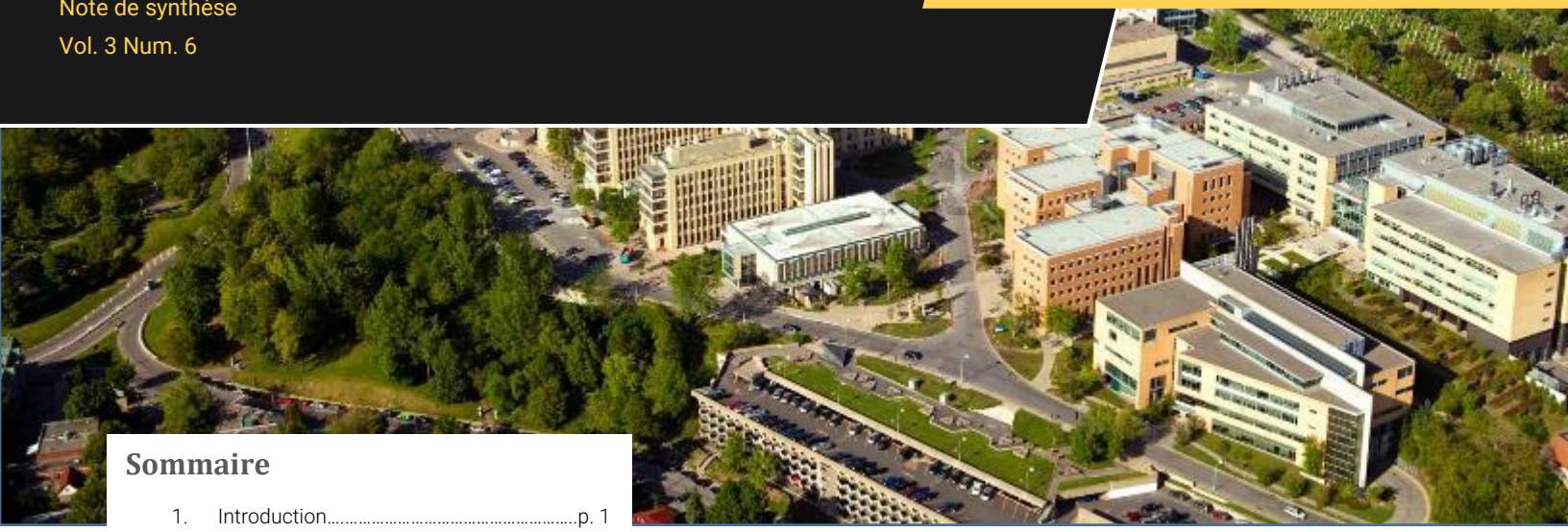
Définir le comportement sécuritaire

Layla Jasic, étudiante au doctorat en criminologie

Note de synthèse
Vol. 3 Num. 6

CRPC | Chaire de recherche en prévention de la cybercriminalité



Sommaire

Jasic, L. (2021). Le comportement sécuritaire pour la protection de l'actif informationnel : mieux comprendre et définir le concept. (Mémoire de maîtrise, HEC). Disponible à https://biblos.hec.ca/biblio/memoires/jasic_layla_m2021.pdf

La Chaire de recherche en prévention de la cybercriminalité a été créée à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada. Dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée de l'Université de Montréal, elle a pour mission de contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention.

Introduction

À mesure que les technologies de l'information (TI) deviennent de plus en plus sophistiquées, les méthodes utilisées pour perpétrer des cyberattaques le deviennent tout autant, augmentant les risques pour la sécurité de l'information[1]. Les employés, par le biais des appareils qu'ils utilisent, constituent la principale voie d'accès pour les incidents de sécurité en permettant notamment à des types d'attaques comme l'hameçonnage, les rançongiciels et les logiciels malveillants de se propager[2].

Même si 39% des entreprises canadiennes perçoivent les employés négligents ou malhabiles comme leur principale vulnérabilité en matière de sécurité de l'information[3], les organisations s'en remettent encore beaucoup aux solutions technologiques pour gérer cette dernière, et ce, malgré le fait que l'erreur humaine constitue l'une des sources les plus importantes d'incidents de cybersécurité[4]. En effet, les incidents dont la cause est interne à l'organisation sont plus fréquents que ceux provenant de l'externe, ce qui met l'accent sur le rôle du comportement des employés et sur l'importance de s'attarder à la dimension humaine de la cybersécurité pour prévenir ces derniers[5].

