Prise en compte des Facteurs Organisationnels et Humains en cybersécurité : aller au-delà de l'erreur humaine

Cecilia DE LA GARZA, Stoessel Charles, Nora Oufi

Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Prise en compte des Facteurs Organisationnels Humains en cybersécurité : aller au-delà de l'erreur humaine

Organizational and Human Factors of cybersecurity : beyond Human Error

DE LA GARZA Cecilia
EDF Lab Paris-Saclay
7 Av. Gaspard Monge, 91120 Palaiseau
cecilia.de-la-garza@edf.fr

STOESSEL Charles
Opus Citatum Conseil
6, rue d'Armaillé, 75017 Paris
charles.stoessel@opus-citatum.com

OUFI Nora
Cnam
41 rue Gay Lussac 75005 Paris
nora.oufi.auditeur@lecnam.net

Résumé — Ce papier propose une revue de littérature dans le domaine des Facteurs Organisationnels et Humains (FOH) de la cybersécurité. Face à l'accroissement des menaces, il est aujourd'hui vital pour les organisations à risques de comprendre les FOH de la cybersécurité. Ce premier état de l'art concentre l'attention sur trois thèmes : 1) produire une cartographie des acteurs de la cybersécurité et caractériser leur attention aux FOH ; 2) mieux comprendre le comportement des utilisateurs finaux ; 3) mieux saisir ce que représente la prise en compte des FOH en cybersécurité. Nombre d'écrits sur la cybersécurité traitent du Facteur Humain dans le cadre du paradigme de « l'erreur humaine », soulignant l'occurrence de comportements humains dits déviants, inappropriés ou non-sécures, Nous centrerons notre regard sur des études cherchant à comprendre les facteurs explicatifs de ces comportements jugés et les contextes dans lesquels ils surviennent.

Mots-clefs — Cybersécurité, facteurs humains et organisationnels, utilisateur final, conception, comportement humain

Abstract — This paper proposes a literature review in the field of Organizational and Human Factors (OHF) of cybersecurity. Facing the increasing of threats, vital for high-risk industries to better understand the OHF dimensions of cybersecurity. This first state of the art focuses attention on three topics: 1) mapping cybersecurity actors and characterizing their attention to HF, 2) better understand end-user behavior and, 3) better understand what does take HF into account in cybersecurity. Many writings on cybersecurity deal with the Human Factor within the framework of the "human error" paradigm, emphasizing the occurrence of so-called deviant, inappropriate or unsafe human behaviors. To go further, we will focus on studies seeking to understand the explanatory factors of these behaviors and the contexts in which they occur.

Keywords — Cybersecurity, human and organizational factors, end user, design, human behavior

INTRODUCTION

La thématique de la cybersécurité, longtemps restée une affaire de spécialistes et paraissant au public principalement dans des œuvres de fiction, apparaît aujourd'hui sur le devant de la scène. En effet, dans le but de préserver un avenir durable dans le monde du numérique, elle est devenue incontournable pour la maîtrise des risques. Cette communication se propose d'œuvrer à une réflexion sur les Facteurs Organisationnels et Humains visant à limiter l'occurrence de crises cyber, et le cas échéant à limiter les impacts d'une crise cyber sur les ressources humaines et, par effet de ricochet, sur la gestion de crise industrielle conventionnelle. Les attaques massives sur des réseaux d'entreprises (Saint-Gobain en 2017 avec le virus *WannaCry*, ou encore Colonial Pipeline en mai 2021 par un ransomware), dans le cadre de campagnes politiques ou de tensions géostratégiques, ou encore reliées à la thématique de la protection des données personnelles, illustrent bien l'importance de la cybersécurité aujourd'hui, et ce quel que soit le secteur économique. L'enjeu est également international, comme nous le rappelle la cyberattaque par rançongiciel par le virus *NotPeya*, qui n'a pas épargné la France. L'entreprise française spécialisée dans la construction de bâtiments Saint-Gobain a été touchée par le virus et a essuyé des pertes de 384 millions de dollars [1]. Ont également été touchés la banque BNP Paribas, le groupe de distribution Auchan ou le fabricant d'emballages en verre Verallia. A la suite de ces attaques le centre de veille de l'ANSSI, l'Agence Nationale de la Sécurité des Systèmes d'Information, rappelle de quelle façon les récentes vagues de rançongiciels, en particulier *NotPetya*, se sont propagées au sein des SI et indique comment les dégâts peuvent être contenus en appliquant une stratégie appropriée de cloisonnement système et réseau [2].

Aujourd'hui, de nombreux secteurs s'intéressent au risque cyber : industriel, militaire, santé, etc. Et surtout, le monde de la santé étudie de près le sujet, et à plus forte raison depuis la crise sanitaire. L'Association Pour la Sécurité des Systèmes d'Information de santé (APSSIS) a ainsi énoncé que « Le coronavirus semble avoir largement inspiré les cybercriminels puisque le baromètre Signal Spam indique que le phishing aurait augmenté de 600 % sur le mois de mars 2020 » [3]. La cybersécurité est centrale pour les centres de soin, notamment dans le but de sécuriser la confidentialité des données patients, comme le montre par exemple le travail de Sonia Cordon juriste à l'Institut Droit et Santé de la Faculté de droit de Paris. Le besoin grandissant de sécurisation des données médicales des établissements de santé impose ainsi le cadre de développement des réponses apportées [4]. Le monde de la défense est aussi en première ligne. Pour une experte militaire belge, « *Le facteur humain fait également partie des priorités de la cybersécurité* », notamment du fait que les cybercriminels visent généralement moins les systèmes que les utilisateurs, singulièrement dans les attaques au rançongiciel [5].

Il apparaît que la cybersécurité et les FOH sont liés à plus d'un titre. Afin de gagner en clarté au long de cette communication, nous proposerons une typologie d'utilisateurs permettant de mieux saisir leurs rôles et responsabilités respectifs, ainsi que leurs interactions. On distingue ainsi concepteurs de systèmes informatiques et utilisateurs de ces systèmes :

- Expert dédié à la cybersécurité ;
- Professionnel de l'informatique (mais non spécialisé en cybersécurité : développeur d'applications métier, responsables et correspondants informatique, personnels de hotline et helpdesk…) ;
- Employé non-professionnel de l'informatique (parfois appelé également utilisateur final).

Cette typologie s'appuie sur une réflexion plus globale sur les utilisateurs, leur rôle, leurs FOH associés et leur implication dans une crise.

