen organizational resilience and improve the prevention of cyberattacks.

Cette étude remet en question le paradigme de l'erreur humaine en soulignant l'impact des tensions organisationnelles sur la cybersécurité. En adoptant une perspective systémique basée sur le modèle d'Engeström, nous identifions les tensions sous forme de contradictions dans le modèle et proposons des solutions centrées sur la collaboration entre les acteurs de l'organisation. Cette approche offre une meilleure compréhension des dynamiques internes, visant à renforcer la résilience organisationnelle et à améliorer la prévention des cyberattaques.

Keywords: Cybersecurity, Human Approach, Organizational Tensions, Activity Theory

Introduction :

Ces dernières années, une intensification des cyberattaques, à l'encontre des organisations, a été observée. On peut citer la campagne d'hameçonnage vocal ayant coûté cent millions de dollars en pertes à la compagnie d'hôtels et casinos MGM, ou encore la faille de sécurité de la Commission électorale britannique ayant exposé les données de 40 millions d'électeurs.

Dans les deux cas, la responsabilité des incidents est attribuée à "l'Erreur Humaine". Grandement influencé par la prévalence et l'efficacité des attaques basées sur l'ingénierie sociale, le paradigme de "l'Erreur Humaine" fait reposer la responsabilité des failles de sécurité d'une organisation sur les individus qui évoluent en son sein (Hweidi & Eleyan, 2023). Cette simplification d'une problématique alarmante a amené les organisations à chercher des solutions aux problèmes de cybersécurité en investissant dans la technique ou des politiques ayant pour objectif de contrôler les individus, avec peu de succès observables (Bada et al., 2015; Smith et al., 2020; NCSC, 2019).

Se focaliser uniquement sur l'erreur humaine revient à "regarder l'arbre et ignorer la forêt". En effet, un certain nombre d'auteurs mettent en avant le fait que les comportements individuels sont influencés par les contraintes organisationnelles. Ils rejettent la thèse de l'humain comme "le lien le plus faible" de la chaîne de la cybersécurité. De La Garza et al. (2022) ont mis en évidence que des éléments comme la pression temporelle ou le manque de communication sont des facteurs de risques cyber.

La cybersécurité étant un enjeu crucial pour la confiance des consommateurs et la réputation des entreprises (Dimitriadis, 2023), il est essentiel d'adopter une vision holistique qui englobe à la fois les comportements humains et les pratiques organisationnelles. C'est pourquoi notre objectif avec cet article est d'explorer, par la mobilisation du modèle d'Engeström, la manière dont les tensions au sein de l'organisation peuvent influencer la cybersécurité. Nous présentons une façon d'identifier et modéliser les tensions internes du système, dans le but de fournir des solutions permettant d'augmenter sa résilience et contribuer à la prévention des attaques.

I. Tensions liées à la cybersécurité au sein des organisations : Un cadre théorique

1- Dépasser le paradigme de l'erreur humaine.

Le paradigme de l'erreur humaine est une actualisation du concept d'attribution de l'erreur à l'opérateur de première ligne, présent dans la littérature concernant la sécurité classique (Amalberti, 2013). Comme évoqué précédemment, cette simplification ignore l'impact que les tensions au sein de l'organisation, peuvent avoir sur les comportements des individus et sur la sécurité. Afin de dépasser ce paradigme, il faut adopter une perspective systémique, dans ce contexte, "le système" correspond à l'ensemble des entités, individus et processus en interaction dans le but d'atteindre un objectif (Engeström, 2015). Pour ce faire, nous nous appuierons sur le modèle de la théorie de l'activité d'Engeström, ainsi que sur les travaux en sciences de gestion sur la structure des organisations et les sources de conflits en leur sein.

2- Le Cas des Universités.

