# Psyber Sécurité : L'apport de la psychologie dans le management de la cybersécurité

**Jeanne Le Roy**

**Résumé :**
L'évolution constante du cyberespace et de la cybersécurité a conduit les organisations à accorder une attention accrue à la sécurité des informations et des systèmes. Ors, ce ne sont pas seulement les systèmes informatiques qui doivent être vérifiés, mais aussi les facteurs humains des organisations. Cet article a pour ambition d'éclairer, chercheurs et gestionnaires sur le rôle de la psychologie dans l'assistance aux individus, aux équipes et aux organisations. A l'issue de cette réflexion, nous constatons que les menaces croissantes dans le cyberespace équivalent à un changement de paradigme où chercheurs et experts en cybersécurité doivent intégrer les risques humains aux côtés des risques techniques. A partir de nos recherches, nous dissocions trois catégories de Comportements à Risques Internes en Cybersécurité (CRIC) : les CRIC non-intentionnels, les CRIC-intentionnels sans gravité, et les CRIC-intentionnels malveillants. A l'issue de cette analyse nous considérons qu'il est impératif d'accompagner les organisations et leurs employés à devenir plus résilients et à s'adapter aux cybermenaces en tenant comptes des travaux de la psychologie organisationnelle.

**Mots Clés :** Cybersécurité, psychologie organisationnelle, comportements à risques

**Abstract** :
The constant evolution of cyberspace et cybersecurity has led organizations to pay increased attention to information et system security. Ors, it is not only computer systems that need to be checked, but also the human factors of organizations. This article aims to enlighten researchers et managers on the role of psychology in assisting individuals, teams et organizations. At the end of this reflection, we note that the increasing threats in cyberspace

amount to a paradigm shift where researchers et experts in cybersecurity must integrate human risks alongside technical risks. Based on our research, we dissociate three categories of Cybersecurity Internal Risk Behaviors (CRIB): passive CRIB, active CRIB with et without malicious intent. At the end of this analysis, we consider that it is imperative to help organizations et their employees become more resilient et adapt to cyberthreats by taking into account the work of organizational psychology.

**Key Words :** Cybersecurity, organizational psychology, risk behaviors

## 1. Introduction

Bien qu'autrefois reléguées aux pages des romans de science-fiction, les idées de "cyber", "cyberespace" et de "cybersécurité" font désormais partis du quotidien des organisations. La cybersécurité a pour mission de sécuriser les informations, les systèmes ou autres biens de valeur contre l'exploitation, le vol ou la manipulation par des voies électroniques. La croissance exponentielle des différents types de menaces provenant de sources multiples (par exemple, les logiciels malveillants, la perte d'informations physiques, les menaces de réseau) a entraîné un besoin accru d'évaluer ces dangers sous des angles autres que ceux des ordinateurs et de la sécurité. Les conclusions d'un examen interdisciplinaire en cybersécurité mettent en lumière que les aspects comportementaux sont encore sous-explorés, les recherches sont essentiellement portées sur l'aspect technologique (Maimon et Louderback, 2019). A travers une revue de littérature sur les recherches conduites ces dernières années dans le champ de la psychologie cet article a pour ambition de mettre en lumière l'apport de la psychologie dans l'étude de la cybercriminalité.

Le cyberespace peut être définie comme un environnement complexe résultant de l'interaction de personnes, de logiciels et de services au moyen de dispositifs technologiques et de réseaux qui y sont connectés, qui n'existe sous aucune forme physique (Apvera, 2018). Par conséquent, les préjugés et les comportements des utilisateurs influencent les interactions avec les logiciels et la technologie et impactent le cyberespace. Les changements dans le cyberespace sont le résultat d'une interaction unique entre les technologies, les organisations, les acteurs individuels, les gouvernements et les institutions universitaires. Même lorsque l'on compare avec d'autres systèmes complexes de machines humaines (par exemple, les systèmes militaires), le rythme et la nature des changements dans les domaines du cyberespace dépassent ceux que l'on connaissait auparavant. Ainsi, malgré les avantages, la croissance exponentielle des technologies introduit des discontinuités presque impossibles à prévoir. En quelques heures, voire en quelques minutes, on peut découvrir une vulnérabilité, une défaillance, qui peut fondamentalement modifier le déploiement des informations et des

systèmes qui définissent une grande partie de la société moderne. En outre, de nombreuses technologies mises au point sont fragiles, au sens où la sécurité et les considérations connexes ne sont souvent qu'une réflexion après coup. Dans ce contexte la cybersécurité devient un acteur clé du bon fonctionnement des organisations. Or, la préférence de longue date de l'accessibilité et de la facilité d'utilisation plutôt que de la sécurité a entravé son développement technologique pendant des décennies (Etriotis, Tryfonas et Oikonomou, 2014). Cette dynamique a donné naissance au mythe du compromis convivialité-sécurité, selon lequel les organisations supposent que pour assurer la sécurité, elles doivent sacrifier la convivialité (Sasse, Smith, Herley, Lipford et Vaniea, 2016). Pour sortir de cette dualité, il semble essentiel de situer une menace de cybercriminalité dans un contexte multidisciplinaire (Holt, 2016). La technologie n'existe pas isolément de l'homme, il est donc prudent de prendre en compte l'élément humain et son interaction avec les technologies de l'information (Pfleeger et Caputo, 2012). Par exemple, considérons un logiciel malveillant ; il provient de l'ordinateur d'un humain et s'appuie sur la vulnérabilité d'un autre humain (la cible) pour atteindre un objectif. Bien que l'attaquant et la cible puissent ne jamais se rencontrer en personne, ils interagissent par le biais de leurs machines et, par procuration, l'un avec l'autre. Le côté comportemental de la cybersécurité nécessite plus de recherche et peut s'améliorer plus rapidement s'il est intégré aux facteurs humains et étudié au travers des sciences sociales.

Par conséquent, un changement de paradigme est essentiel à l'efficacité des techniques et pratiques actuelles. Étant donné que 90% des cyber-incidents sont d'origine humaine (selon le rapport de Kaspersky lab ,2019), ce changement nécessite d'étendre la recherche à des domaines sous-explorés tels que les aspects comportementaux de la cybersécurité. La cyberpsychologie considère l'existence humaine dans le contexte de nos propres outils numériques et de la façon dont nous interagissons dans un espace numérique (Norman, 2008). Les praticiens dans ce domaine étudient un large éventail de sujets, tels que l'utilisation des médias sociaux par les utilisateurs finaux, le profilage des cybercriminels, la sensibilisation du public aux risques de la cybersécurité ou encore le changement des comportements utilisateurs (Wiederhold, 2014). Les erreurs des utilisateurs ne sont pas influencées uniquement par la formation, qui est l'objectif principal des Responsables de La Sécurité des Systèmes d'Information (RSSI). Elles sont également initiées par le système lui-même, les préjugés des utilisateurs, la charge de travail de l'environnement, la gestion administrative, les pratiques de communication, les interfaces homme-machine, les distractions existantes. Il peut être plus facile de blâmer l'humain lors d'un cyber-incident que de blâmer le cyber-programme ou la conception des systèmes. En fait, la conception du système qui ne tenait pas compte du facteur humain est également à blâmer. Souvent, l'utilisateur ne voit pas les politiques de sécurité de la même manière que ceux qui les ont rédigées ou veulent qu'elles soient mises en œuvre.