Dans les termes de notre typologie, les utilisateurs non-professionnels des outils numériques peuvent contribuer, malgré eux, à une intrusion de menaces informatiques sur le système informatique de l'entreprise. De même, les experts en cybersécurité, ainsi que les autres professionnels de l'informatique sont des acteurs dont les compétences, les comportements, les décisions et les actions, vont avoir un impact sur la performance cybersécurité globale. En outre, tous les utilisateurs peuvent avoir à faire face à des environnements de travail complètement différents – et dégradés, dans le cas où une cyberattaque mettrait à mal l'intégrité des systèmes informationnels. Les auteurs ont également identifié l'importance de la dimension organisationnelle et de la prise de décision de niveau macroscopique : la cybersécurité peut être vue comme un simple coût, mais aussi comme un avantage concurrentiel ; elle peut être conçue comme strictement technologique, ou être comprise comme reposant sur des compétences humaines à valoriser ; la transparence peut être la stratégie de communication choisie, mais le secret peut aussi représenter une tentation pour certains dirigeants, etc. Toutes ces interrogations montrent l'importance du sujet, sa dimension systémique et multifactorielle, et l'urgence d'instruire le problème au moyen d'une réflexion pluridisciplinaire intégrant les Facteurs Organisationnels et Humains.

I. Comprendre le contexte de la cybersécurité

A. Les acteurs institutionnels de la cybersécurité

Dans cette première partie, nous présenterons l'état de nos recherches visant à disposer d'une cartographie des acteurs de la cybersécurité, de comprendre leur rôle et, le cas échéant, de citer leurs travaux traitant des FOH de la cybersécurité. Le Tableau 1 présente un premier bilan de cette cartographie qui sera à terme exhaustive. Cette cartographie illustre des autorités nationales, aux Etats-Unis et en Europe impliquées dans la veille, la sensibilisation et la formation, la gestion de crise, la défense, des organismes de R&D et des organismes impliqués dans les enquêtes à la suite d'une cyberattaque. Il semblerait que peu d'organismes s'intéressent à une analyse post évènement critique en cyber, au-delà d'une enquête policière ou en cybercriminalité. Or il est nécessaire de comprendre les mécanismes par lesquels une attaque est engendrée et comment les utilisateurs finaux sont impliqués, utilisés, trompés ou autre. Notre réflexion théorique sera orientée donc sur les études Facteurs Organisationnels et Humains (FOH) en vue de contribuer à la prévention.

B. Les utilisateurs impliqués dans les évènements d'atteinte à la cybersécurité

Dans cette deuxième partie, nous présenterons certaines recherches qui traitent de l'impact des utilisateurs sur la cybersécurité des systèmes. Les questions posées sont donc les suivantes :

- Existe-t-il des études empiriques sur les comportements des utilisateurs face au risque cyber, sur les interactions entre utilisateurs et spécialistes cybersécurité ou encore sur les moyens déployés au sein des entreprises (formations, exercices de crise, ReX…) ?
- Existe-t-il des analyses de l'activité des utilisateurs pour mieux comprendre leurs contraintes et contextes d'intervention en relation avec la cybersécurité ?
- Quelles sont les contraintes quotidiennes auxquelles font face les utilisateurs qui pourraient expliquer une forme de « d'inattention » portée au risque cyber (vu des experts) ?

Notre hypothèse de départ est que nombre d'écrits sur la cybersécurité traite du Facteur Humain dans le cadre du paradigme de « l'erreur humaine ». Nombre de travaux soulignent en effet l'occurrence de comportements humains dits « déviants », « inappropriés » ou « non sécures ». Une citation emblématique de ce mode de pensée est issue d'un ouvrage d'un des plus grands experts internationaux en cybersécurité, Bruce Schneier :

> *« Les mathématiques sont logiques ; les gens sont erratiques, capricieux et à peine compréhensibles » [6]*

Si nous pouvons comprendre ce découragement du mathématicien face à l'imprévisibilité des comportements humains, nous chercherons toutefois à aller plus loin, centrant notre regard sur des travaux visant à dépasser ce paradigme,

et cherchant à comprendre les raisons et les facteurs explicatifs de ces comportements jugés inadéquats.

C. Tour rapide sur l'approche en termes d'erreur humaine et ses limites par rapport à la prévention

Une étude a particulièrement retenu notre attention [7]. Elle propose une taxonomie des comportements des utilisateurs finaux (*end users*) concernant la sécurité des Systèmes d'Information (SI). Ici, le sens donné au terme « utilisateurs finaux » renvoie « aux utilisateurs des technologies de l'information dans les organisations » (*information technology users within organizations*). Un grand nombre d'entretiens (n=110) ont été réalisés avec des professionnels des technologies de l'information, des managers et des employés, ce qui a permis aux chercheurs de cartographier les comportements relatifs à la sécurité en six catégories, selon deux dimensions.

- **L'intentionnalité** (*malicious, neutral, beneficial*), à savoir si le comportement décrit est intentionnellement malveillant ou bénéfique, ou quelque part entre les deux.
- **L'expertise technique** (*high, low*) correspond au degré de connaissances et de compétences en informatique que l'utilisateur devait posséder pour adopter le comportement en question.

Le croisement de ces deux dimensions (intentionnalité / degré d'expertise) permet aux auteurs de proposer six types de comportements d'utilisateurs finaux. Ces 6 types de comportements permettent ensuite d'identifier des

Institutions / Domaines		Veille	Sensibilisation/ Formation	Gestion de crise	Défense	R&D	Enquête post-crise
Françaises	ANSSI	x	x	x	x	x	
	COSSI / SDO	x		x	x		
	CERT-FR	x		x	x		
	OZSSI	x	x				
	AQSSI	x	x				
	CALID	x			x		
	COMCYBER				x		
	CNIL	x	x			x	
Etats-Uniennes	Cybersecurity Directorate	x	x		x	x	
	CISA	x		x	x	x	
	NCSA		x				
	DHS		x		x		
	CSD					x	
	CATS (FBI)						x
	USCYBERCOM				x		
Britaniques	GCHQ	x		x	x		x
	OCSIA	x	x	x			
	CSOC	x		x			
	NCSC		x	x		x	
	Ministères			x	x		
Allemandes	BMI				x		
	BSI	x		x	x		
	Nationale Cyber-Abwehrzentrum	x		x	x		
	Cybersicherheitsrat		x		x		
Européennes	ECSO	x	x			x	
	ENISA		x		x		
Think-tanks	IFRI (et autres, à poursuivre)					x	
Privées	Kaspersky Lab		x				
	NRG					x	
	FAI	x		x			
	Laboratoires académiques					x	