Depuis la pandémie de Covid-19, les universités ont dû adapter et développer leurs environnements numériques pour répondre aux besoins engendrés par la situation sanitaire. Cette transition a accru leur exposition aux risques cybernétiques, en raison de la nature stratégique de ces organisations (Haque et al., 2023; Mohammed & Bamasoud, 2022). Elles détiennent un volume significatif de données sensibles, incluant des informations liées à la recherche, ainsi que des données personnelles concernant leur personnel et, surtout, leurs étudiants, ce qui en fait des cibles privilégiées pour les cyberattaques (Ulven & Wangen, 2021;

Haque et al., 2023). Bien que la recherche sur les pratiques de cybersécurité dans l'enseignement supérieur se développe, elle reste encore lacunaire. Dans ce contexte, elle tend à privilégier des approches centrées sur la régulation des comportements des utilisateurs, particulièrement les étudiants (Ulven & Wangen, 2021; Lallie et al., 2023), ces derniers étant souvent considérés comme des vulnérabilités du système, ce positionnement étant dans la lignée du paradigme de l'erreur humaine dans le traitement des facteurs humains. Hedström et al. (2010) se distinguent par leur approche systémique basée sur une étude de cas d'un incident cyber au sein d'une université. En mobilisant l'Actor Network Theory comme outil d'analyse, ils mettent en évidence que les failles de sécurité résultent souvent d'interactions complexes entre acteurs humains et non-humains, nécessitant un alignement des intérêts au sein des acteurs universitaires.

3- La théorie de l'activité et le modèle d'Engeström.

Le modèle d'Engeström, est un modèle d'analyse systémique basé sur la théorie de l'activité. Ce modèle analyse les systèmes d'activité en tant qu'unités d'analyse, en mettant l'accent sur les interactions entre les différentes composantes, sur la pluralité des voix et les éléments culturels et historiques inhérents au système. Les systèmes d'activité évoluent au fil du temps et subissent des cycles de transformation lorsque l'objet de l'activité est reconceptualisé en raison de changements au sein du système (Engeström, 2001).

a) Le modèle :

Le modèle d'Engeström considère six éléments interagissant entre eux (Fig. 1):

• Le sujet : correspond à l'individu ou entité qui réalise l'activité (ex : la DSI d'une université).

• L'objet : renvoie au but de l'activité, la finalité du système (ex : la sécurité et le maintien de l'université).

• Les outils : correspondent aux processus (physiques ou mentaux) utilisés pour accomplir l'activité (ex : antivirus, sensibilisation à la cybersécurité).

• La communauté : correspond à l'ensemble des individus ou des entités impliqués dans l'activité (ex : la DSI, la gouvernance, les utilisateurs, les autres départements…).

• La division du travail : concerne la manière dont les responsabilités sont réparties dans l'exécution de l'activité (ex : entre les différentes équipes de la DSI, la data protection officer…).

• Les règles : intègrent les normes, politiques et procédures qui régissent l'activité et le système (ex : la charte informatique, les règles d'hygiène numérique, la RGPD…).

Afin de mieux comprendre les tensions internes au sein des organisations au regard des problématiques de cybersécurité, nous nous sommes focalisés sur deux principes du modèle : la multivocalité et les contradictions.

b) Multivocalité et contradictions :

La multivocalité est un concept qui permet de mettre en avant la nature intrinsèquement multiple des systèmes d'activités. Un système d'activité concentre en lui les différents points de vue de ses acteurs. La multivocalité reflète l'éventail des perspectives présentes au sein du système d'activité. Le système d'activité étant l'unité fondamentale de mesure de l'activité, il peut se décomposer en sous-systèmes à la manière de poupées russes. Cette structuration permet une vision holistique du système à ces niveaux macro, méso et micro. Par exemple, les normes de cybersécurité sont perçues par la DSI et la gouvernance comme des outils permettant d'assurer la sécurité du système, tandis que pour les autres membres de la

communauté (enseignements, personnel administratif, etc.) elles sont perçues comme des règles. Cette diversité de voix et de perceptions peut être à l'origine de tensions, notamment dans des systèmes complexes comme les organisations. Ces tensions sont qualifiées par Engeström de "contradictions".