Il ne fait aucun doute que la cybersécurité comportementale est importante et nécessite davantage de recherche. Dans cet article, nous discutons des contributions des recherches conduites en psychologie et en cybersécurité comportementale dans le domaine de la cyber sécurité. Cet examen nous permettra de nous interroger sur la manière dont les utilisateurs peuvent prendre des décisions éclairées lors d'incidents de cybersécurité. Nous pensons que faire progresser cette recherche interdisciplinaire pourrait apporter plus de pertinence et une augmentation des articles sur la cybercriminalité. Il est à noter que le faible nombre de manuscrits sur la cybercriminalité est dû au faible nombre de criminologues qui étudient la cybercriminalité (Payne et Hadzhidimova, 2018). Nous proposons ici d'aborder les vulnérabilités de la cybersécurité au regard des cyber comportements des salariés et plus spécifiquement au travers des comportements à risque réalisés par les personnes internes à l'organisation. Nous nous appuyons sur les travaux de Rodriguez, Bell, Brown et Carter (2017) sur l'erreur humaine pour définir le risque humain en cyber sécurité comme un évènement contingent et dommageable issue de toute action humaine qui dépasse une certaine limite de contrôle définie par le système d'exploitation. Comme présenté dans la figure 1, les Comportements Internes à Risque en Cybersécurité (CIRC) peuvent être appréhendés au regard de deux critères leur intentionnalité et leur conséquence (Arend, Shabadi, Idan, Keiran et Bereby-Meyer, 2020; Maalem Lahcen, Caulkins, Mohapatra, et Kumar, 2020). Un comportement à risque non intentionnel peut être due à un manque de connaissances organisées ou de compétences opérationnelles. Ce comportement à risque peut rester involontaire ou se transformer en un autre type (intentionnel ou malveillant). Aborder la cybersécurité à partir des comportements à risque permet d'adopter les leçons tirées des industries qui ont une longue histoire dans l'application des facteurs humains et ont construit des programmes matures.

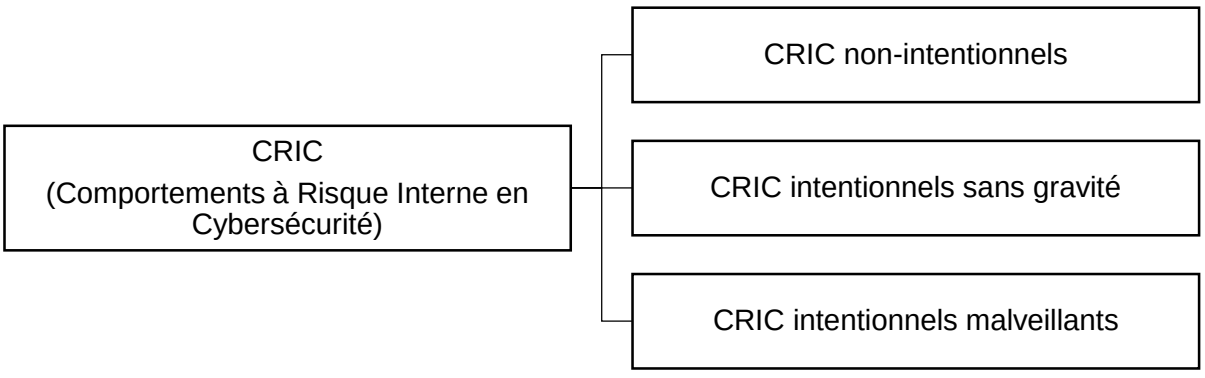


**Figure 1.** Classification des Comportements à Risques Internes en Cybersécurité (CRIC)

## 2. CRIC non-intentionnels via l'ingénierie sociale

### 2.1 CRIC non-intentionnels : le détournement amygdalien

Alors que les récits de cybercriminalité évoquent principalement le piratage d'ordinateurs, on observe que le cerveau de l'utilisateur peut aussi être, dans une certaine mesure, piraté. Le piratage informatique de haute technologie peut être difficile, surtout lorsque l'organisation cible a investi de nombreuses ressources dans les technologies de cybersécurité. En raison de cette difficulté, de nombreux cybercriminels ont découvert qu'il est souvent plus facile de convaincre une personne, ayant accès au système ou à l'information cible, de partager cet accès avec l'attaquant (que ce soit sciemment ou non). Les attaquants "hackent" essentiellement le cerveau de l'individu pour obtenir qu'il se conforme à leurs demandes. Pour ce faire, ils utilisent une technique connue sous le nom d'ingénierie sociale, qui repose sur un phénomène connu sous le nom de détournement amygdalien. L'amygdale est une petite structure située près du bas du cerveau qui joue un rôle essentiel dans le traitement des émotions. La théorie cognitive des émotions soutient que le ressenti d'émotions fortes comme la peur, la colère ou l'anxiété entraînent des comportements d'approches ou de retrait. En fonction de la forte émotion ressentie les individus s'engageront dans des comportements de fuite ou d'affrontement et ce de manière quasi-automatique au risque de nuire à l'organisation (Le Roy, Bastounis, Minibas-Poussard, 2020). Quand l'amygdale est stimulée - entrainant une émotion forte- l'activité du cortex préfrontal est réduite, soit le contrôle conscient du raisonnement, de la pensée critique et de la prise de décision. Ce phénomène a été désigné par Golelam (1997) comme le détournement de l'amygdale où la forte réaction de l'amygdale entraîne en réponse une réaction impulsive excessive à une situation. Tout comme les systèmes informatiques présentant des vulnérabilités techniques les rendant faibles face à un agresseur, le détournement amygdalien peut être considéré comme une vulnérabilité des humains qui, lorsqu'elle est correctement exploitée, peut manipuler un individu pour qu'il prenne une mesure impulsive et malheureuse. Dans le contexte de la cybersécurité, cette action peut consister à cliquer sur un lien vers un site web malveillant, à ouvrir une pièce jointe de courriel malveillant ou à donner aux attaquants des informations qu'ils pourront utiliser à des stades ultérieurs de leurs attaques. Les attaquants tentent de créer un sentiment de peur, d'anxiété, d'urgence, de panique, voire d'excitation pour convaincre leurs cibles d'agir de manière impulsive et sans penser que la situation est peut-être dangereuse et destinée à piéger des utilisateurs sans méfiance. Les agresseurs essaient de tirer parti de leurs compétences sociales combinées au désir inné de l'Homme d'aider et de faire confiance aux autres. De nombreux auteurs ont cherché à identifier et définir les principes d'influence qui guident les comportements à risques non intentionnels (Caulkins 2017 ; Cialdini 2008 ;

Ferreira et al., 2015). Dans le tableau 1 ci-dessous nous proposons une définition et une illustration pour les sept principales stratégies d'ingénierie sociale.