Le comportement sécuritaire

Pour mitiger les risques associés aux erreurs humaines, les études en cybersécurité évoquent souvent l'idée d'un comportement sécuritaire des employés, sans que l'on sache précisément ce qu'il en ressort. Ce concept est couramment mentionné dans les études scientifiques comme dans les rapports professionnels, mais il se présente sous différents noms, avec différentes descriptions ou encore avec des disparités notables dans les moyens pour le mesurer. Le comportement sécuritaire est donc un concept qui semble bien ancré dans la littérature, mais qui est ambigu en raison de l'absence d'une définition claire et partagée.

Plusieurs raisons justifient l'importance de définir clairement ce qu'est un comportement sécuritaire. Par exemple, la sensibilisation à la sécurité de l'information en conjonction avec l'éducation et la formation a été identifiée comme un moyen efficace pour réduire les risques de sécurité liés aux facteurs humains[6]. Toutefois, pour élaborer un programme de sensibilisation efficace, c'est-à-dire qui aura un impact positif sur le comportement des employés, il est important de comprendre ce qui influence le comportement des employés[7] et par conséquent, il faut définir ce qui est entendu par « comportement ». Outre la création de ces programmes, il est également important de les évaluer pour déterminer si les objectifs en matière de sécurité ont été communiqués adéquatement, et, éventuellement, y apporter des changements[6]. Un rapport révèle, par ailleurs, que peu de gestionnaires en sécurité parviennent à décrire ou documenter des objectifs mesurables pour leurs programmes de sensibilisation, ce qui implique la difficulté de déterminer si ces programmes sont un succès ou non et si les effets escomptés, à savoir un meilleur comportement sécuritaire, est produit[8]. L'évaluation est un élément important pour les organisations, qui doit leur permettre d'avoir un portrait de leur posture en matière de cybersécurité. Cependant, puisque ces programmes visent avant tout le changement des comportements des employés et que le comportement sécuritaire est un concept flou, il y a lieu de se demander comment les programmes peuvent être évalués de manière fiable.

Il convient alors de proposer une définition conceptuelle du comportement sécuritaire pour la protection de l'actif informationnel, c'est-à-dire une description aussi précise que possible de ce qu'est un comportement sécuritaire, les caractéristiques qu'il possède et les dimensions qui le composent.

Une revue de littérature systématique s'appuyant sur 83 articles issus de la littérature académique et de la littérature professionnelle a été menée afin de proposer une définition. Le choix d'avoir recours à ces deux types de littérature s'explique par le fait que le sujet de cette étude est plutôt récent. Encore peu d'études empiriques ont été produites et le flou autour de la définition du comportement sécuritaire est un enjeu commun aux deux types de littérature.

Analyse des définitions et des actions reliées au comportement sécuritaire

Une analyse plus approfondie des définitions du comportement sécuritaire a permis d'identifier trois thèmes principaux s'y rattachant : 1) la protection des systèmes ou des actifs informationnels[9, 10]; 2) le suivi des politiques et des recommandations de l'organisation[11], et 3) l'évaluation d'une situation, des conséquences de ses actions, l'adaptation à une nouvelle situation ou la prise d'initiatives pour favoriser la sécurité[7, 11].

On retrouve également le thème du comportement non sécuritaire dans certaines définitions[12], mais il n'a pas été retenu puisque la définition d'un concept doit reposer sur ce qu'il est et non ce qu'il n'est pas[13]. Par ailleurs, quelques définitions renvoyaient à l'idée d'intention d'un comportement sécuritaire[14], mais ce thème n'a pas été retenu non plus, car le but des pratiques de cybersécurité n'est pas de développer des intentions positives à l'égard de la sécurité de l'information chez les employés, mais bien de voir des changements réels s'opérer dans leur comportement[15]. En effet, le comportement sécuritaire des employés ne devrait ni être défini, ni mesuré sur la base d'intentions, car ces dernières ne sont pas toujours suivies du comportement désiré[16] et dans les pratiques de prévention en cybersécurité, ce sont

avant tout les actions concrètement posées et non les intentions qui comptent[17].