Tableau 1 *Cartographie des acteurs selon leur nature et leurs domaines d'activité (figure* Opus Citatum*).*

recommandations d'action prioritaires. En effet, nombre de dysfonctionnements sont dus à des « *naïve mistakes* », de la part d'utilisateurs « moyens » (ni malveillants ni particulièrement consciencieux). La taxonomie s'appuyant sur des notes chiffrées, leurs auteurs avancent pouvoir être en mesure de quantifier les comportements ainsi que l'amélioration des comportements des utilisateurs. Elle est intéressante car elle distingue des formes de comportement conduisant à l'évènement critique et d'autres considérés comme sûrs. Toutefois, ce type d'étude interroge à plusieurs égards. Premièrement, la catégorie « *intentional destruction* » (Destruction intentionnelle) nécessite un haut niveau d'expertise et implique une intention malveillante (soit une forte intention de nuire) vis-à-vis de des ressources de l'organisation de la part de l'individu. Ce comportement correspond donc plutôt à un profil d'un cyber criminel plutôt qu'à celui d'un utilisateur final non professionnel ou d'un expert en cybersécurité dont l'activité est de protéger les ressources de l'entreprise. A partir de là, nous ne partageons pas ce point de vue.

Deuxièmement, le comportement de type *Detrimental misuse* (Mauvaise utilisation préjudiciable) renvoie lui à un utilisateur non professionnel, mais à nouveau, de notre point de vue ce type de comportement n'est pas non plus intentionnel. Dans le cas contraire il s'agit de sabotage. Le non-respect des règles peut être motivé comme nous le verrons plus loin par des aspects intrinsèques à l'organisation et à l'activité de travail. Et non pas à une intention particulière de « nuire »

Troisièmement, le *Dangerous Tinkering* (Bricolage dangereux) requiert un haut niveau d'expertise mais pas d'intention claire de nuire aux ressources de l'entreprise. En d'autres termes, il s'agit d'une personne ayant une forte expertise technique et pouvant affecter la sécurité du système. Par exemple, un employé configure une passerelle sans fil qui permet par inadvertance à des personnes extérieures (et à proximité) à l'entreprise d'accéder sans fil à son réseau. Il est intéressant de comprendre là aussi ce qui motive cette action (gain de temps ? contrainte professionnelle ?)

Viennent ensuite les *Naïve mistakes* (Erreurs naïves). Un faible niveau d'expertise est requis et il n'y a aucune d'intention claire de nuire de la part de l'utilisateur. Par exemple, choisir un mauvais mot de passe (faible niveau de sécurité, comme "mot de passe") ou utiliser son numéro de sécurité sociale. Ces erreurs naïves suggèrent un manque de sensibilisation aux principes de base de la cybersécurité davantage qu'une intention de nuire.

Du côté des comportements positifs, le comportement d'*Aware assurance* (Assurance consciente) requiert quant à lui un haut niveau d'expertise et une forte intention de faire le bien pour préserver et protéger les ressources. Par exemple, reconnaître la présence d'un programme backdoor par une observation attentive de son propre ordinateur. On peut supposer qu'il s'agit d'experts en cybersécurité dont leur activité est de protéger les SI.

Enfin, le dernier comportement de la typologie de nos auteurs, *Basic hygiene*, fait référence à l'Hygiène de base. Ici, une faible expertise technique est nécessaire mais l'individu manifeste une intention claire de préserver et de protéger le système. Par exemple, un employé formé et sensibilisé résiste à une tentative d'attaque par ingénierie sociale en refusant de communiquer son mot de passe à un interlocuteur se faisant passer pour un membre du département informatique. Il s'agit ici d'un individu ayant compris les risques et acquis une forme de culture cybersécurité, comme nous le verrons plus loin.

Sur la **Erreur ! Source du renvoi introuvable.**, la zone jaune au centre du graphique correspond aux comportements menant à la sécurité ou à l'insécurité (*unintentional (in)security*). Des comportements neutres, non intentionnels, peuvent donc conduire à un état sécure ou au contraire insécure.

D'après les auteurs, les corrélations établies sont pour la plupart positives, suggérant qu'un plus grand degré de formation et de sensibilisation se traduit par une plus grande fréquence des comportements sécures. Plus généralement, la formation, l'application d'une AUP[1], informer les salariés sur la façon dont ils sont surveillés et appliquer une politique de récompense semble avoir un effet positif sur la fréquence de changement des mots de passe et sur la création de mots de passe complexes. Cependant, le changement fréquent des mots de passe pourrait avoir un « effet pervers » : les employés écrivent leurs mots de passe sur des post-its ou cahiers pour s'en souvenir. La complexification des mots de passe, en partie imposée par la charte informatique (ex : mots de passe devant être composés de chiffres, majuscules, caractères spéciaux et être différents pour chaque service) n'empêche pas les utilisateurs d'utiliser des mots de passe tels que « Password1 », « P@ssword1 » et « Nomdel'entreprise01 », qui sont les plus courants [8].

Enfin, la divulgation des mots de passe ne semble pas corrélée avec la formation, l'application d'une AUP, et le contrôle des salariés, nécessitant selon les chercheurs cités précedemment un approfondissement des recherches à ce sujet.

Ainsi, comme précisé auparavant, l'erreur humaine ne suffit pas à expliquer les comportements inadéquats, voire elle est inadaptée. La taxonomie proposée illustre que finalement les « erreurs naïves » ne sont pas à proprement parler des « erreurs ». Il faut donc chercher d'autres facteurs explicatifs pour comprendre ces comportements inadéquats.

II. QUELQUES FACTEURS EXPLICATIFS DES COMPORTEMENTS CONSIDERES INADEQUATS

Les situations qui nous intéressent d'explorer pour contribuer à la prévention dans le domaine de la cybersécurité, ne sont donc pas des situations où l'utilisateur appuie « par erreur » sur un bouton. Ce ne sont pas non plus des situations dans lesquelles il y a un manque de compréhension de sa part parce la situation est extrêmement complexe. Ce sont plutôt des situations dans lesquelles l'utilisateur peut croire que c'est une information utile pour lui (par exemple le phishing) ou par méconnaissance des risques induits par son action (pas de changement de mot de passe ou utilisation d'un mot de passe pas sûr). Ainsi, il faut chercher à identifier des facteurs explicatifs propres à ces situations. Nous en avons identifié deux qui interagissent et peuvent avoir des impacts distincts

[1] Une *Acceptable Use Policy* (AUP) est un document précisant les contraintes qu'un utilisateur doit accepter afin de pouvoir se connecter à un réseau d'entreprise

selon les contextes de travail et les activités des acteurs : la pression temporelle (subie, ressentie) et la charge travail.