**Tableau 1**. Définitions et Illustrations des sept principales stratégies d'ingénierie sociale

| Appellation | Définition | Exemple |
|---|---|---|
| **Aimer** | Génère un faux sentiment de crédibilité | Les cybercriminels peuvent l'utiliser pour établir des relations ou encourager certains comportements en générant de faux likes et en augmentant artificiellement le nombre de followers sur les réseaux sociaux pour donner l'impression que d'autres personnes soutiennent ce comportement. |
| **Réciprocité** | Provoque un sentiment d'obligation de rendre des faveurs | Les cybercriminels peuvent offrir des services ou des produits gratuits et s'attendre à un accès ou à des données en retour. |
| **Preuve sociale ou le consensus** | Facilite le soutien et l'engagement dans les attitudes d'autrui | Les cybercriminels peuvent utiliser ce type de validation pour influencer les utilisateurs et accéder aux données. Lorsque les utilisateurs ne sont pas certains, ils peuvent facilement répondre à d'autres personnes, en particulier à leurs pairs. |
| **Persuasion par les pairs** | Persuasion par les pairs | Les cybercriminels peuvent persuader des initiés de voler des données pour une cause qu'un pair ou un modèle de rôle promeut. |
| **Autorité** | Abus de pouvoir de l'autorité | L'autorité peut apporter de fausses réclamations et influencer un utilisateur qui se méfie de la perte d'emploi. |
| **Cohérence.** | S'appuie sur le besoin d'apparaître ou de rester cohérent | Les cybercriminels peuvent découvrir des actions cohérentes et les utiliser pour distraire un utilisateur avant une attaque. |
| **Rareté des ressources** | Rend un utilisateur vulnérable | Il peut inciter un utilisateur à prendre une action immédiate sans penser aux conséquences telles qu'une violation de données. |

Les vecteurs d'attaque couramment utilisés par les cybercriminels sont le *phishing* (par e-mail), le *vishing* (appel téléphonique), l'usurpation d'identité et le *smishing* (SMS). Une autre escroquerie d'ingénierie sociale courante consiste à offrir à la victime la possibilité de participer pour gagner un objet de valeur, tel qu'un téléphone. Un attaquant pourrait envoyer un courriel à des centaines d'employés d'une entreprise leur offrant la possibilité de cliquer sur un lien et d'entrer le nom d'utilisateur et le mot de passe de leur ordinateur de travail pour "vérifier leur identité" lors de la procédure d'inscription. Bien entendu, les attaquants collectent ensuite les identifiants à utiliser dans les étapes ultérieures de leurs attaques. Par ailleurs, certains attaquants envoient des courriers électroniques en se faisant passer pour du support technique. Ces courriels indiquent aux destinataires qu'ils viennent de cliquer sur un lien dans un courriel de *phishing* et qu'ils doivent télécharger et exécuter un programme pour nettoyer tout logiciel malveillant sur leurs ordinateurs et les sécuriser à nouveau. En réalité, ce programme donne à l'attaquant un accès secret et à distance aux ordinateurs des victimes. Lorsqu'ils envoient ce genre de courriels, les attaquants créent de l'excitation en offrant la possibilité de participer à un dessein, et ils créent de la peur et de la panique lorsqu'ils informent la victime de la possibilité d'une infection par un logiciel malveillant. Ces deux prétextes suscitent une forte réaction émotionnelle et un comportement impulsif. L'agresseur a exploité avec succès la vulnérabilité du détournement d'amygdales pour manipuler le comportement des victimes et obtenir des noms d'utilisateur, des mots de passe et un accès à distance aux ordinateurs.

La myriade d'escroqueries liée à la COVID-19 est un exemple très significatif d'ingénierie sociale. L'idée d'attraper ce virus a terrifié un nombre impressionnant de personnes, et beaucoup souhaitent porter des masques pour se protéger des maladies. C'est une grande opportunité pour les ingénieurs sociaux malveillants. Les personnes qui sont terrifiées à l'idée d'attraper le virus n'hésiteraient pas à cliquer sur un lien qui prétend les conduire à un site web à partir duquel elles peuvent acheter des masques de haute qualité à un prix abordable. Un attaquant pourrait facilement mettre en place un faux site web de commerce électronique qui infecterait les ordinateurs des victimes avec un logiciel malveillant une fois qu'ils ont visité le site. Dans ce scénario, l'attaquant crée un puissant sentiment d'excitation qui déclenche une réaction automatique, presque désespérée, en raison de la peur ressentie par la victime. L'amygdale prend le relais et inhibe l'activité du cortex préfrontal, de sorte que l'utilisateur, sans méfiance, ne doute pas de la légitimité du lien.

Bien qu'il puisse être difficile de résister à ce type d'attaques, il existe un moyen de se défendre. Si un courriel ou un appel téléphonique génère de l'anxiété, de la peur ou une grande excitation et demande une action, la solution pour l'utilisateur réside alors dans le fait de réduire dans un premier temps l'intensité émotionnelle afin que cette dernière ne soit pas

l'élément déclencheur de l'action mais bien la raison. Ainsi une relaxation intentionnelle et une réflexion consciente aide le cortex préfrontal à reprendre le contrôle de la situation et à prévenir les mauvaises décisions. La connaissance des techniques des agresseurs ainsi que stratégies de réductions de l'intensité émotionnelle perçue sont des remparts au détournement d'amygdales. L'implémentation des formations de prévention accès sur la réduction des comportements à risque non intentionnelles doit ainsi combiner à la fois l'information des stratégies d'ingénieries sociale en fonction notamment des caractéristiques utilisateurs (variables environnementales : fonction, type de poste, lieu de travail… et variables interpersonnelles : personnalité, genre, culture…) couplée au mécanisme cognitif en jeu afin de les contourner.

### 2.2 CRIC non-intentionnels : Caractéristiques utilisateurs

Il est reconnu que l'humain en tant qu'utilisateur final peut être une porte dérobée critique dans le réseau (Karwowski et Ahram, 2019). Cartographier l'utilisateur et l'environnement nécessite de poser un ensemble de questions sur leurs caractéristiques, rôles, connaissances, compétences, expérience, tâches, responsabilités, traits de personnalité, points d'accès et emplacements, interface homme-machine, etc. De nombreuses études ont constaté que l'efficacité des principes d'ingénierie sociale est liée aux caractères de la personnalité de l'utilisateur. A titre d'exemple, l'agréabilité d'un utilisateur a augmenté la vulnérabilité envers le goût, l'autorité, la réciprocité et la preuve sociale. Le névrosisme indique qu'un utilisateur est moins sensible à la plupart des attaques d'ingénierie sociale. Un utilisateur consciencieux peut ne pas résister aux principes d'autorité, de réciprocité, d'engagement et de cohérence, en particulier lorsque les engagements sont rendus publics. L'utilisateur d'extraversion peut être plus vulnérable au principe de rareté puisque ce dernier est considéré comme une excitation. La conscience peut réduire la vulnérabilité de l'utilisateur aux cyberattaques. Pourtant, la conscience a une tendance plus élevée à respecter les engagements qui peuvent rendre la personne vulnérable à la poursuite des tactiques d'ingénierie sociale. L'agréabilité d'un utilisateur peut augmenter sa vulnérabilité au *phishing* et au partage de mots de passe. L'ouverture réduit la vulnérabilité de l'ingénierie sociale car les utilisateurs plus éduqués au numérique détectent mieux les attaques d'ingénierie sociale (Caulkins 2017; Uebelacker et Quiel, 2014). Par ailleurs, Halevi et col., (2013) ont observé que les femmes sont plus vulnérables aux attaques de *phishing* que les hommes, ils ont également observé une forte corrélation entre la névrose et la réactivité aux attaques de *phishing*. Whitty et al. (2015) ont constaté que les jeunes étaient nettement plus susceptibles de s'engager dans la pratique peu sûre du partage de mots de passe. Ces premiers résultats sont intéressants dans une

démarche de prévention ciblée des utilisateurs. Toutefois, il est important de noter qu'il existe encore trop peu d'études sur le sujet permettant de confirmer ces premières observations.