Autre principe central du modèle d'Engeström, les contradictions représentent les tensions au sein du système d'activité, notamment entre ses différentes composantes. Ces points de friction sont considérés comme les moteurs du changement et du développement du système. Engeström identifie 4 niveaux de contradictions :

• Contradictions primaires : elles surviennent à l'intérieur d'une même composante du système d'activité. Par exemple, entre deux outils de cybersécurité ou deux règles contradictoires,

• Contradictions secondaires : elles apparaissent entre deux composantes différentes. Par exemple, entre une règle de sécurité et un outil,

• Contradictions tertiaires : elles se produisent lorsqu'une nouvelle pratique ou une nouvelle version du système d'activité entre en conflit avec la version actuelle de ce dernier. Par exemple, l'introduction d'un nouvel outil qui ne respecte pas les protocoles de sécurité,

• Contradictions quaternaires : ces contradictions apparaissent entre plusieurs systèmes d'activité interconnectés, comme entre une entreprise et ses partenaires externes.

Les contradictions représentent des points de tension dans le système d'activité qui, si elles ne sont pas résolues, vont nuire à l'efficacité du système et affecter aussi bien son fonctionnement que sa sécurité.

II - Méthodologie

1- Contexte

Le travail présenté ici est une analyse approfondie de travaux de modélisation du système de cybersécurité de l'Université Bretagne Sud (UBS), à travers les perspectives fournies par les sciences de gestion. Cette université est notamment connue pour son pôle de formation en cybersécurité. Depuis la pandémie de Covid-19, le nombre de cyberattaques contre l'établissement a augmenté de façon exponentielle, comme en ont témoigné les membres du personnel de l'université. Pour l'UBS, la cybersécurité n'est pas seulement une question de sécurité, mais aussi une question d'image de marque, l'université étant reconnue pour sa formation d'ingénieurs en cyberdéfense. Ce contexte en fait un terrain pertinent pour l'identification des tensions organisationnelles liées à la cybersécurité. Nous présenterons dans les sections suivantes une étude de cas d'un conflit autour des enjeux de cybersécurité au sein de l'organisation.

2- Collecte des données

Dans le cadre de notre analyse du système de l'UBS, nous avons opté pour une approche qualitative, basée sur la méthodologie employée par Engeström et d'autres chercheurs ayant choisi ce modèle pour analyser des systèmes complexes (Engeström, 2001; Mwanza, 2001; Schroder et al., 2020). Ce choix méthodologique s'inscrit dans une volonté de rompre avec les approches classiques centrées sur l'erreur humaine en cybersécurité, qui se limitent souvent à l'évaluation des risques. Nous cherchons à comprendre la complexité des interactions entre les acteurs du système et l'impact de ces relations sur le fonctionnement du système, notamment au regard des impératifs de cybersécurité. Une approche qualitative permet de capturer ces dynamiques et de faire ressortir un niveau de nuance qui peut être plus difficile à obtenir en employant des méthodes quantitatives.

Huit entretiens individuels semi-directifs avec des membres clés du personnel ont été réalisés auprès de notamment ceux de la direction des systèmes d'information (DSI), l'officier de protection des données (DPO) et la présidente de l'université. Chaque entretien a duré environ une heure. La grille d'entretien a été construite en s'appuyant sur le modèle de l'activité d'Engeström, avec des questions spécifiquement liées à chaque composante du modèle. Nous avons également exploré les contraintes que les acteurs rencontrent dans la mise en œuvre de la cybersécurité, dans le but de faire émerger les contradictions.

A titre illustratif, un exemple de question pour chaque composante du système interrogée est donné ci-dessous, voici une sélection de questions illustrant ce travail :

• Objet : quelle est la fonction de la cybersécurité au sein de l'Université Bretagne Sud ?

• Sujets : quels sont les différents profils des personnes impliquées dans la cybersécurité à l'université ?

• Communauté : comment la cybersécurité est-elle organisée à l'Université Bretagne Sud ?

• Outils : pourquoi ces processus ont-ils été choisis pour assurer la cybersécurité à l'université ?

• Règles : quelles sont les conséquences en cas de violation des règles de cybersécurité ?

• Division du travail : comment les responsabilités en matière de cybersécurité sont-elles réparties ?

• Contradictions : quelles sont les contraintes que vous rencontrez dans la mise en œuvre de la cybersécurité ?