De plus, plusieurs études ne donnaient pas de définition, mais proposaient des actions reliées au comportement sécuritaire. L'analyse des actions rapportées dans ces études montre que le comportement sécuritaire devrait être défini et mesuré sur la base d'actions observables. Ces dernières peuvent être facilement observables (p.ex. suivre une formation, rapporter des incidents de sécurité, verrouiller son ordinateur) ou un peu moins faciles à observer au quotidien (p.ex. faire preuve de prudence avec les courriels, effectuer des copies de sauvegarde régulièrement, utiliser des technologies de protection comme les antivirus). Ces caractéristiques sont importantes, car si les organisations veulent évaluer l'efficacité de leurs programmes de sensibilisation à la cybersécurité sur le comportement des employés, il est important qu'elles aient des proxys objectifs et mesurables (comme les actions observables) pour ce faire. En effet, des actions mal définies ou qui ne peuvent être observées, comme le simple fait de suivre les politiques, ne permettraient pas une évaluation efficace.

Dimensions

Plusieurs dimensions ou aspects au comportement sécuritaire ont été mis en lumière par la littérature, démontrant que le comportement sécuritaire est bel et bien un concept multidimensionnel, c'est-à-dire qu'il contient plus d'une facette distincte qui le caractérise. Ainsi, les aspects de la conformité, de l'éthique et du jugement, sont des dimensions constituant des éléments clés pour la compréhension du concept de comportement sécuritaire.

Conformité

La conformité est couramment associée au concept de comportement sécuritaire et est parfois décrite comme étant la principale dimension de celui-ci[18, 19]. Un comportement de conformité consisterait à suivre les règles et principes inscrits dans les politiques organisationnelles. En effet, ces dernières sont fréquemment utilisées par les organisations dans le but de former ou d'influencer le comportement de leurs employés à l'égard de la sécurité de l'information[20]. Par ailleurs, 20 des études analysées ont avancé l'idée qu'il existerait des relations entre les trois dimensions du comportement sécuritaire et la conformité pourrait constituer le fondement sur le lequel un employé peut développer l'éthique et le jugement[21, 22].

Éthique

L'éthique est un ensemble de principes permettant d'identifier ce qui est bien ou mal en termes de comportements liés à la sécurité de l'information. Le comportement des employés ne peut plus être déterminé seulement par le respect des règles établies, comme celles présentes dans les politiques organisationnelles[22] : les employés doivent être sensibilisés aux conséquences possibles de leurs actions et comprendre pourquoi certains comportements sont adéquats et d'autres non. Ainsi, plus l'employé prend conscience des impacts possibles d'une action, plus il a de chances d'entreprendre des gestes pour assurer la sécurité de l'information.

Jugement

Le jugement fait référence à un type de comportement qui va au-delà de la conformité et même de l'éthique. Ce concept fait référence à l'idée que les utilisateurs réfléchissent aux conséquences en termes de cybersécurité avant de poser une action, développent des réflexes pour mieux protéger l'information et acquièrent une capacité à évaluer les situations avant d'agir ou encore s'adapter à de nouvelles situations dans un contexte de prévention des incidents. Compte tenu du dynamisme et de l'évolution continue du domaine de la cybersécurité, les individus ont besoin de mises à jour fréquentes et d'une grande capacité d'adaptation[22]. À cet effet, les employés doivent donc faire preuve de jugement, puisque le fait de se conformer à des politiques ou de suivre des principes éthiques ne peut pas constituer une solution à chaque nouvelle situation rencontrée. Par ailleurs, un comportement relevant du jugement des utilisateurs consisterait aussi à choisir les actions en lien avec la sécurité qui semblent appropriées, sans nécessiter d'autres directives spécifiques[17].

Un point commun ressort par ailleurs entre les dimensions identifiées, soit le fait qu'elles relèvent toutes d'un **degré d'initiative différent de la part de l'individu**. La conformité nécessite le moins d'initiative, puisqu'elle consiste essentiellement à suivre les politiques. L'éthique en requiert un degré un peu plus élevé, car elle nécessite que l'individu évalue lui-même si ses actions constituent le « bien » dans une situation donnée pour assurer la protection de l'actif informationnel. Enfin, le jugement est la dimension qui relève du plus haut degré d'initiative, car elle nécessite que l'individu évalue une situation, qui est parfois nouvelle, et en se basant sur cette évaluation, détermine les actions à poser.

Définitions

L'analyse des différents éléments mentionnés ci-dessus a permis de proposer une définition plus uniforme du concept. Cette section présente donc dans un premier temps une définition « de dictionnaire » du comportement sécuritaire, puis une synthèse des dimensions identifiées pour ce concept.

Comportement sécuritaire pour la protection de l'actif informationnel : ensemble d'actions objectivement observables qu'adopte un individu afin de prévenir des incidents de sécurité et, ultimement, de protéger l'actif informationnel.