### 2.3 CRIC non-intentionnels : Stratégies de préventions

La disponibilité accrue de l'information a des effets positifs importants, cependant le simple fait de fournir des informations ne suffit pas à entraîner un changement de comportements significatif et durable (Smith et Petty, 1996). Les gouvernements et les entreprises investissent des sommes considérables pour influencer le comportement en ligne et le succès de cette démarche serait maximisé s'ils s'appuyaient sur des preuves solides du comportement réel des personnes (Dolan, Hallsworth, Halpern, King et Vlaev, 2010). Divers articles de recherche ont examiné les facteurs qui influencent le comportement humain et le changement de comportement, mais l'un des plus complets est celui de Dolan et col., (2010). Dans leur article, les auteurs présentent neuf facteurs critiques, à savoir (1) le messagé qui communique l'information; (2) les incitations (nos réactions aux incitations sont façonnées par des raccourcis mentaux prévisibles, comme éviter fortement les pertes) ; (3) les normes (comment les autres nous influencent fortement); (4) les défauts (nous suivons des options prédéfinies); (5) la saillance (ce qui nous concerne attire généralement notre attention); (6) l'amorçage (nos actes sont souvent influencés par des signaux subconscients); (7) l'affect (les associations émotionnelles peuvent fortement influencer nos actions); (8) les engagements (nous cherchons à être cohérents avec nos promesses publiques et nos actes réciproques); (9) l'ego (nous agissons de manière à nous sentir mieux dans notre peau). Ces facteurs mettent en évidence les ingrédients clés d'une approche globale visant à influencer le changement de comportement, puisque les mécanismes psychologiques auxquels ils font référence sont au cœur de tout type de décision. En outre, ces mécanismes peuvent influencer la motivation de l'utilisateur à adopter réellement les connaissances offertes par une campagne de sécurité et à se comporter en conséquence. Afin de mettre en œuvre le changement, les sources d'influence actuelles (conscientes ou inconscientes, personnelles, environnementales ou sociales) doivent être identifiées.

Pour savoir comment se prévenir des attaques utilisant de l'ingénierie sociale, nous nous proposons de regarder le cas de l'entreprise Facebook. En 2014, le département sécurité de Facebook souhaitait encourager les utilisateurs à profiter davantage des fonctionnalités de sécurité de la plateforme, telles que l'activation des notifications de connexion, des approbations de connexion et des contacts de confiance. L'entreprise a alors investi dans des stratégies de préventions. Das, Kramer, Dabbish et Hong (2014) ont testé l'augmentation de l'observabilité des normes sociales de cybersécurité sur la persuasion des utilisateurs à adopter ces fonctionnalités de sécurité. L'équipe de recherche a montré à un échantillon de

50000 utilisateurs actifs de Facebook l'une des huit annonces de sécurité possibles les incitant à adopter ces fonctionnalités de sécurité. Les sept messages de protection sociale ont informé les utilisateurs que leurs amis Facebook utilisaient déjà ces fonctionnalités de sécurité. Ces messages variaient en termes de spécificité et de formulation - de l'indication du nombre exact d'amis au simple énoncé de «quelques» amis. Un groupe de contrôle a reçu un message sans aucun encadrement social (par exemple, «Vous pouvez utiliser les paramètres de sécurité pour protéger votre compte et vous assurer qu'il peut être récupéré si jamais vous perdez l'accès»). Les résultats de cette recherche démontrent que si toutes les interventions basées sur la preuve sociale étaient efficaces, le plus efficace était de montrer simplement aux utilisateurs le nombre spécifique de leurs amis qui utilisaient des fonctionnalités de sécurité sans aucun cadrage subjectif - ce qui a conduit 37% des utilisateurs en plus à explorer les fonctionnalités de sécurité promues par rapport à l'annonce non sociale.

### 3. CRIC – Intentionnel sans gravité

Un comportement à risque intentionnel est causé par un utilisateur qui a pleinement conscience de réaliser un comportement à risque et agit en conséquence. Comme mentionné précédemment, bien qu'elles puissent être les premières qui viennent à l'esprit, les personnes extérieures ne sont pas la seule menace pour les organisations. 60% des menaces de cybersécurité proviennent d'une source interne (selon Cyber Security Intelligence Index, IBM, 2016). Liu et col., (2016) distinguent sept principaux CRIC-Intentionnels (1) l'escalade des privilèges dans laquelle l'utilisateur tente d'obtenir l'accès en utilisant tous les privilèges et applications locales disponibles ; (2) les supports amovibles dans lesquels l'utilisateur tente de copier des données et des fichiers sur un dispositif amovible tel qu'un disque dur, une clé USB ou un CD ; (3) l'exportation par courrier électronique dans laquelle l'utilisateur tente d'envoyer des données par courrier électronique ; (4) le changement d'extension de fichier dans lequel l'utilisateur tente de changer d'extension de fichier afin de tromper tout code de surveillance de réseau ; (5) le chiffrage et déchiffrage des opérations dans lesquelles l'utilisateur essaie de modifier par calcul un document secret ; (6) la recherche inhabituelle dans laquelle l'utilisateur cherche des documents auxquels il n'est pas autorisé à accéder ; (7) l'installation de logiciels malveillants sur le système. Les trois derniers renvoient plus spécifiquement à des cas de CRIC-intentionnels à des fins malveillantes.

Les menaces internes sont particulièrement préoccupantes pour les organisations car les employés ont déjà accès aux systèmes d'information et aux serveurs de l'organisation (Coovert, Dreibelbis, et Borum, 2016). C'est donc un domaine dans lequel les recherches conduites en psychologie organisationnelle peuvent être particulièrement utiles. En effet, au regard de cette littérature, il est intéressant de noter que les comportements à risques

intentionnels peuvent être considérés comme des comportements contre-productifs. Les Comportements Contre-productifs Motivés (CCM) sont des comportements allant à l'encontre des normes établies et ce faisant nuisent à l'organisation et/ou ses membres (Le Roy, Finkelstein et Rubens, 2012). Il existe deux philosophies différentes sur la manière d'aborder les menaces internes : (a) les prévenir ou (b) les attraper. La prévention de tel comportement passe par la compréhension de leur facteurs explicatifs, pour cela nous pouvons nous appuyer largement sur les travaux conduits en psychologie organisationnelle sur les CCM.

### 3.1 Facteurs explicatifs des CRIC-intentionnels sans gravités

Les facteurs expliquant la part la plus importante des CRIC-intentionnels sans gravités sont essentiellement liés à la culture organisationnelle et le type de management mis en place. Ainsi on observe que les organisations ayant une culture cybersécurité (1) pas assez ciblée (2) manquant de cohérence entre le discours et la pratique (3) pas assez liée aux postes des salariés (4) non-engageante, ont des CRIC-intentionnels sans gravités nettement plus élevés (Trim et Huptron, 2016). Face à une culture mettant en place des processus et des règles non comprises, non expliquées ou encore pouvant être jugées arbitraires, les salariés apporteront leurs propres réponses à leurs incompréhensions pouvant conduire à des comportements de contournements de la règle soit des CRIC-intentionnels sans gravité, comportements adaptatifs pouvant, par ailleurs, conduire à de l'innovation et de la performance (Brière, Le Roy, Meier, 2020).