3- Analyse des entretiens

Afin d'analyser le matériel collecté, le corpus d'entretiens a été entièrement retranscrit et analysé à l'aide du logiciel NVivo. Le logiciel permet de coder thématiquement le corpus en fonction des liens avec le modèle d'Engeström. Un premier codage a eu lieu afin d'établir la modélisation du système d'activité de la DSI et des éléments gravitant autour de la cybersécurité à l'UBS. Il s'agit d'une modélisation partielle du système d'activité de l'UBS à travers la lentille de la cybersécurité. Une autre partie du codage s'est concentrée sur l'identification des contradictions au sein du système présentes dans le corpus, ce qui a permis d'établir une liste des types de contradictions. Le codage des contradictions nous a également permis d'établir une liste d'incidents ayant conduit à des problèmes pour la cybersécurité de l'UBS. Nous présenterons l'analyse d'un de ces incidents dans la partie résultats.

III- Résultats

Pour nos résultats, nous avons choisi de présenter l'étude de cas d'un incident impliquant deux départements de l'UBS (Fig. 1). Avant d'établir les faits de l'incident, il nous faut présenter les observations faites sur le système dans son ensemble. Premièrement, les résultats montrent que l'objectif du système de l'UBS consiste à la fois à : "Enseigner" aux étudiants et à "Développer de la recherche". Ensuite, l'UBS est un système complexe soutenu par un nombre important de sous-systèmes, chacun ayant des objectifs propres mais qui ont pour but de soutenir celui de l'organisation. L'UBS ne peut pas atteindre ses objectifs sans le soutien de tous ses sous-systèmes ; l'incident présente une contradiction entre deux d'entre eux.

Le premier de ces systèmes est celui de la DSI, dont l'objectif est le "Maintien de l'infrastructure technologique de l'UBS", un objectif avec plusieurs facettes incluant la cybersécurité. Lors de la pandémie de COVID-19, la DSI a permis le maintien des cours à distance et d'assurer la continuité de la recherche depuis le domicile du personnel de la recherche, permettant à l'université de poursuivre ses missions. Le second est le département d'écologie qui, dans son objectif de répondre aux objectifs de développement durable, a décidé d'implémenter une application permettant d'évaluer l'empreinte carbone des personnes

employées par l'organisation. La DSI a bloqué cette initiative car le logiciel choisi par le département d'écologie n'était pas conforme aux standards de sécurité. Cette situation conduit à une impasse, où l'évolution du système du département d'écologie est stoppée**.** Cet incident permet d'observer la nature multivocale du système qui affecte aussi les contradictions identifiées.

Si l'on considère l'UBS comme sujet de l'activité, il s'agit à la fois d'une contradiction primaire entre deux membres de sa communauté (DSI et département écologie) et d'une contradiction tertiaire entre une nouvelle version du système d'activité avec l'introduction d'une nouvelle technologie. Si l'on se place au niveau des départements, alors on est face à une contradiction quaternaire entre l'objectif de durabilité du service écologique et l'objectif de sécurité de la DSI. Enfin, au sein des systèmes des deux départements : Pour le département écologie c'est une contradiction secondaire entre un outil et les règles qu'ils doivent respecter, pour la DSI c'est une contradiction primaire entre leur objectif d'assister l'intégration de nouveaux logiciels et leur objectif de sécurité.

Les résultats mettent en avant un rapport historique de compétition entre les deux départements, pour des questions de ressources humaines. Le contexte historique peut être considéré comme facilitateur dans l'émergence de contradictions.