A. *Pression temporelle et charge de travail induite par des tâches de sécurité*

En nous intéressant aux facteurs qui ont un impact sur les comportements jugés inadéquats en termes de cybersécurité, un premier ensemble de travaux empiriques menés par Noman H. Chowdhury et ses collègues, qui portent sur la pression temporelle et la surcharge de travail, viennent éclairer ces propos (« *driving factors behind non-secure HCS [Human CyberSecurity] behavior* ») [9].

Ces auteurs ont interviewé 35 personnes, au sein desquels ils distinguent les « experts cybersécurité » (*Cybersecurity experts (CSEs*)) des « utilisateurs généraux » (*general users*) que sont les « professionnels de l'informatique hors-cybersécurité » (*non–sec professionals*) et les « utilisateurs privés » (*private users*). Cette typologie est proche de celle que nous avons établie (cf. p. 2), à la différence que les utilisateurs privés sont des particuliers, et les « *non sec-professionals* » sont des employés non informaticiens. Comme nous nous intéressons aux comportements relatifs à la cybersécurité dans les organisations, nous laisserons de côté les *private users, c'est-à-dire des particuliers*.

Cette étude a montré que les comportements dits non-sécures, adoptés par les utilisateurs (au sens large) en situation de pression temporelle, sont causés en premier lieu par des facteurs contextuels. En ce sens, il convient de considérer 1) les sources, 2) la nature et 3) la temporalité de la pression temporelle exercée sur l'individu.

- Les experts cybersécurité soutiennent que, par la nature de leur travail, ils font généralement face à des dates buttoirs rapprochées. Cela concerne les mises en œuvre et les opérations (sauvegardes, mises à jour des systèmes, migrations technologiques) tout comme les tâches indirectement liées à la sécurité, à l'image des programmes de sensibilisation. Par conséquent, les tâches conçues pour renforcer la sécurité peuvent involontairement menacer la sécurité en créant une pression temporelle dans d'autres domaines.
- Pour les non-professionnels de la sécurité, la pression temporelle est souvent associée à une charge de travail élevée, l'exigence de respect des délais (ex : répondre à un supérieur entraîne intrinsèquement un sentiment d'urgence). Cette pression découle aussi de facteurs généraux comme l'environnement de travail (ex : manque de personnel) ou la nature du travail à réaliser (ex : un CSE dénonce que le multitâche implique un sentiment de « manque de temps », en plus de gêner la concentration).
- Bien que la pression temporelle ne soit pas permanente et survienne dans des moments prédéfinis comme l'arrivée d'une date buttoir, ou inattendus comme lorsqu'un système crash, ses impacts n'en sont pas moins importants.

La manière dont la cybersécurité est perçue et appliquée dans l'organisation fait également partie des facteurs contextuels. Ainsi, les politiques de sécurité ou les outils qu'elle met à disposition pour lutter contre le risque cyber, ou les programmes de sensibilisation sont entre autres, des éléments situationnels pouvant renforcer les effets de la pression temporelle. Les experts cybersécurité ont également pointé le fait que, même eux, en tant professionnels de la sécurité, pouvaient avoir des comportements inadéquats, en particulier sous pression temporelle.

Les comportements non-sécures sont également causés par des constructions psychologiques reposant sur 1) l'affect, 2) la cognition et 3) la perception.

- Dans leur revue de littérature [10], les auteurs avaient identifié dix-sept émotions que les utilisateurs éprouvent sous la pression temporelle. Nombre de ces variables ont été confirmées lors de la présente étude :
  - L'ennui, relatif aux notifications incessantes ;
  - Les sentiments d'anxiété et de frustration liés à l'exécution des tâches urgentes ;
  - Le stress et le sentiment d'obligation à savoir prendre des décisions risquées et prioriser les réponses rapides plutôt que de prendre le temps de la réflexion ;
  - Et la peur de l'échec qui accentue l'état émotionnel dans lequel les personnels sont lorsqu'ils sont sous une pression temporelle.
- Réaliser une tâche sous pression temporelle réduit la capacité cognitive des utilisateurs (au sens large) afin qu'ils puissent traiter les informations qui ne sont pas reliées à la tâche qu'ils sont en train de faire. Cette réduction de capacité, les acteurs malveillants peuvent l'exploiter, par exemple avec les courriels de phishing aux heures de pointe. Par exemple, les experts sécurité ignorent certaines configurations de sécurité. Dans l'ensemble, les répondants se sont montrés peu préoccupés par l'utilisation de systèmes inconnus, et considèrent que les conséquences de leur comportement non-sécure est négligeable.
- Les résultats obtenus ont confirmé que la pression temporelle avait des effets néfastes sur la perception qu'ont les utilisateurs (au sens large) du rapport coût/bénéfice concernant l'adoption d'un comportement dit sécure, l'importance de la cybersécurité et l'efficacité personnelle à agir de façon sécurisée. Sous la pression temporelle, les utilisateurs (au sens large) ont du mal à appliquer les exigences de sécurité. Ils peuvent même contourner les règles de sécurité ou chercher des solutions de contournement, pourtant non sécurisées. Ceci afin de ne pas être gênés dans la réalisation de leur activité courante. Pourtant, en temps normal (hors pression temporelle), la plupart des utilisateurs (au sens large) sont en mesure d'appliquer les règles de sécurité. Cette perception est accentuée par l'impression que la (cyber)sécurité n'est pas importante ni prioritaire, à la fois pour leurs pairs (collègues, famille…) et pour leurs supérieurs, comparée à leurs tâches habituelles. Les utilisateurs pensent que leur entreprise investit suffisamment en matière de cybersécurité, et donc que celle-ci est optimisée quel que soit leur propre comportement.

B. *Variation de l'impact de la pression temporelle en interaction avec le contexte de travail*

La pression temporelle peut être modulée, accentuée en interaction avec des facteurs tels que : 1) les caractéristiques de la tâche à accomplir, 2) celles de l'utilisateur et 3) celles du lieu de travail, viennent compléter et renforcer ces

éléments menant à des comportements non-sécures sous la pression temporelle.

- L'influence de la pression temporelle varie selon la nature de la tâche (complexité, implication…). Les utilisateurs (au sens large) ont indiqué aux chercheurs que leur comportement s'améliorerait s'il y avait des pénalités liées aux comportements non-sécures. En outre, les utilisateurs sont d'autant plus susceptibles d'adopter un comportement non sécure que leur incertitude quant aux conséquences est élevée (ex : pénalité, évaluation des performances). En somme, plus la communication sur les exigences de sécurité est claire, moins les utilisateurs sont susceptibles d'adopter un comportement non sécure.