De même une culture organisationnelle axée sur le contrôle et/ou la méfiance générera un niveau d'engagement organisationnel très faible dans lequel les salariés seront moins respectueux de leur organisation et de ses processus. On observe que les organisations prenant le temps d'expliquer les raisons des règles établies ou encore laissant la possibilité aux salariés d'exprimer leur avis se verront avoir un taux de comportement contreproductif intentionnels sans gravités nettement moins élevés. Ainsi quand les organisations observent des comportements intentionnels de contournement de la règle, la stratégie à adopter n'est pas de réaliser un rappel à la règle - qui par moment peut même être accompagnée de sanctions en cas de contournement. Cette stratégie renforcera la distance entre l'organisation et ses salariés, le sentiment d'injustice procédurale et interactionnelle développant alors une volonté de représailles organisationnelle renforçant la réalisation de de comportements contreproductifs sans gravités (Wolfe et Lawsen, 2020). Comportement pouvant évoluer vers des comportements à risques et/ou des CRIC-intentionnels malveillants avec de réelles intentions de nuire. Ainsi, quand les salariés n'ont pas la possibilité de quitter l'entreprise et se sentent alors « prisonniers » de cette dernière ils peuvent être conduits à réaliser des comportements de représailles à des fins malveillantes (Wolfe et Lawsen, 2020).

### 3.2 Les défis de la prévention des CRIC-intentionnels sans gravités

Sinclair et Smith (2008) abordent les défis de la prévention des attaques par le contrôle d'accès. En particulier, ils discutent de la difficulté de trouver un équilibre entre le fait de permettre aux membres des organisations de remplir leurs tâches avec succès et le déploiement de la technologie de contrôle d'accès pour prévenir les menaces d'initiés qui interfèrent dans leurs activités. Ainsi, les utilisateurs peuvent parfois se lasser des procédures et des processus de sécurité, surtout s'ils perçoivent la sécurité comme un obstacle qui les empêche de s'acquitter de leur tâche principale (par exemple, être bloqué pour visiter un site de téléchargement de musique parce que le navigateur a déclaré que le site pouvait contenir un logiciel malveillant). Il peut également être stressant de rester à un niveau élevé de vigilance et de sensibilisation à la sécurité. Ces sentiments décrivent ce qu'on appelle la "fatigue de la sécurité" et peuvent être dangereux pour la santé générale d'une organisation ou d'une société. Dans le domaine de la sécurité, le "triangle de la sécurité, de la fonctionnalité et de l'utilisabilité" décrit la situation où l'on essaie de créer un équilibre entre trois objectifs, généralement contradictoires (Waite, 2010). Si vous commencez au milieu et que vous vous dirigez vers la sécurité, vous vous éloignez également de la fonctionnalité et de la convivialité. Dans le cas d'un système super sécurisé on observe à la fois des difficultés dans la réalisation des tâches par manque d'accès à certaines fonctionnalités ainsi qu'une volonté de contournement des systèmes de sécurité par « peur du gendarme » car les logiciels de sécurité sont ceux qui permettent le mieux d'observer les faits et geste des salariés. A l'inverse, dans le cas où l'accent est mis sur la convivialité le système est alors bien moins sécurisé et tout le monde peut l'utiliser (même les personnes indésirables, comme les cybercriminels). Un exemple récent du type de cyber attaque lorsque la convivialité est privilégiée est le *zoombombing ou zoom raiding* (Marotti, 2020) soit l'une intrusion non désirée et perturbatrice, lors d'une vidéoconférence. Un incident typique de *zoombombing*, est le détournement d'une session de téléconférence par l'insertion de matériel de nature obscène, raciste ou antisémite, entrainant généralement la fermeture de la session. Lors du confinement lié à la Covid-19, généralisant le travail à distance, le *zoombombing* a causé des problèmes importants aux écoles, aux entreprises et aux organisations du monde entier. En conclusion, la fatigue de la sécurité devient un problème lorsque le triangle penche trop loin du côté de la sécurité et que les exigences sont trop lourdes à gérer pour les utilisateurs. Il faut donc trouver un équilibre entre la sécurité du système, la facilité d'utilisation et les fonctionnalités (Nurse, Creese, Goldsmith et Lamberts, 2011).

Par ailleurs, le contrôle perçu de son environnement de travail, qui peut être impacté par l'autonomisation, a une incidence forte sur l'engagement et les comportements organisationnels (Eklund et Backstrom, 2006). Les effets positifs du contrôle perçu

apparaissent principalement dans les situations où les individus peuvent améliorer leur condition par leurs propres efforts. Lorsque nous appliquons cette théorie à la cybersécurité, nous pouvons supposer que les utilisateurs d'ordinateurs domestiques ont souvent un niveau élevé de contrôle effectif sur leur exposition aux risques. En psychologie, la théorie de l'approche réglementaire (Higgins,1998) propose que, dans un mode d'autorégulation axé sur la promotion, les comportements des individus sont guidés par le désir de s'aligner sur son moi idéal (le "moi idéal" est-ce qui motive généralement les individus à changer) et la recherche de gains. Dans un mode d'autorégulation axé sur la prévention, les comportements individuels sont guidés par un besoin de sécurité, la nécessité de s'aligner sur son "soi" idéal en remplissant ses devoirs et obligations et en s'efforçant de ne pas subir de pertes. Ainsi, l'efficacité des campagnes de prévention peut être améliorée soit en utilisant deux types de messages (axés sur la prévention et la promotion), soit en mettant l'accent sur un type de réglementation par le biais de publicités (More,2011).

## 4. CRIC-intentionnels Malveillants : Réussir à la détecter

La menace interne liée à des CRIC malveillants est largement reconnue comme un problème de la plus haute importance pour la gestion de la cybersécurité (Theoharidou et al., 2005 ). La menace d'initié fait référence à la menace que représentent pour les organisations les personnes qui ont le droit légitime d'accéder au système interne d'une organisation. Un initié est un cybercriminel de l'intérieur de l'organisation ; par conséquent, cet initié a des droits d'accès et se trouve derrière les pares-feux. Les menaces d'initiés comprennent la fraude, le vol de propriété intellectuelle et les tentatives de sabotage du réseau de l'organisation (Retazzo, Keeney, Kowalski, Cappelli, et Moore, 2004). D'après Fyffe (2008) les données personnelles extraites des bases de données peuvent être vendues sur le marché pour 48£ par donnée. Ainsi, un initié qui vole un million d'enregistrements de données à une société de cartes de crédit, d'assurance ou de soins de santé peut potentiellement se faire jusqu'à 48 millions de livre sterling.

