CRPC | Chaire de recherche en prévention de la cybercriminalité

Notes *de synthèse*

Vol. 4, Num. 4
2024

Les sources menant à la fatigue de sécurité chez les employés

Laura Desjardins, étudiante à la maîtrise en criminologie

Introduction

La cybersécurité est désormais un enjeu majeur de notre société, notamment au sein des petites et des grandes entreprises. L'utilisation de la technologie est devenue omniprésente, ce qui provoque une diversification de méthodes criminelles et l'émergence de nouveaux stratagèmes délinquants. Les entreprises se voient donc obligées de mettre en place davantage de mesures et de politiques de sécurité à des fins de protection et de neutralisation des cybermenaces. Néanmoins, **la complexité de la cybersécurité et de ses modalités d'application peut mener à une fatigue en matière de sécurité auprès des employés**. **Ce phénomène survient lorsque les utilisateurs des systèmes et le personnel des organisations se lassent d'investir temps et concentration en ce qui a trait à la sécurité, ou de rencontrer des messages et des avertissements en relation avec celle-ci** [1]. À ce moment, advient le franchissement d'un seuil où les individus deviennent découragés et désensibilisés [1]. De cette façon, cette lassitude amène le personnel à prendre des risques accrus en matière de sécurité et à adopter des comportements non conformes [2]. Ainsi, il est primordial de s'attarder aux sources de fatigue de sécurité, dans le but de mettre en place des dispositions adéquates et des programmes novateurs qui limitent autant que possible cette lassitude.

Une bonne compréhension et considération des facteurs à l'origine de la fatigue des usagers face aux programmes de sécurité améliorera grandement l'efficacité de ceux-ci.

Les sources cognitives

La charge cognitive excessive

Premièrement, les sources de fatigue de sécurité sont majoritairement d'ordre cognitif [3]. **La fatigue de type cognitif réfère à la capacité limitée dont les individus disposent quant aux prises de décisions dans un contexte de charge cognitive accrue** [4, 5]. Une charge cognitive excessive peut se caractériser par l'effort quotidien de **mémorisation des mots de passe** qui doivent être modifiés fréquemment, par la **mémorisation des étapes d'un processus de sécurité compliqué**, par des **politiques de sécurité** qui obligent les employés à modifier leur routine, par des **décisions de sécurité fréquentes**, par une **surcharge d'informations**, ainsi que par la **complexité et l'incertitude des politiques** [3, 4, 6]. Dans le même ordre d'idées, **la fatigue reliée aux mots de passe serait un type de lassitude cognitive assez répandu chez les individus**, caractérisés par une fatigue induite par la mémorisation constante de plusieurs mots de passe [2].

Par ailleurs, il existe aussi **les concepts de fatigue d'alarme et d'alerte**. La première fait référence à **la fatigue quant à l'attention que les individus doivent porter à l'analyse des alarmes résultant de faux positifs**. La seconde est **un épuisement mental découlant de la méfiance générée par un flot régulier d'alertes** [2]. En effet, les employés sont lassés de devoir être constamment en état d'alerte face aux risques de sécurité et en ont assez de tenter de comprendre les origines et les conséquences de ces risques [8]. Cela engendre un sentiment de résignation et une perte de contrôle chez les individus [8].

La quantité d'informations

La quantité de communications et d'activités liées aux politiques de sécurité représente également une source importante de fatigue [8]. De ce fait, les rappels d'exigences en matière de politique de sécurité deviennent excessifs et difficiles à traiter lorsque les employés atteignent leur capacité maximale de traitement de ces rappels [8]. Effectivement, **la surcharge d'informations engendre des conséquences négatives telles que le manque de perspective des individus, de la tension et du stress cognitif, une moindre satisfaction au travail et une paralysie d'analyse** [8]. Cette paralysie se manifeste par une incapacité de l'individu à utiliser les informations qui lui ont été transmises pour prendre des décisions [8]. **Il est possible de relier cette paralysie à la fatigue de type décisionnelle, caractérisée par un état de dépassement des capacités cognitives rendant les décisions de sécurité plus difficiles à prendre** lorsqu'il est question de manipulations de systèmes d'informations et de systèmes informatiques [2, 8]. Ainsi, face à cette fatigue, les employés se dirigeront vers des prises de décisions impulsives, intuitives et biaisées, ou s'abstiendront simplement de prendre des décisions délicates. Également, cette lassitude peut être liée aux conseils de sensibilisation. Dans cette perspective, l'accumulation excessive de conseils entraine une fatigue chez les employés [4, 9].

Par exemple, à long terme, un individu peut être fatigué de recevoir des informations fréquentes sur les politiques et les procédures à suivre, à un point tel qu'il éprouvera un blocage, voire un rejet, à la seule mention d'activités liées à la cybersécurité [4].