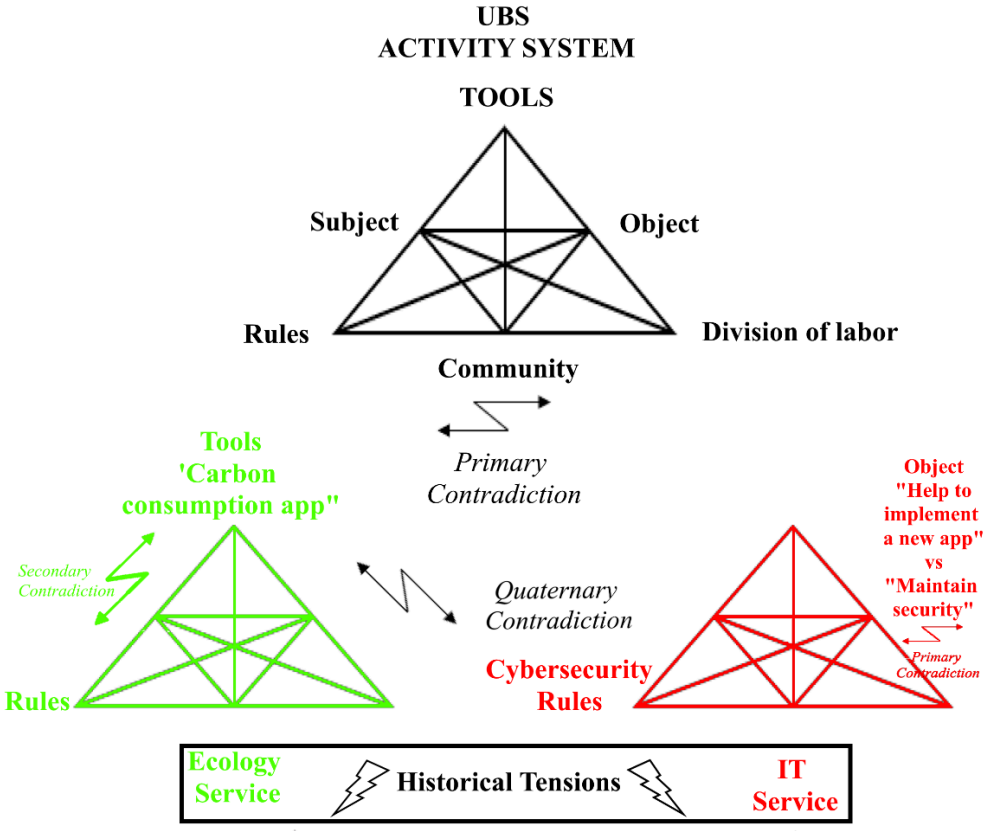

Fig. 1. Représentation des contradictions à l'UBS basé sur Engeström (2015)

IV- Discussion

La cybersécurité est une problématique transversale et ne peut être atteinte que par la participation des différents acteurs du système ; de même pour l'écologie, qui demande un effort commun. Un regret souvent émis par les membres de la DSI lors des entretiens est le manque d'implication dans la conception des projets des autres départements de l'UBS. En effet, ils estiment que s'ils avaient été consultés dès le début du projet, les choses auraient pu se dérouler différemment. Ces résultats sont cohérents avec les observations de Hedström et al. (2010), qui soulignent que les problèmes liés à la complexité des systèmes universitaires, le manque de communication entre les acteurs, les problèmes de ressources et l'échec de l'alignement des intérêts constituent des facteurs de risque cyber pour les universités.

L'usage du modèle d'Engeström a permis de mettre en avant la complexité du système de l'UBS, qui se constitue de plusieurs sous-systèmes. Les contradictions sont en partie attribuables aux interactions entre ces systèmes qui, même s'ils partagent une finalité commune, ont des objectifs différents, mettant en avant la multivocalité du système. La cybersécurité n'opère pas de manière isolée ; elle se confronte à d'autres objectifs du système, qui doit alors apprendre à concilier ces différents sous-systèmes et résoudre ses contradictions s'il veut continuer à évoluer de façon dynamique et augmenter sa résilience et la prévention en matière de cybersécurité.

Le contexte historique, montre que les conflits antérieurs entre les départements, notamment les rapports de compétition, jouent un rôle sur les comportements entre les différents acteurs.

Une question se pose alors : comment résoudre les contradictions dans le système ? Les approches basées sur les méthodes participatives comme les laboratoires du changement (Engestrom et al., 1996) et les environnements capacitants (Falzon, 2010) sont pertinentes. Engestrom (2011) suggère aux managers de créer des Zone Proximales de Développement, impliquant activement les collaborateurs dans la résolution des contradictions. Le but de ces approches est d'encourager la co-construction et de développer le pouvoir d'agir des individus, des collectifs et des organisations dans un domaine (comme la cybersécurité). Il s'agit d'une part de faire prendre conscience aux différents départements de la nature transversale de leurs objectifs, et de coconstruire le système en fonction des besoins des uns et des autres, avec une perspective commune de cybersécurité.