### 4.1 Menaces d'initiés : Les techniques des cybercriminels

Il est important de comprendre les techniques de piratage et les motivations des cybercriminels afin d'anticiper leurs mouvements. Bien qu'un cybercriminel puisse suivre diverses étapes pour exécuter une attaque réussie, une intrusion réseau habituelle implique (i) une reconnaissance pour collecter des informations, (ii) une analyse pour configurer un profil de vulnérabilité, (iii) l'obtention ou l'intrusion d'un point accès (iv) maintenir l'accès en franchissant d'autres niveaux

ou en implantant des programmes pour garder l'accès et couvrir les traces pour masquer les sentiers (Lahcen, Mohapatra et Kumar, 2018 ).

Shetty, Shetty, Shetty et D'Souza (2018) ont étudié les techniques de cyber attaques : (i) L'attaque des mots de passe dit vulnérables cassés par dictionnaire. Le cybercriminel profite du fait que les utilisateurs ne peuvent pas se souvenir des mots de passe difficiles ou de ceux qui n'ont aucun sens, ils utilisent donc des mots de passe pertinents ou faciles. Souvent, les cybercriminels trouvent les utilisateurs qui adoptent des mots de passe faibles tels que « 123456 » ou « mot de passe ». Actuellement, les entreprises améliorent la syntaxe des mots de passe et imposent des procédures de modification spécifiques. Pourtant, les utilisateurs utilisent toujours les mêmes mots de passe sur les sites Web L'attaque des mots de passe quand le cyber criminel a aucune connaissance de la cible, est appelé « l'attaque force brute » elle tient compte de l'ensemble des possibilités. (ii) Injection SQL (*Structured Query Language*) de code nuisible pour modifier la structure de la requête SQL. Il manipule la base de données du site Web. (iii) *Cross Site Scripting* (XSS) est un vecteur d'attaque qui injecte des scripts malveillants dans les pages Web de la victime. (iv) Le *phishing* via l'ingénierie sociale. (v) Le piratage sans fil, en raison d'une faiblesse de certains réseaux. (vi) Le *Keylogger,* soit un logiciel qui s'exécute en arrière-plan et capture le clavier de l'utilisateur. Avec lui, les cybercriminels peuvent enregistrer les informations d'identification.

Le Black Report 2018 (Pogue, 2018) accorde une attention particulière au temps nécessaire aux cybercriminels pour s'introduire dans un cyber-système d'une organisation. La nette majorité des répondants disent qu'ils peuvent accéder au système d'une organisation, cartographier et détecter des données précieuses, pour les compromettre dans les 15 heures. Désormais, la plupart des rapports du secteur indiquent que l'écart moyen entre une brèche et sa découverte se situe entre 200 et 300 jours (Pogue, 2018). Il est clair que les cybers criminels ont toujours un avantage sur les cybers défenseurs. Tous les cybercriminels ne pensent pas de la même manière que les cyberdéfenseurs ou de manière linéaire. Par conséquent, les défenseurs doivent être interdisciplinaires afin de prendre en compte diverses techniques et angles d'attaques. Ainsi, les particularités du comportement humain ainsi que celles du contexte organisationnel doivent être prises en considération à l'ère du développement technologique, au lieu d'être mise de côté.

### 4.2 Menaces d'initiés : Profils des salariés et contexte organisationnel

Un cybercriminel informatique est un humain qui utilise l'intellect technique pour obtenir un accès non autorisé aux données afin de les modifier, les supprimer ou les vendre par quelque moyen que ce soit (Pal et Anet, 2018). La littérature traite de plusieurs profils de

cybercriminels. Ils ont différents niveaux de formation, ils sont soit indépendants, soit au service d'organisations (cf. Tableau 2).

**Tableau 2.** Listes (non exhaustives) des principales catégories de cybercriminels

| Appellations | Niveau de compétences | Motivations |
|---|---|---|
| ***Scriptkiddies*** | Novices | La curiosité ou la notoriété. |
| ***Cyber-punks*** | Moyen | La notoriété avec un gain financier |
| ***Black hat*** Cybercriminels professionnels | Très élevé | Gain financier |
| **Cyber-mercenaires** Guerriers de l'information | Très élevé | Espionnage (placés sous des groupes d'État-nation) |
| **Hacktivistes** | Très élevé | Motivation idéologique |

Hormis les *scriptkiddies*, les menaces d'initiés peuvent provenir de tous les profils de cybercriminels. Toutes les organisations ne vont pas attirer les mêmes cybercriminels. La première étape est donc d'identifier les types d'attaques potentielles ainsi que les profils de cybercriminels motivés par une attaque de l'organisation au regard du profil de cette dernière. Cette identification permettra au défenseur de se mettre davantage dans « la peau » des cybercriminels afin de proposer / d'investir dans des stratégies de défense plus ciblés. La seconde étape se situera au niveau du recrutement. Ainsi le recrutement des cyber défenseur doit savoir s'écarter des recrutements plus classiques. Une stratégie de cybersécurité solide commence par la sélection des bonnes personnes pour identifier, construire et protéger les systèmes de cyberdéfense d'une organisation. En outre, en raison de la nature intrinsèquement cognitive et informatisée du travail de cybersécurité, les techniques de sélection non conventionnelles peuvent être particulièrement utiles, notamment les méthodes telles que les entretiens cognitifs, les observations de systèmes et même les activités de tri (par exemple, Paul et Whitley, 2013). Les praticiens ont récemment recommandé une approche multidimensionnelle de la cybersécurité pour recruter et retenir le personnel de cybersécurité qui tient compte des caractéristiques distales (par exemple, la capacité cognitive, la personnalité) et proximales (par exemple, les compétences sociales, les connaissances techniques (Jose, La Port, et Trippe, 2016). Mais il est encore nécessaire de comprendre les prédicteurs de succès pour les emplois professionnels de la cybersécurité. Les recherches ont montré que les cyber-défenseurs qui réussissent doivent connaître la technologie et les systèmes d'information, ainsi que la capacité d'apprendre et de s'adapter (Ben-Asher et Gonzalez, 2015). Il existe également des considérations éthiques pour le recrutement et la sélection d'analystes talentueux : par exemple, les pirates informatiques au

sein d'une organisation peuvent facilement utiliser leurs compétences à des fins altruistes (pirates en chapeau blanc) ou malveillantes (pirates en chapeau noir), ou quelque part entre les deux (pirates en chapeau gris). Il est donc essentiel de prendre en compte les motivations des cyber-défenseurs lors du processus de sélection afin de réduire le risque de menace interne. Enfin, l'identification des initiés peut également passer par une phase plus technique.

### 4.3 Menaces d'initiés : les techniques de détections

La détection d'initiés malveillants représente un énorme défi pour de nombreuses raisons. Tout d'abord, le nombre d'initiés malveillants découverts au sein d'une organisation donnée est généralement très faible, peut-être une poignée seulement sur une décennie. Du point de vue des algorithmes d'apprentissage automatique, cela donne un ensemble de données très déséquilibré (plus de 99,9% des utilisateurs « honnêtes », et généralement bien moins de 0,1% d'initiés malveillants) dont on peut tirer automatiquement des enseignements (Pfleeger, 2008). Dans le cas des menaces d'initiés, ce type de résultat est très problématique, car nous nous intéressons à la détection de la classe minoritaire.

Deuxièmement, il n'existe pas d'ensemble de données exhaustives accessible au public à des fins de test - les entreprises sont réticentes à partager de telles données et les organismes de sécurité ne le peuvent pas. Ainsi, même les données de formation provenant de sources du monde réel sont difficiles à obtenir.