La minimisation des enjeux de cybersécurité

La minimisation par les employés du danger et de l'impact des cybercrimes peut favoriser la fatigue de sécurité chez ceux-ci. Effectivement, les individus ont souvent le sentiment qu'ils ne sont pas personnellement en danger puisqu'ils ne sont pas assez importants ou haut placés dans l'entreprise pour que leurs informations soient volées [7]. De plus, certains employés considèrent que peu importe les efforts mis, cela ne suffira jamais pour offrir une protection efficace [7]. **Cette perception négative des programmes de sécurité résulte en partie du fait que les individus ont de la difficulté à se représenter de manière concrète les avantages qu'ils procurent** [7]. Ainsi, les employés considèrent bien souvent les politiques de sécurité comme injustes, déraisonnables et inutiles [7]. Par conséquent, la combinaison de ces attitudes de défiance peut à un moment ou à un autre constituer un terrain favorable à des violations routinières des politiques de sécurité.

Les sources comportementales

La charge physique excessive

Les sources de la fatigue de sécurité peuvent aussi relever du domaine comportemental. **Ce type de fatigue découle de l'accumulation de tâches ou de comportements qui représentent une charge physique élevée et/ou exigent une préparation excessive** [3]. Par exemple, les employés peuvent être lassés de modifier constamment leurs mots de passe, d'être dans l'obligation d'analyser la légitimité de chaque courriel de manière approfondie, d'être quotidiennement obligés de se rappeler d'avoir en leur possession leur carte d'identification ou un jeton d'authentification multifacteur, ou de constamment avoir l'obligation de verrouiller leur

ordinateur [3, 4, 10]. Ainsi, cette fatigue liée à l'action, appelée **fatigue d'authentification**, provient des comportements répétitifs nécessaires au maintien de la sécurité [4, 11]. À cet effet, **la fatigue de sécurité proviendrait des mesures de sécurité qui doivent être appliquées quotidiennement à répétition** [12]. De plus, on recense **trois facteurs comportementaux qui contribuent et modulent la fatigue de sécurité**, soit **l'effort exigé de la part de l'utilisateur pour se conformer aux normes**, **la difficulté d'application des politiques**, et enfin **l'importance que l'individu accorde au besoin de sécurité** [1].

La distraction au travail

La distraction au travail est une autre source importante de fatigue. Effectivement, l**es exigences des politiques de sécurité frustreraient les employés en raison de l'inefficacité et des freins à la productivité qu'elles engendrent** [8, 10, 11]. De plus, les pressions au travail ainsi que les tâches urgentes viennent rendre les exigences de sécurité plus lourdes, ces dernières étant perçues comme des distractions chronophages [3]. Un autre facteur déclencheur de fatigue découle de **procédures qui peuvent provoquer un blocage dans les tâches que les employés cherchent à accomplir, qui entrainent des opportunités manquées et qui entrent ainsi en conflit avec les attentes du poste qu'ils occupent** [3, 6, 11]. Il s'agit par exemple de cas où les employés sont dans l'obligation d'attendre le soutien informatique d'experts en cybersécurité pour résoudre un incident avant de pouvoir reprendre le travail, ou doivent décliner de nouvelles opportunités commerciales lorsque la mise en place d'un accès informatique sécurisé semble trop compliquée [3]. Dans de telles circonstances, les individus ressentiront **un sentiment d'épuisement et un désengagement moral** caractérisés par une tendance à ne plus se préoccuper de ce qui est souhaitable ou indésirable comme comportement concernant la cybersécurité [4].

Formations et politiques de sécurité

Finalement, **les modalités de formation et des politiques de cybersécurité doivent être prises en compte comme facteurs potentiels contribuant à la fatigue de sécurité**. En effet, la longueur, le style, le format, le support et la clarté des communications et activités peuvent constituer un facteur significatif de fatigue [8, 13]. Plusieurs aspects des programmes de formation et de sensibilisation peuvent expliquer la lassitude de certains individus à l'égard de la sécurité [13]. À cet effet, l'absence d'incitatifs ou de récompenses à la suite d'une formation réduit l'enthousiasme et la motivation des employés à suivre de futurs programmes [13]. Également, des formations trop génériques et peu spécifiques au secteur d'activité de leur organisation et du poste occupé diminuent l'engagement des employés [13]. De la même façon, la mise à jour fréquente des formations afin de bien représenter les dernières menaces de cybersécurité et d'intégrer les commentaires réguliers des employés concernant la pertinence des formations est primordiale [6, 13]. **La perception des employés quant à l'efficacité des formations joue également un rôle central dans la fatigue de sécurité de ceux-ci**. En effet, une formation inefficace en matière de cybersécurité contribue à la frustration et à l'épuisement des employés, diminuant l'adhésion aux formations – **un phénomène aussi connu sous le nom de « fatigue de l'entrainement »** [2]. Dans le même ordre d'idées, le manque de motivation des employés peut se manifester lorsqu'ils ont l'impression que la haute direction ne se soucie pas réellement de la sécurité, et qu'elle met plutôt en œuvre des programmes de formation dans le but de répondre aux exigences de conformité [14].