- Impact en fonction de la personne (ou du poste). Les experts cybersécurité interrogés ont suggéré que les cadres supérieurs sont les plus enclins à adopter un comportement non sécurisé sous la pression du temps notamment car ils reçoivent beaucoup d'e-mails. L'expérience joue aussi un rôle dans le comportement, tout comme la maîtrise du langage de la cybersécurité (comme la terminologie utilisée dans les messages d'avertissement).

- Plusieurs experts cybersécurité déclarent que, souvent, les organisations ne communiquent pas correctement leurs politiques de cybersécurité aux utilisateurs (au sens large), ce qui peut entraîner une ambiguïté quant aux comportements attendus. Aussi, les utilisateurs (au sens large) sont influencés par le comportement qu'ils observent dans leur environnement (ex: celui des collègues sur le lieu de travail).

Ces facteurs induits par une pression liée au temps contribuent à l'adoption de cinq comportements des utilisateurs, au sens large, non souhaités.

- L'évitement (*avoiding*) : Décrit la tendance que les utilisateurs ont à éviter les mesures de sécurité comme les sauvegardes ou le chiffrage des données par exemple.

- Le contournement (*bypassing*): Comportement adopté par les utilisateurs qui contournent les politiques de sécurité. Par exemple, les utilisateurs contournent parfois les politiques de contrôle d'accès pour donner l'accès plus rapidement aux centres de données ou à des lieux physiques contenant des informations sensibles.

- La divulgation (*disclosing*) : Les utilisateurs soumis au stress de la pression temporelle sont plus enclins à divulguer des informations d'identification à leurs collègues.

- L'ignorance (*disregarding*) : Les utilisateurs soumis à une pression temporelle ont tendance à ne pas tenir compte des mesures de sécurité mises en œuvre par leur organisation. Par exemple, ils utilisent des logiciels non-autorisés, ne respectent pas les protocoles techniques lors de la configuration des systèmes ou laissent leurs postes de travail sans surveillance.

- L'excès de confiance (*over-relying*) : Sous la pression temporelle, les utilisateurs peuvent avoir tendance à surestimer la fiabilité des contrôles et la sécurité de l'infrastructure. Ils ont confiance en la sécurité mise en œuvre par l'organisation et pensent que cela suffit pour les protéger, indépendamment de leur comportement. Ils peuvent alors devenir vulnérables aux attaques.

Ces résultats sont intéressants dans la mesure où ils apportent des éléments individuels et organisationnels impliqués dans les évènements de cybersécurité.

III. PENSER LA PREVENTION DANS LE DOMAINE DE LA CYBERSECURITE

A partir de cette première réflexion, surgit alors la question de la prévention et de comment peut-on la renforcer dans ce contexte. Plusieurs axes de travail se dégagent, dont trois qui ont été relativement bien explorés : la sensibilisation, la formation des utilisateurs et le développement de la culture en cybersécurité. Ces axes permettent d'apporter des éléments pour combattre les cinq comportements décrits auparavant mais, uniquement en partie.

En effet, deux autres axes, nécessaires pour compléter une réflexion FOH ont été beaucoup moins explorés : l'organisation du travail et la conception des SI.

Nous discuterons ces différents axes de travail ci-après.

A. Sensibilisation, formation des utilisateurs et culture de cybersécurité

Parmi les mesures préconisées par les différents auteurs que nous avons cités, la sensibilisation et la formation des utilisateurs en cybersécurité apparaît comme essentielle afin de prévenir l'adoption des comportements dits non-sécures. L'enjeu est alors de mettre en place des programmes efficaces et pertinents au regard des besoins de l'organisation certes, mais également selon les caractéristiques de chaque individu, en fonction de son positionnement hiérarchique. En effet, comme nous l'avons vu et comme le rappellent Sarrazin et Gaignaire :

> *« Tous les membres du personnel, sans exception aucune, ont un rôle à jouer en matière de prévention des cyberattaques, peu importe qu'ils fassent partie de la haute direction ou qu'ils soient des employés subalternes. » [11]*

Des organismes de formation proposent des programmes de formation et de sensibilisation à la cybersécurité adaptables en fonction du niveau hiérarchique des individus et de leur département. C'est le cas par exemple, de Kaspersky Lab, qui offre différents outils et formats de formation, organisés et conçus selon le niveau organisationnel [12]. Afin de motiver les salariés à assister à ces formations et de renforcer l'assimilation du message, l'entreprise met à disposition plusieurs méthodes pédagogiques telles que des jeux de simulation basés sur la réalité virtuelle ou des ateliers interactifs.

D'autres insistent plutôt sur : 1) la récurrence et la constance des programmes. 2) Le fait d'adapter la formation au niveau d'expertise et au rôle des personnes, ou encore, en remettant en contexte les situations en fonction de l'activité habituelle de l'individu. Ce qui peut aider à donner du sens à la cybersécurité en relation avec l'activité de travail de chacun. 3) Et le fait de « donner envie » plutôt que d'être anxiogène, en faisant preuve de pédagogie, et en n'hésitant pas à sortir du

cadre professionnel [8]. Ce dernier point est très important car il est de plus en plus récurrent que les employés utilisent leur propre outil informatique pour travailler.

Mettre en place des exercices ou des simulations d'incidents peut s'avérer un moyen efficace pour créer une prise de conscience chez les individus. En particulier si ceux-ci sont construits d'après des vrais incidents, comme ceci a été prouvé dans d'autres domaines [13]–[15].

Dans tous les cas, : les programmes de sensibilisation doivent être conçus autour de la manière dont la cyber-vulnérabilité affecte la vie des participants (c'est-à-dire en se référant aux choses qui comptent le plus pour eux) [9]. Des experts cybersécurité ont suggéré d'organiser des « sessions de sensibilisation » au cours desquelles les utilisateurs partagent leur expérience des incidents précédents, et que les décideurs soient sensibilisés aux dangers d'un contrôle insuffisant ainsi qu'aux défis auxquels est confronté le personnel chargé de la sécurité. Enfin, ils ont souligné l'importance de compléter les programmes de sensibilisation par des formations. Un non-professionnel de la sécurité (*non-sec professional*) a aussi suggéré que les nouveaux employés passent du temps dans le département cybersécurité. Enfin, les experts cybersécurité ont suggéré que les utilisateurs reçoivent une formation pour développer des compétences qui ne sont apparemment pas reliées à la cybersécurité comme la gestion du temps.