Troisièmement, le peu de données sur la formation qui sont publiquement disponibles sont imparfaites. Par exemple, nous connaissons des données sur la formation dans lesquelles les données des utilisateurs honnêtes sont réelles alors que celles des "initiés malveillants" sont injectés artificiellement (Maloof et Stephens, 2007). De plus, dans de tels cas, les initiés injectés sont souvent basés sur des attaques passées, ce qui laisse implicitement supposer que les futurs attaquants le feront de la même manière que par le passé. Ainsi, même les données qui étaient auparavant déclarées "réelles" souffrent de graves lacunes. L'une des principales fragilités des travaux menés à ce jour, repose sur le manque d'études comportementales mesurant le comportement réel des utilisateurs pouvant être potentiellement malveillant. La seule exception que nous connaissons est une expérience à petite échelle conduite par Caputo, Maloof, et Stephens (2009) où les participants ont été affectés au hasard à l'une des deux conditions suivantes utilisateur bénin (groupe témoin) ou utilisateur malveillant (groupe expérimental). Dans les deux conditions, les participants lisent un scénario en se mettant dans la peau d'un salarié qui rencontre des difficultés financières et doit trouver et fournir les informations les plus utiles afin d'améliorer sa situation financière. Dans le cas d'une situation bénigne, la personne a été formée à la notion de performances exceptionnelles, performance régulièrement associée à une promotion et une augmentation

de salaire. Dans le cas de la situation malveillante, la personne a eu la possibilité de commencer un nouvel emploi mieux rémunéré, mais l'offre était conditionnée à l'apport d'informations internes provenant de l'ancienne société, ce qui lui donnait un avantage concurrentiel. Ils ont surveillé les activités des participants. Leur analyse préliminaire a révélé des modèles intéressants et significatifs de comportements malveillants. Certains des schémas qu'ils ont trouvés pour distinguer le comportement normal du comportement malveillant sont liés aux actions comme la récupération de documents, l'édition de documents et la sauvegarde de documents sur des supports externes. Ces premiers résultats confirment la pertinence du jeu de rôle comme méthodologie pour étudier la menace d'initié. Cette première étude comportementale très prometteuse nous éclaire sur la nécessité d'accentuer les recherches dans ce domaine afin de comprendre et de prévenir les attaques d'initiés dans l'avenir.

Le quatrième défi qui complique la détection des menaces d'initiés est que le comportement malveillant de l'initié ne représente qu'une petite partie des actions du sujet. Les actions malveillantes ont lieu parallèlement à d'autres comportements normaux qu'un initié adopte dans le cadre de son travail. Cela renforce la nature déséquilibrée de l'ensemble de données, car non seulement il y a un petit nombre de sujets malveillants, mais pour ces sujets, seule une petite partie du comportement est malveillante. Myers, Grimaila, et Mills (2009) soutiennent que les menaces d'initiés impliquent deux scénarios : (1) L'utilisation non autorisée de privilèges dans laquelle un initié malveillant tente d'accéder à des données auxquelles il n'est pas autorisé à accéder (par exemple, en accédant à des compartiments de données qui ne sont pas pertinents pour sa mission) et/ou utilise des ressources autorisées de manière inappropriée (par exemple, en envoyant par courriel un fichier auquel il est autorisé à accéder à une personne qui n'est peut-être pas autorisée à le voir). (2) L'utilisation d'outils de cartographie pour détecter les systèmes critiques et leurs éventuelles faiblesses.

En conclusion de ces quatre défis, nous pouvons citer la démarche de prédiction des menaces d'initiés développée par Magklaras et Furnell (2001) qui s'articule autour de trois tâches principales : (1) Surveiller les aspects liés à l'emplacement des fichiers et des répertoires afin de tenir compte du fait que certains types d'utilisation abusive d'un système informatique sont liés au placement de certains fichiers dans certains répertoires. (2) Analyser le contenu des fichiers afin de vérifier certains schémas tels que les signatures de virus à l'intérieur des fichiers. (3) Contrôler l'intégrité des fichiers afin de vérifier si l'un d'être eu a été compromis, par exemple des fichiers système ou des fichiers de démarrage. Ils développent ensuite des mesures de menace potentielle évaluée qui caractérisent les caractéristiques du comportement des utilisateurs, telles que leur connaissance d'un système de fichiers, le contenu des fichiers dans leur espace de travail et la manière dont ils interagissent avec le réseau (par exemple, l'histogramme des types de trafic qu'ils reçoivent

et/ou envoient). Enfin, nous pouvons également rajouter un dernier niveau d'analyse qui consiste à classifier les fichiers auxquels les salariés accèdent. Toutefois, aucun résultat empirique n'a encore été rapporté sur l'efficacité de ces quatre outils de prédictions des menaces d'initiés.

## 5. Conclusion

Il existe une relation symbiotique entre les disciplines de l'informatique et de la psychologie : les psychologues ont aidé de nombreuses manières à comprendre la façon dont les systèmes informatiques sont développés et utilisés. De plus, la compréhension des ordinateurs a également aidé les psychologues à modéliser et à étudier les processus cognitifs et sociaux des utilisateurs. Ainsi, pour concevoir, développer, mettre en œuvre et évaluer des systèmes informatiques sécurisés, les cyber-défenseurs comme les dirigeants doivent comprendre les concepts et les méthodes de recherche en psychologie. Pour comprendre les risques potentiels des systèmes sociotechniques, les experts en cybersécurité doivent comprendre et prendre en compte la façon dont les utilisateurs perçoivent, se souviennent, ressentent, pensent et résolvent les problèmes. Il est également important de prendre en considération les différences individuelles des utilisateurs et les comportements sociaux pour parvenir à une interaction efficace entre les personnes et les systèmes informatiques. La compréhension de ces sujets psychologiques permettra d'envisager les capacités et les limites potentielles des utilisateurs d'ordinateurs et de les aider à concevoir des systèmes informatiques plus efficaces pour divers types d'utilisateurs.

## 6. Références

Andriotis, P., Tryfonas, T., et Oikonomou, G. (2014). Complexity metrics and user strength per-ceptions of the pattern-lock graphical authentication method. In *International Conference onvHuman Aspects of Information Security, Privacy, and Trust* (pp. 115–126). Cham, Germany:Springer.

Arend, I., Shabtai, A., Idan, T., Keinan, R., et Bereby-Meyer, Y. (2020). Passive-and Not Active-Risk Tendencies Predict Cyber Security Behavior. *Computers et Security*, 101-129.

Ben-Asher, N., et Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 48, 51–61.

Brière, M., Le Roy, J., et Meier, O. (2020). Linking servant leadership to positive deviant behavior: The mediating role of self-determination theory. *Journal of Applied Social Psychology*.

Caputo, D., Maloof, M., et Stephens, G. (2009). Detecting insider theft of trade secrets. *IEEE Security et Privacy*, *7*(6), 14-21.

Caulkins, B. (2018). Lecture title Modeling and Simulation of Behavioral Cybersecurity, Retrieved on December 26, 2018 *Cybersecurity: A Multidisciplinary Approach*

Coovert, M. D., Dreibelbis, R., et Borum, R. (2016). Factors influencing the human-technology interface for effective cybersecurity performance. In S.J. Zaccaro, R.S. Dalal,L.E.Tetrick, et J.A.Steinke, (Eds.), *Psychosocial dynamics of cyber security* (pp. 267–290). New York, NY:Routledge.