Ainsi, on retrouve **cinq facteurs liés aux formations et politiques, contribuant à la fatigue en matière de cybersécurité** [14]. Le premier facteur est lié à une perception selon laquelle **les formations en cybersécurité manquent de soin, d'efforts et d'attention aux détails** [14]. Le deuxième facteur est celui de la

réaction émotionnelle des employés face aux formations, qu'ils trouvent ennuyeuses [14]. En ce qui concerne le troisième facteur, il découle de l'**inadaptation du contenu et du style des formations** [2, 13]. Le quatrième facteur est lié au **sentiment d'inutilité perçue de la formation pour l'employé**, tandis que le dernier et cinquième facteur réfère à la mesure dans laquelle **le participant estime que la formation ne lui est pas destinée et qu'elle serait plus bénéfique aux autres qu'à lui-même** [13]. En résumé, l'étendue, la forme, le style, la pertinence, l'efficacité, l'utilité, la spécificité et la perception des employés face aux des formations peuvent être des sources de fatigue en matière de cybersécurité.

Conclusion

La littérature scientifique a identifié plusieurs causes pouvant contribuer à la fatigue de sécurité chez les employés. **Ces facteurs contributifs peuvent prendre la forme de conseils excessifs, d'une charge cognitive élevée associée aux mesures de cybersécurité, l'obligation constante d'être en alerte, une grande quantité de communications et d'activités liées aux politiques de sécurité, une minimisation du danger, une préparation et une charge comportementale élevée, ainsi que par le sentiment de distraction des fonctions principales que suscitent les programmes de sécurité**. Toutes ces sources de fatigue provoquent chez certains employés des sentiments de colère, d'abandon et de perte de contrôle qui vont mener à des prises de décision impulsives, intuitives et biaisées menant à des comportements non sécuritaires. **Il est donc primordial de considérer ces sources de fatigue dans l'élaboration des formations et des politiques de cybersécurité**. À cet effet, il est important de **démontrer et expliquer l'utilité et les retombées des formations et politiques afin de favoriser l'adhésion des employés, d'émettre des politiques simples et claires, de limiter la quantité de conseils et d'informations dispensés aux employés, ainsi que d'implanter des politiques et des programmes de formations adaptés à l'évolution des risques et spécifiques aux postes et aux rôles des employés**. Il est enfin important de souligner qu'aucune des sources de lassitude présentées dans cette note ne considère les facteurs individuels et personnels propres à chaque employé, qui peuvent prédisposer certains individus à cette fatigue de sécurité et sont difficiles à altérer une fois la personne en poste.

Références

[1] Furnell, S. et Thomson, K-L. (2009). Recognising and addressing « security fatigue ». *Computer Fraud & Security*, (11), 7-11.

[2] Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA–Journal of Business and Public Administration*, *13*(1), 49-72.

[3] Parkin, S., Krol, K., Becker, I., et Sasse, M. A. (2016). Applying cognitive control modes to identify Security fatigue hotspots. *Twelfth Symposium on Usable Privacy and Security*.

[4] Reeves, A., Delfabbro, P. et Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE open*, *11*(1).

[5] Dykstra, J. et Paul, C. L. (2018). Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations. *11th USENIX Workshop on Cyber Security Experimentation and Test* (CSET 18).

[6] Bhana, A. et Ophoff, J. (2022). Security fatigue: a case study of data specialists. In *International Symposium on Human Aspects of Information Security and Assurance*, 275-284.

[7] Stanton, B., Theofanos, M., Prettyman, S., et Furman, S. (2016). Security fatigue. *It Professional*, *18*(5), 26-32.

[8] Cram, W., Proudfoot, J., et D'Arcy, J. (2021). When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal*, *31*(4), 521-549.

[9] Serfontein, R., Drevin, L. et Kruger, H. (2018). The feasibility of raising information security awareness in an academic environment using SNA. *IFIP World Conference on Information Security Education*, 69-80.

[10] Coopamootoo, K. P., Gross, T. et Pratama, M. F. R. (2017). An Empirical Investigation of Security Fatigue: The Case of Password Choice after Solving a CAPTCHA.

The LASER Workshop: Learning from Authoritative Security Experiment Results, 39-48.

[11] Sasse, M. (2013). Technology Should Be Smarter Than This! A Vision for Overcoming the Great Authentication Fatigue. *Workshop on Secure Data Management*, Cham: Springer International Publishing, 33-36.

[12] Tanimoto, S., Hatashima, T., Nagai, K., Hata, K., Sakamoto, Y. et Kanai, A. (2017). A concept proposal on modeling of security fatigue level. 2*017 5th Intl Conf on Applied Computing and Information Technology/4th Intl Conf on Computational Science/Intelligence and Applied Informatics/2d Intl Conf on Big Data, Cloud Computing, Data Science*, 29-34.

[13] He, W. et Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249-257.

[14] Reeves, A., Calic, D. et Delfabbro, P. (2023). Generic and unusable : Understanding employee perceptions of cybersecurity training and measuring advice fatigue. *Computers & Security*, *128*, 103-137.