Figure 1. Différents formats de formation pour différents niveaux organisationnels proposés par Kaspersky Lab

L'ensemble de ces points va dans le sens d'instaurer une culture de (cyber)sécurité ce qui permet de faire en sorte que les individus perpétuent les comportements appropriés, de mettre en avant les comportements sécures et de réduire les facteurs émotionnels en respectant l'équilibre vie privée - vie professionnelle dans la définition des postes. L'importance de la culture de (cyber)sécurité est également soulignée par Nicolas Arpagian dans son ouvrage de synthèse « La cybersécurité » :

> *« Il convient de diffuser une véritable culture de la sécurité auprès de tous les échelons hiérarchiques, bien au-delà des équipes de direction ou des informaticiens. Si des salariés disposent d'un ordinateur, d'un smartphone ou d'une tablette reliés au Net ou à un réseau interne, ils doivent être considérés comme partie prenante du processus global de sécurité » [16].*

Certains acteurs parlent même d'« évangélisation » des employés, de « démystifier le sujet », à l'image [8].

B. Organisation du travail, Conception et impacts des FOH

Les aspects organisationnels sont loin d'être négligeables dans la prévention d'évènements de cybersécurité. Nous avons identifié *a minima* trois points sur lesquels il faut être attentif.

Du point de vue des ressources humaines, les aspects réglementaires sont encadrés par la norme ISO/IEC 27002:2022 « Sécurité de l'information, cybersécurité et protection de la vie privée » [17, p. 59] via notamment la publication d'une charte utilisateur , la clarification des règles de sécurité applicables aux salariés quand ils auront quitté l'entreprise, etc.

Ajoutons toutefois qu'au-delà de ces aspects réglementaires, les ressources humaines doivent être en nombre suffisant dans le département cyber, et le personnel doit y être bien formé afin de pouvoir répondre aux questions des utilisateurs (au sens large), et de réaliser les tâches de cybersécurité nécessaires à l'entreprise, dans les délais voulus et un haut niveau de qualité. Les ressources humaines des autres services doivent également être adaptées aux besoins de l'entreprise afin d'éviter d'avoir des salariés en surcharge de travail, ce qui ne favorise pas l'attention nécessaire aux tâches de sécurité.

Le management doit prendre en compte les différentes tâches relatives à la cybersécurité et être impliqué dans certaines de ces tâches (relecture et validation des politiques de sécurité, participation aux sessions de sensibilisation, …). Il est également nécessaire qu'il prenne en compte la charge de travail des différents utilisateurs afin de bien percevoir dans quelle mesure le contexte organisationnel peut favoriser des actions cyber-sécure.

Au niveau de la conception plusieurs réflexions pourraient être explorées telles que : anticiper des sauvegardes, ne pas laisser certaines tâches aux utilisateurs (au sens large) afin de ne pas leur rajouter une charge de travail et garantir un niveau de sécurité, anticiper et gérer les mises à jour, planifier les périodes changement de mot de passe, etc…

Ryan West, chercheur en design chez Dell Inc. au Texas, avance que l'importance du rôle de l'utilisateur pour garantir le succès des mécanismes de sécurité a été reconnue en 1883 par Auguste Kerckhoffs [18] dans *La cryptographie militaire*. En parlant de la conception des systèmes de cryptographie, ce dernier énonce un des principes qui portent aujourd'hui son nom :

> *« … il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer. » West [19]*

Selon lui, les concepteurs doivent comprendre comment les utilisateurs (au sens large) prennent des décisions en matière de sécurité, car, même si l'interface est « élégante » et « intuitive », si l'utilisateur ignore les avertissements ou transgresse involontairement les politiques de l'organisation, la sécurité est compromise.

L'étude qualitative menée par Kraemer, Carayon et Clem avec des experts en Computer and Information Security (CIS) (n=10), a montré l'influence des FOH sur des vulnérabilités qui apparaissent dès la conception des systèmes d'information [20]. Ainsi, bien que cette étude illustre le lien entre des FOH et quatre types de vulnérabilités que sont les vulnérabilités liées à la conception (*design*), à la mise en œuvre (*implementation*), à la configuration du système (*configuration*), et à la dimension opérationnelle (*operational*), nous nous concentrerons dans cette partie sur les facteurs menant à des vulnérabilités de conception.

Ces auteurs ont mis en lumière onze chemins menant à des vulnérabilités liées à la conception, sur la cinquantaine de chemins identifiés, toutes catégories confondues. Autrement dit, onze relations de cause à effet, composées de FOH regroupés selon neuf thèmes sont susceptibles de créer des vulnérabilités dès la conception : influences externes, erreur humaine, management, organisation de la cybersécurité, gestion de la performance, politiques, gestion des ressources, technologie et formation.

Dans une approche un peu plus technique, Salaün part de la compréhension initiale que l'utilisateur (ici tout employé utilisant un outil informatique avec un contrôle d'accès) a des interfaces de conditions d'accès aux données qu'il crée. Son travail vise à lui fournir les moyens nécessaires pour qu'il puisse protéger son travail réalisé sur la machine. Pour ce faire, il propose des modèles permettant de s'adapter aux usages de l'utilisateur, et notamment un modèle basé sur « les propriétés de sécurité d'une interface homme-machine (IHM) nécessaires à la compréhension fiable et sûre du système par l'utilisateur » [21, p. i]. Ces modélisations permettent alors d'intégrer la contribution de l'utilisateur à la sécurité de son activité numérique, tant au niveau de l'utilisation de son outil informatique (modèle s'adaptant de façon transparente à ses changements d'activité), qu'à la conception des conditions d'accès à ce dernier (modèle basé sur une interface homme-machine dite de confiance, à savoir « établir un lien entre les entités avec lesquelles l'utilisateur pense communiquer, et celles avec lesquelles il communique vraiment »).

De leur côté, Conti, Ahamad et Stasko affirment que pour que les systèmes de visualisation de données soient efficaces, il faut que leurs concepteurs soient alertes sur les façons dont chaque système peut protéger les utilisateurs et les façons dont ils peuvent être manipulés [22]. Autrement dit, du fait de leur vulnérabilité face aux attaques, les systèmes de visualisation de l'information, et en particulier ceux utilisés dans la prise de décision, doivent être conçus en tenant compte de la sécurité. A ce propos, ils proposent aux concepteurs des principes et des hypothèses de conception pour contrer les visualisations malveillantes (utilisation des vulnérabilités présentes dans les systèmes de visualisation de données pour accomplir des actes malveillants). Au-delà de la formation, il s'agit d'une part, de concevoir le système de façon à le protéger en supposant que le système sera attaqué. D'autre part, de protéger la génération de données et le flux de données en améliorant la qualité des données dans le but d'éviter que les sources malveillantes ne s'infiltrent dans le système.