Das, S., Kramer, A. D., Dabbish, L. A., et Hong, J. I. (2014). Increasing security sensitivity with social proof: A large-scale experimental confirmation. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security* (pp. 739-749).

Dolan P., Hallsworth, M., Halpern, D., King,D., Vlaev, I. (2010). Mindspace influencing behaviour through public policy, Institute for Government, Cabinet Office.

Eklund, M., et Backstrom, M. (2006).The role of perceived control for the perception of health by patients with persistent mental illness. *Scandinavian Journal of Occupational Therapy*, 13, 249-256.

Ferreira A, Coventry L, Lenzini G (2015) Principles of Persuasion in Social Engineering and Their Use in Phishing. Springer International Publishing.

Fyffe, G. (2008). Addressing the insider threat. *Network security*, (3), 11-14.

Goleman, D. (1997). Emotional intelligence, why it can matter more than IQ. New Statesman, (126), 31-31.

Jose, I., LaPort, K., et Trippe, D. M. (2016). Requisite attributes for cyber security personnel and teams: Cyber risk mitigation throught alent management . In S.J.Zaccaro, R.S.Dalal, L.E.Tetrick, et J. A. Steinke (Eds.),*Psychosocial dynamics of cyber security* (pp. 167–193). New York, NY:Routledge.

Kaspersky Security Bulletin 2018: Overall Statistics for 2018, Kaspersky Lab (2019).

Karwowski, W., et Ahram, T. (2019). Intelligent human systems integration In *Proceedings of the 2nd International Conference on Intelligent Human Systems Integration: Integrating People and Intelligent Systems*.

Lahcen RAM, Mohapatra R, Kumar M (2018) Cybersecurity: A survey ofvulnerability analysis and attack graphs. In: International Conference on Mathematics and Computing. Springer. pp 97–111.

Le Roy, J., Bastounis, M. & Minibas-Poussard, J. (2012). The Mediating Role of Negative Emotions on the Relationship between Interactional Justice Counterproductive Work Behaviors. *Social Behavior and Personality: an International Review. 40 (8), 1341-1356.*

Le Roy, J., Finkelstein, R., & Rubens, L. (2012). Comment étudier les comportements hostiles au travail? Conceptualisation et application dans un contexte français. *Les cahiers internationaux de psychologie sociale*, (3), 393-416.

Liu, X., Shahidehpour, M., Li, Z., Liu, X., Cao, Y., & Li, Z. (2016). Power system risk assessment in cyber attacks considering the role of protection systems. *IEEE Transactions on Smart Grid*, *8*(2), 572-580.

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., et Kumar, M. (2020). *Review and insight on the behavioral aspects of cybersecurity*. *Cybersecurity*, (*3)*, 1-18.

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology*.

Magklaras, G. B., et Furnell, S. M. (2001). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers et Security*, *21*(1), 62-73.

Maloof, M. A., et Stephens, G. D. (2007). Elicit: A system for detecting insiders who violate need-to-know. In *International Workshop on Recent Advances in Intrusion Detection* (pp. 146-166). Springer, Berlin, Heidelberg.

Marotti, A. (2020). Zoom video meetings are being interrupted by hackers spewing hate speech and showing porn. It's called 'Zoombombing.' Here's how to prevent it. *Chicago Tribune*, 2 avril 2020 (consulté le 11 avril 2020).

More, J. (2011). Measuring Psychological Variables of Control, In Information Security.

Myers, J., Grimaila, M. R., et Mills, R. F. (2009, April). Towards insider threat detection using web server logs. In *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies* (pp. 1-4).

Norman, K. L. (2008).Cyberpsychology: An introduction to human-computer interaction (Vol. 1). NewYork, NY: Cambridge University Press.

Nurse, J.R.C., Creese, S., Goldsmith, M., Lamberts, K. (2010). Guidelines for usable cybersecurity: Past and present. *The 5th International Conference on Network and System Security (NSS 2011),* Milan, Italy, 6-8 September.

Pal, S.K., et Anand S. (2018) InfoSec : A Comprehensive Study. *IUP J Comput Sci XII*:45–65.

Partners, C.R. (2015). Insider Threat Spotlight. *Report. Tech. rep. Crowd Research Partners*

Paul, C. L., et Whitley, K. (2013). A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness. *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 145-154).

Payne, B.K., Hadzhidimova L (2018) Cyber security and criminal justice programs in the United States: Exploring the intersections. *International Journal of Criminology Justice* 13(2):385–404

Pogue, C. (2018) Decoding the minds of hackers. https://www.nuix.com/black-report/black-report-2018

Pfleeger, C.P. (2008). Reflections on the insider threat. In *Insider attack and cyber security* (pp. 5-16). Springer, Boston, MA.

Pfleeger, S.L., et Caputo D.D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computer Security* 31(4):597–611

Randazzo, M., Keeney, M., Kowalski, E., Cappelli, D., et Moore,A. (2004) Insider threat study: Illicit cyber activity in thebanking and finance sector, *US Secret Service and CERT Co-ordination Center/Software Engineering Institute: Philadelphia*, p. 25

Rodriguez, M.A, Bell J, Brown M, Carter D (2017) Integrating Behavioral Sciencewith Human Factors to Address Process Safety. *Journal of Organizational Behavior Management* 37:301–315

Sasse, M. A., Smith, M., Herley, C., Lipford, H., et Vaniea, K. (2016). Debunking security-usability tradeoff myths. *Security et Privacy,* 14(5), 33–39

Shetty, S.S, Shetty RR, Shetty TG, D'Souza DJ (2018) Survey of hacking techniques and it's prevention. *International Conference Power Control Signals Instrument* (ICPCSI). 1940–1945.

Sinclair, S., et Smith, S.W. (2008). Preventative directions for insiderthreat mitigation via access control. *Insider Attack and CyberSecurity*. 165–194

Smith, M.S., Petty, E.R. (1996). Message Framing and Persuasion : A Message Processing Analysis*. Pers Soc Psychol Bull* 22(3) 257-268.

Theoharidou M, Kokolakis S, Karyda M, Kiountouzis E (2005) The insider threatto information systems and the effectiveness of iso17799. *Computer Security.* 24 (6): 472–484

Trim, P., & Upton, D. (2016). *Cyber security culture: Counteracting cyber threats through organizational learning and training*. Routledge.

Uebelacker, S., et Quiel, S. (2014, July). The social engineering personality framework. In *2014 Workshop on Socio-Technical Aspects in Security and Trust* (pp. 24-30). IEEE..

Waite, A. (2010) Info Sec Triads : Security / Functionality / Ease-of-Use, 12 juin 2010.

Wallston, K.A. (2001). Control beliefs. In Smelser N.J., et Baltes. P.B*., International encyclopedia of the social and behavioral sciences*. Oxford, UK: Elsevier Science.

Whitty, M., Doodson, J., Creese, S., et Hodges, D. (2015). Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, *18* (1), 3-7.

Wiederhold, B.K. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, and Social Networking*,17(3), 131–132.

Wolfe, S. E., & Lawson, S. G. (2020). The organizational justice effect among criminal justice employees: A meta-analysis. *Criminology*.