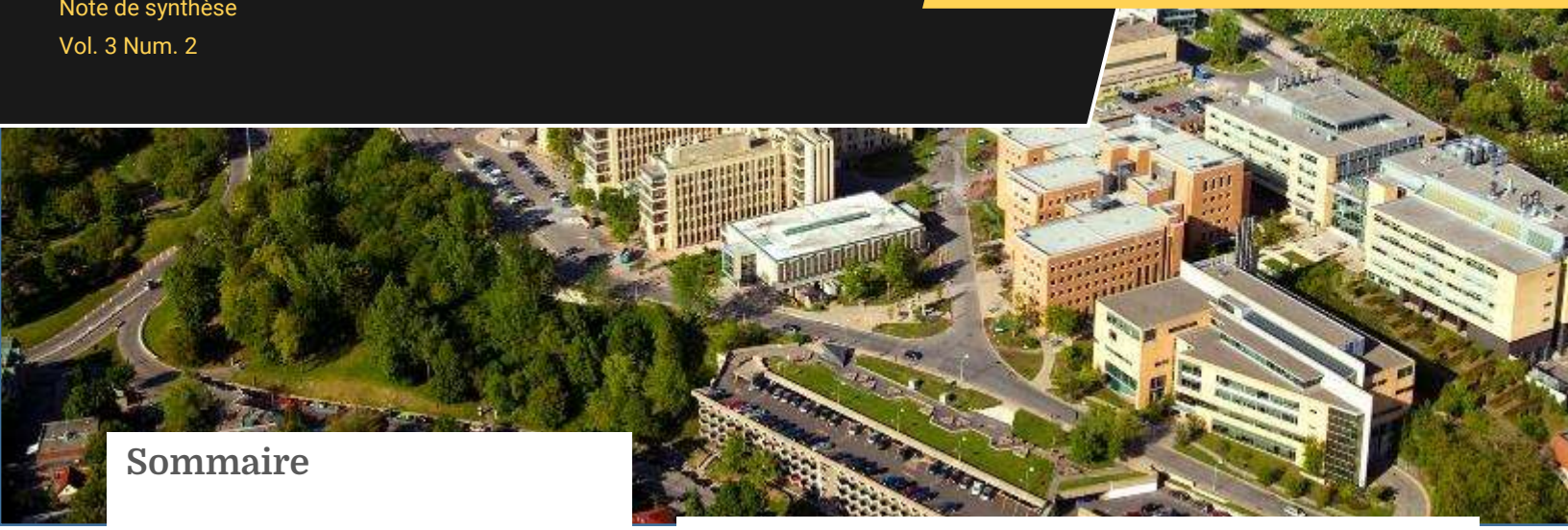
La culture de sécurité et la conformité à l'ère de l'information numérique

Hugo Savard, candidat à la maîtrise

Note de synthèse
Vol. 3 Num. 2

CRPC | Chaire de recherche en prévention de la cybercriminalité



Sommaire

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 l'instar de l'écosystème virtuel dans lequel elle s'opère, la cybersécurité est un secteur complexe qui ne pourrait être dissocié de ses contreparties matérielles, soit d'un environnement physique formé d'innombrables acteurs, interactions et instruments tangibles. **La cybersécurité concerne donc à la fois la sécurité technologique et humaine, expliquant de ce fait pourquoi elle nécessite deux ordres d'interventions distincts**[1]. Il est ainsi nécessaire de s'émanciper d'une vision purement « technique » de la sécurité du cyberespace, car une perceptive technocentriste négligerait une proportion significative des menaces qui pèsent aujourd'hui sur les systèmes informatiques. Les données actuelles démontrent d'ailleurs qu'une proportion considérable des brèches peut être attribuée à des facteurs humains, représentant dans certains cas près du tiers de celles-ci[2, 3]. Ce constat confirme qu'au-delà de sa dimension digitale, la cybersécurité est une problématique qui doit être analysée à travers le prisme des sciences sociales et de la recherche qualitative. En ce sens, toute stratégie de mitigation des cyberrisques qui se voudrait cohérente ou efficace devrait incorporer des éléments tirés de domaines tels que la sociologie, la psychologie et la criminologie. Il est d'autant plus pertinent de transférer la question vers ces domaines lorsque l'on considère la pandémie de COVID-19, puisque ce contexte particulier a conduit les organisations à privilégier le travail à distance.