Enfin, dans l'objectif de contrecarrer les comportements identifiés comme non-sécures, (particulièrement favorisés par la pression temporelle) [9] Norman H. Chowdhury et ses collègues proposent également de mettre l'accent sur des repères visuels colorés dans les messages d'avertissement, dans le but d'avertir plus facilement l'utilisateur sur le contenu et la gravité de ce dernier. Ces repères visuels peuvent également être mobilisés dans la configuration de l'espace de travail, afin de rappeler aux utilisateurs les comportements attendus en matière de HCS voire de renforcer une culture de sécurité.

CONCLUSION

Cette communication rend compte d'un travail en cours de recension de la littérature académique sur la cybersécurité vue sous l'angle des Facteurs Organisationnels et Humains, ceux-ci devant permettre d'aller au-delà du paradigme de « l'erreur humaine », encore assez présent dans les milieux techniques informatiques. Il apparaît à la lecture des travaux sélectionnés et présentés, qu'un courant de recherche se développe depuis quelques années mais qu'il semble encore manquer d'un peu de volume, du point de vue du nombre de publications présentant des recherches qualitatives sur ce thème. Or, le paradigme de l'erreur humaine est loin d'être pertinent dans ce domaine. Un certain nombre d'études centrées sur les comportements des utilisateurs finaux – experts cyber et non-experts -, mettent en avant des situations de travail dans lesquelles les utilisateurs se retrouvent à devoir faire des arbitrages entre des buts de sécurité et de production face à une charge de travail importante, un manque de ressources, à des solutions de sécurité considérées trop contraignantes ou encore des solutions de sécurité qui n'ont pas été clairement expliquées. Un élément commun à ces situations problématiques est la non prise en compte de la réalité de l'activité des différents acteurs. Il s'agit donc de comprendre les conditions de travail qui risquent de défiabiliser la cybersécurité dans le quotidien et face à une cyber attaque.

Aussi, des analyses d'évènements critiques cyber avec une approche FOH semblent manquer en vue de mieux saisir les processus pouvant générer des cyberattaques et les modalités opérationnelles de gestion d'une crise cyber (par les pilotes de crise et les opérationnels). L'étude de la gestion des évènements cyber et d'une crise réelle, comme l'étude de tout évènement critique, est difficile à observer, in situ, sauf si celle-ci est longue, comme la crise sanitaire, ce qui semble être le cas dans certaines cyberattaques. Ainsi, il faut pouvoir envisager cette éventualité.

Un autre point commun à d'autres crises qui ressort est un besoin d'approches pluridisciplinaires pour leur étude. Les FOH permettant de comprendre des processus cognitifs complexes pouvant être gage de fiabilité comme la surveillance, le diagnostic, la prise de décision, les modalités de transmission et de traitement de l'information, les interactions entre les collectifs impliqués, comme dans d'autres crises, avec certainement des particularités propres à la une cyberattaque. En effet, il ressort des phases dans la gestion d'une cyber crise cruciales identifiés par différents auteurs qui sont : la prévention/surveillance, la détection, le diagnostic et la réponse.

Dans tous les cas, comme pour l'étude d'autres évènements critiques d'envergure, il est nécessaire de construire des scénarios de cyberattaques afin de former et de permettre à différents experts cyber et autres personnels, intervenant dans une crise cyber, de s'entraîner. Ces scénarios doivent s'inspirer de situations réelles d'attaque pour avoir une validité écologique, i.e. qu'elles soient représentatives de situations futures probables de crise et qui permettent aux différents acteurs de développer des compétences ad'hoc. Au travers des études analysées il ressort :

- Des situations de préparation/évaluation pour des futurs experts en cybersécurité.
- Des situations de préparation à la gestion d'une cyberattaque du point de vue d'acteurs distincts : les experts cyber qui sont en surveillance, les utilisateurs finaux des SI pouvant engager la sûreté des installations (opérateurs en salle de commande) ou des utilisateurs pouvant engager la sécurité de données sensibles.

- Des situations d'entraînement dans lesquelles les interactions entre différents types d'utilisateurs et d'experts impliqués dans la gestion d'une crise puissent être mises en pratique.

Sur le plan de l'organisation de la gestion de crise, on constate que la gestion d'une crise cyber, comme dans d'autres domaines, nécessite la mise en place d'un réseau d'acteurs, d'entités, etc. prévu en amont et, qui comme dans d'autres cas, sera un réseau ponctuel et éphémère, qui disparaît lors de la fin de la crise. Ce réseau semble se caractériser par des entités et des experts divers et semble être assez complexe en termes d'interactions et de coordinations, à distance, sans compter que la complexité d'une situation de cyber attaque, de ce que nous avons pu comprendre, dépasse largement l'entreprise, voire les frontières d'un pays. Ainsi deux aspects se dégagent pouvant être instruits d'un point de vue FOH :

- l'organisation de crise prévue en amont avec des rôles clairs, une hiérarchisation de ceux-ci afin de faciliter la gestion de la cybercrise.
- La nécessité d'outiller, de soutenir les échanges pour les faciliter et les fiabiliser, dans une situation ou les informations peuvent différer entre acteurs et entités impliquées dans la gestion de la cyber crise, peuvent être lacunaires, confuses.

Du point de vue de la conception au sens large, peu d'études associant les FOH et la cybersécurité ont été identifiées. Ainsi, des perspectives d'étude concernent la conception de solutions de sécurité, conception d'interfaces humain-machine, conception de dispositifs de travail des experts en cybersécurité, conception d'organisations de travail intégrant la cybersécurité dans le quotidien, conception d'organisations de crise, de PCA et de Plan de reprise d'activité, conception de simulations pour des entraînements

La prochaine étape de notre travail est de réaliser une typologie des cyberattaques existantes, afin d'y associer les catégories d'utilisateurs finaux, les impacts qu'elles peuvent avoir sur les SI, ainsi que les modes de prévention possibles pour s'y protéger. L'étude abordera également la question de la décision opérationnelle et de la gestion de crise, dans le but de comprendre l'organisation des ressources à déployer dans le but d'optimiser la cybersécurité des systèmes. En effet, bien que des moyens de préventions comme la sensibilisation ou la prise en compte des risques en amont (lors de la conception des systèmes SI) aient des effets positifs sur la cybersécurité, il n'est pas possible d'exclure des attaques qui sont par ailleurs difficilement anticipables. Penser la cybersécurité passe donc également par l'étude des comportements et des moyens organisationnels et techniques qui permettent une résilience face à une attaque potentiellement délétère pour une organisation.