En conclusion, l'utilisation du modèle d'Engeström s'est révélée efficace pour identifier et analyser les contradictions au sein de l'organisation. En mettant en avant la multivocalité et les contradictions entre les sous-systèmes, ce modèle permet de comprendre comment différents objectifs peuvent entrer en conflit malgré une finalité commune. Cette approche systémique a mis en évidence non seulement les tensions actuelles, mais également les dynamiques sous-jacentes influencées par le contexte historique de l'université, comme la réputation de la DSI et les tensions entre les départements, pouvant mener à un ressenti de compétition. Et à donc à revoir le modèle organisationnel de collaboration entre département autour des enjeux de cybersécurité.

Le modèle d'Engeström offre une grille d'analyse pertinente pour déceler les points de tension dans des environnements complexes. Il ne se limite pas à une observation statique des conflits, mais propose un cadre pour envisager des solutions, notamment à travers la co-construction et la participation active des acteurs impliqués. En identifiant les contradictions, il devient possible d'orienter le système vers des approches plus collaboratives, non seulement en cybersécurité, mais également dans la gestion de tout autre enjeu transversal au sein de l'organisation.

V- Bibliographie :

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

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? Dans International Conference on Cyber Security for Sustainable Society (pp. 118-131).

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. Dans 42ème Congrès Lambda Mu de l'IMdR, EDF Lab Paris Saclay.

Dimitriadis, C. (2023). Consumer trust and perspectives on cyber security. Computer Fraud & Security, 2023(5), 11-13. https://doi.org/10.1016/S1361-3723(23)70020-1

Engeström, Y. (2001). Expansive learning at work: Toward an activity theoretical reconceptualization. Journal of Education and Work, 14(1), 133-156. https://doi.org/10.1080/13639080020028747

Engeström, Y. (2011). Théorie de l'activité et management. Management & Avenir, 42(2), 170-182. https://doi.org/10.3917/mav.042.0170

Engeström, Y. (2015). Learning by expanding: An activity-theoretical approach to developmental research (2e éd.). Cambridge University Press.

Engeström, Y., Pihlaja, J., Helle, M., Virkkunen, J., & Poikela, R. (1996). The change laboratory as a tool for transforming work. Lifelong Learning in Europe, 1(2), 10-17.

Haque, M. A., Ahmad, S., John, A., Mishra, K., Mishra, B. K., Kumar, K., & Nazeer, J. (2023). Cybersecurity in Universities : An Evaluation Model. *SN Computer Science*, *4*(5). https://doi.org/10.1007/s42979-023-01984-x

Hedström, K., Dhillon, G., & Karlsson, F. (2010). Using Actor Network Theory to Understand Information Security Management. Dans *IFIP advances in information and communication technology* (p. 43-54). https://doi.org/10.1007/978-3-642-15257-3_5

Hweidi, R. F. A., & Eleyan, D. (2023). Social engineering attack concepts, frameworks, and awareness: A systematic literature review. International Journal of Computing and Digital Systems, 13(1), 691-700. https://doi.org/10.12785/ijcds/130155

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2023). Understanding Cyber Threats Against the Universities, Colleges, and Schools. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2307.07755

Mohammed, M., & Bamasoud, D. M. (2022). The Impact of Enhancing Awareness of Cyber-security on Universities Students: A Survey Paper. J. Theor. Appl. Inf. Technol, 100. Retrieved from https://www.jatit.org/volumes/Vol100No15/19Vol100No15.pdf

Mwanza, D. (2001). Where theory meets practice: A case for an activity theory based methodology to guide computer system design. Dans Proceedings of INTERACT 2001: Eighth IFIP TC 13 Conference on Human-Computer Interaction (pp. 342-349). Tokyo, Japon.

National Cyber Security Centre. (2019). Annual review 2019: Making the UK the safest place to live and work online. https://www.ncsc.gov.uk/annual-review-2019

Schröder, L. U., Wals, A. E. J., & Van Koppen, C. S. A. (2020). Analysing the state of student participation in two eco-schools using Engeström's second generation activity systems model. Environmental Education Research, 26(8), 1088-1111. https://doi.org/10.1080/13504622.2020.1779186

Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, *13*(2), 39. https://doi.org/10.3390/fi13020039