Actions objectivement observables: les actions doivent relever de différents degrés d'initiative de la part de l'individu, correspondant aux différentes dimensions du comportement. Seules des actions objectives et perceptibles par autrui constituent un comportement. Les actions non observables ne s'inscrivent pas dans un comportement (il s'agirait plutôt d'attitudes ou de croyances, par exemple).

Dimensions du comportement sécuritaire

- **Conformité :** le fait d'appliquer les règles et les principes inscrits dans la politique organisationnelle;
- **Éthique** : ensemble de critères permettant de distinguer ce qui est bien de ce qui est mal, de manière à pouvoir en assumer les conséquences;
- **Jugement :** les réflexes individuels de protection découlant de l'évaluation d'une situation et le fait d'agir ou prendre des décisions en ayant conscience des conséquences possibles de ses gestes.

Conclusion et recommandations

Le comportement sécuritaire des employés est un élément fondamental pour prévenir les cyberattaques et assurer la protection de l'actif informationnel des organisations. La littérature académique, tout comme la littérature professionnelle, témoignent de l'importance de ce concept, répandu, mais flou. Cette étude propose un premier pas vers une définition claire et uniforme, et il est donc possible de formuler deux recommandations clés pour servir de point de départ aux professionnels dans l'élaboration de leurs programmes de formation en cybersécurité :

- Définir clairement ce qu'on entend par « comportement sécuritaire », par exemple en utilisant la définition proposée ici, pour établir des objectifs clairs en matière de cybersécurité pour les employés.
    - Il est important de se rappeler que le comportement doit être défini et évalué par des gestes réels et non par des croyances ou des intentions et qu'il doit être perceptible à travers des actions objectivement observables.
- Ensuite, définir les indicateurs de performance pertinents et les politiques en matière de cybersécurité qui permettront aux employés de mieux comprendre ce qui est attendu d'eux en matière de prévention et de protection.

- Puisque la sécurité de l'information et la prévention des cyberattaques relèvent de tous les employés d'une organisation, il est important que chaque individu comprenne les responsabilités qui lui incombent.

Références

[1] Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13-24.

[2] PwC. (s.d.). Workforce Pulse Survey: It's time to adopt a cyber-savvy culture. Retrieved from https://www.pwc.com/us/en/library/covid-19/workforce-pulse-survey.html?WT.mc_id=CT1-PL50-DM2-TR1-LS4-ND40-PR3-CN_Covid19WorkplaceReboot-&eq=CT1-PL50-DM2-CN_Covid19WorkplaceReboot

[3] EY. (2020). Your employees are the weakest link in your cybersecurity chain. Récupéré de https://www.ey.com/en_ca/cybersecurity/your-employees-are-the-weakest-link-in-your-cybersecurity-chain

[4] Sampath, S. (2019). Fight Unsecure Employee Behaviors by Fixing Your Risk Culture. Gartner.

[5] McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. Computers in Human Behavior, 69, 151-156.

[6] Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). Human factors and information security: individual, culture and security environment. Defence Science and Technology Organisation Edinburgh (Australia) Command Control Communications and Intelligence DIV.

[7] Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46, 815-825.

[8] Huisman, J. (2018). Effective Security Awareness Starts With Defined Objectives. Gartner.

[9] Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security, 28(8), 816-826.

[10] Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. Computers & Security, 56, 70-82.

[11] Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness. Information Systems Research, 26(2), 282-300.

[12] Khatib, R., & Barki, H. (2020). An activity theory approach to information security non-compliance. Information and Computer Security, 28(4), 485-501.

[13] MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. MIS Quarterly, 35(2), 293-334.

[14] Williams, C. K., Wynn, D., Madupalli, R., Karahanna, E., & Duncan, B. K. (2014). Explaining Users' Security Behaviors with the Security Belief Model. Journal of Organizational and End User Computing, 26(3), 23-46.

[15] Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Quarterly, 39(4), 837-864.

[16] Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Computers & Security, 49, 177-191.

[17] van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. International Journal of Human-Computer Studies, 123, 29-39.

[18] Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. Decision Support Systems, 92, 25-35.

[19] Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. Decision Support Systems, 92, 36-46.

[20] Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management, 52, 69-79.

[21] Buytendijk, F., Lee, B., & Howard, C. (2020). Digital Ethics: What Every Executive Leader Should Know. Gartner.

[22] Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. Computers & Security, 53, 65-78.

[23] Ruighaver, A. B., Maynard, S. B., & Warren, M. (2010). Ethical decision making: Improving the quality of acceptable use policies. Computers & Security, 29(7), 731-736.