Ainsi, nous voyons d'ores et déjà l'importance de la cybersécurité pour la maîtrise des risques, fondamentale dans le contexte actuel, afin de garantir au monde et aux générations présentes et futures un avenir durable. Les innovations produites et restant à produire en cybersécurité devront ainsi comporter à la fois des composantes techniques mais également des composantes humaines et organisationnelles. Si l'expert cybersécurité, en charge de la conception des futures interfaces, doit innover pour produire des matériels sûrs et résilients, il est également indispensable de prendre en compte les Facteurs Organisationnels et Humains, qu'il s'agisse de penser des interfaces adaptées aux contraintes réelles des employés ou de les former et de les entraîner pour faire face aux crises cyber-sécuritaires.

ACKNOWLEDGMENT

Cette communication s'inscrit dans le cadre du Projet Européen PRAETORIAN (Protéger les infrastructures critiques contre les menaces avancées combinant risques physiques et cybernétiques).

REFERENCES

[1] M. Gros, « Saint-Gobain évalue à 250 M€ les dégâts liés à l'attaque NotPetya - Le Monde Informatique », LeMondeInformatique, 1 août 2017. https://www.lemondeinformatique.fr/actualites/lire-saint-gobain-evalue-a-250-meteuro-les-degats-lies-a-l-attaque-notpetya-68955.html (consulté le 7 avril 2022).

[2] ANSSI, « Bulletin d'actualité CERTFR-2017-ACT-029 – CERT-FR », 24 juillet 2017. https://cert.ssi.gouv.fr/actualite/CERTFR-2017-ACT-029/ (consulté le 7 avril 2022).

[3] R. Février, « Covid-19 et cyberattaques », Revue francaise de gestion, vol. 293, nº 8, p. 81-94, 2020.

[4] S. Cordon, « Le besoin grandissant de sécurisation des données médicales des établissements de santé et le cadre de développement des réponses apportées », Journal du Droit de la Sante et de l'Assurance - Maladie (JDSAM), vol. 29, nº 2, p. 63-66, sept. 2021.

[5] E. Hoorickx, « Les États, acteurs clés de la cyberstratégie euro-atlantique », Revue Defense Nationale, vol. 818, nº 3, p. 93-98, 2019.

[6] B. Schneier, Secrets and Lies: Digital Security in a Networked World. Wiley, 2015. Consulté le: 12 mai 2022. [En ligne]. Disponible sur: https://www.wiley.com/en-us/Secrets+and+Lies%3A+Digital+Security+in+a+Networked+World-p-9781119183631

[7] J. M. Stanton, K. R. Stama, P. Mastrangelo, et J. Jolton, « Analysis of end user security behaviors », Computers & Security, vol. 24, nº 2, p. 124-133, mars 2005, doi: 10.1016/j.cose.2004.07.001.

[8] Olfeo, Livre Blanc « Responsabilisez vos collaborateurs ». Paris, 2022. Consulté le: 17 mai 2022. [En ligne]. Disponible sur: https://www.olfeo.com/fr/lb-responsabilisez-vos-collaborateurs

[9] N. H. Chowdhury, M. T. P. Adam, et T. Teubner, « Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures », Computers & Security, vol. 97, p. 101931, oct. 2020, doi: 10.1016/j.cose.2020.101931.

[10] N. H. Chowdhury, M. T. P. Adam, et G. Skinner, « The impact of time pressure on cybersecurity behaviour: a systematic literature review », Behaviour & Information Technology, vol. 38, nº 12, p. 1290-1308, déc. 2019, doi: 10.1080/0144929X.2019.1583769.

[11] C. Sarrazin et A. Gaignaire, « Cybersécurité : misez sur la prévention ! », Gestion, vol. 44, nº 3, p. 78-82, sept. 2019.

[12] « Formation Kaspersky de sensibilisation à la sécurité ». https://www.kaspersky.fr/enterprise-security/security-awareness (consulté le 17 mai 2022).

[13] J. Alengry, P. Falzon, C. De La Garza, et P. Le Bot, « What is “Training to Cope with Crisis Situations”? Developing a Reflexive Training Device for a Crisis Support Team », in Proceedings of the 20th Congress of the International Ergonomics Association (IEA 2018), 2019, p. 60-67.

[14] C. De La Garza, P. Le Bot, et Q. Baudard, « The simulation of extreme situations for the analysis of resilience: an original methodology to improve simulation and organizational resilience », in Proceedings of the 20th Congress of the International Ergonomics Association (IEA 2018), 2018, vol. 821, p. 13-22. [En ligne]. Disponible sur: https://doi.org/10.1007/978-3-319-96080-7_2

[15] P. Le Bot et C. De La Garza, « PEPSS & TESS: training tools for crisis first responders, managers and their support teams », présenté à Symposium INCOSE Human Systems Integration Conference, Biarritz, oct. 2019.

[16] N. Arpagian, La cybersécurité. Paris: Que sais-je ? / Repères, 2018. Consulté le: 25 mars 2022. [En ligne]. Disponible sur: https://www-cairn-info-s.proxy.bu.dauphine.fr/la-cybersecurite--9782130799511.htm

[17] Comité technique : ISO/IEC JTC 1/SC 27, « ISO/IEC 27002:2022 », 2022. Consulté le: 10 juin 2022. [En ligne]. Disponible sur: https://www.iso.org/cms/render/live/fr/sites/isoorg/contents/data/standard/07/56/75652.html

[18] R. West, « The psychology of security », Communications of the ACM, vol. 51, nº 4, p. 34-40, 2008, doi: 10.1145/1330311.1330320.

[19] A. Kerckhoffs, « La cryptographie militaire », Journal des sciences militaires, vol. 9, p. 5-38, janv. 1883.

[20] S. Kraemer, P. Carayon, et J. Clem, « Human and organizational factors in computer and information security: Pathways to vulnerabilities », Computers & Security, vol. 28, nº 7, p. 509-520, oct. 2009, doi: 10.1016/j.cose.2009.04.006.

[21] M. Salaün, « Intégration de l’utilisateur au contrôle d’accès : du processus cloisonné à l’interface homme-machine de confiance », Thèse de doctorat en informatique, Télécom SudParis, Paris, 2018. Consulté le: 3 mai 2022. [En ligne]. Disponible sur: https://www.ssi.gouv.fr/agence/publication/integration-de-lutilisateur-au-controle-dacces-du-processus-cloisonne-a-linterface-homme-machine-de-confiance/

[22] G. Conti, M. Ahamad, et J. Stasko, « Attacking information visualization system usability overloading and deceiving the human », in Proceedings of the 2005 symposium on Usable privacy and security - SOUPS ’05, Pittsburgh, Pennsylvania, juill. 2005, p. 89-100. doi: 10.1145/1073001.1073010.