À cet effet, l'adoption expéditive et généralisée d'outils de travail à domicile met à rude épreuve les départements de sécurité des entreprises, qui doivent préserver les mêmes normes de protection sans entraver le travail d'employés situés hors site. Pour les employés, le stress occasionné par la situation sanitaire peut être exacerbé par des facteurs supplémentaires, tels que de nouvelles charges en lien avec la sécurité de l'information ou une absence de supervision qui oblige un plus grand degré de responsabilisation individuelle[4]. Ainsi, tout comme la pandémie de COVID-19, **le travail à distance représente un vecteur anxiogène qui a le pouvoir d'affaiblir le « pare-feu humain » (*human firewall*) d'une organisation et rendre sa force de travail plus encline à des attaques dans lesquelles l'humain occupe un rôle de premier plan** (p. ex. l'ingénierie sociale, l'hameçonnage, le harponnage, etc.). Bien que cette situation exacerbe les défis sécuritaires des entreprises, elle permet en contrepartie de justifier les solutions « non-techniques », car ces dernières ont une influence sur les comportements des employés et dépendent donc moins de leur lieu de travail. La note de synthèse subséquente tentera d'explorer les stratégies centrées sur l'humain qui semblent se démarquer et abordera deux aspects centraux, soit la culture organisationnelle et la conformité aux politiques de sécurité.

La culture de sécurité de l'information

Qu'elle soit explicite ou davantage occulte, la culture d'entreprise est une réalité de chaque organisation, étant constituée d'un amalgame de suppositions, perceptions, normes et valeurs qui orientent les comportements de ses membres et forgent son identité. Cependant, bien qu'elle soit traditionnellement rattachée au domaine des affaires, de nombreux auteurs attestent que la culture professionnelle s'immisce également dans le continuum de la cybersécurité. Effectivement, la notion de « **culture de la sécurité** » en est une récurrente dans la littérature, faisant généralement référence à **l'ensemble des éléments qui déterminent l'état d'esprit et les comportements des membres d'une organisation vis-à-vis la sécurité de leurs systèmes informatiques**[5]. Conséquemment, elle désigne la manière dont les individus perçoivent la cybersécurité et s'additionne des actions qu'ils posent pour assurer la protection des informations digitales[6, 7]. Lorsqu'elle est bien implémentée, la culture est en mesure de placer la sécurité de l'information au sommet des priorités de tous les employés et de favoriser les comportements sécuritaires. Ainsi, selon le concept de « cybersécurité de tous les jours »[1], la protection des données doit être intériorisée par la force de travail, car cela lui permet de surpasser ce qui serait autrement un simple code de conduite. Cette vision est partagée par d'autres chercheurs[8, 9], qui voient eux aussi la normalisation des bonnes pratiques comme une condition *sine qua non* à la sécurité de l'entreprise.

En outre, plusieurs recherches suggèrent qu'une des facettes les plus déterminantes de la culture « positive » est le fait qu'elle s'insinue dans une logique de prophétie autoréalisatrice, car elle encouragerait la reproduction de comportements bénéfiques et permettrait ainsi de continuellement renforcer la sécurité d'une organisation sans qu'aucun acteur n'ait à injecter des ressources supplémentaires[10, 11, 12]. Selon la littérature, **une culture de la sécurité efficace impliquerait idéalement des éléments tels que le respect des politiques de sécurité, le signalement de toute activité suspecte et un engagement à tous les niveaux hiérarchiques**[13]. En revanche, une culture inadéquate ou « négative » serait surtout ponctuée d'un manque de compréhension de la sécurité (vulnérabilités, menaces, protocoles, etc.), d'une indifférence envers les politiques internes et de carences au niveau de la conformité[1, 14, 15]. Ainsi, au-delà des ramifications comportementales, instaurer une culture de la sécurité permet aux employés de saisir l'importance des pratiques de cybersécurité et de comprendre que leur application est profitable tant sur le plan individuel qu'organisationnel[1]. Cette qualité pluridimensionnelle est notamment mise en évidence par d'autres chercheurs, qui soutiennent

que **la culture est façonnée à la fois par des facteurs individuels** (p. ex. perceptions, attitude, habitudes, connaissances) **qu'environnementaux d'une organisation** (p. ex. normes, disponibilité des ressources, interactions), signifiant qu'elle ne peut être analysée ou altérée de manière isolée[16]. Cette dynamique est également observable dans la pratique, étant illustrée par l'étendue des moyens qui sont mis en œuvre par les entreprises pour assurer l'adoption d'une « bonne » culture de cybersécurité. Ces moyens peuvent aller des campagnes de sensibilisation (échelle macro) à l'imposition de sanctions (échelle micro).

Quoique cette complexité nuit à l'atteinte d'un consensus quant à la définition de ce qu'est réellement la culture de sécurité, la majorité des auteurs considèrent tout de même qu'elle est essentielle à la réalisation des stratégies de protection de l'information. En effet, hormis les débats sémantiques qu'elle génère, elle est globalement perçue comme **« l'instrument » le plus efficace pour remédier au facteur humain de la cybersécurité**[9, 11, 14]. Son rapprochement avec la dimension humaine est principalement expliqué par son but recherché, qui n'est ultimement pas celui de rendre le cyberespace plus sûr, mais plutôt d'**outiller les utilisateurs et ainsi donc de renforcer leur engagement et leur capacité à faire face aux menaces**. Ce dernier point est déterminant, car il admet que dans un environnement digital en constante mutation, l'innovation n'est pas une prérogative unique aux acteurs *bona fide* (entreprises, experts en sécurité, etc.). En ce sens, accroître la résilience des membres d'une organisation est une stratégie « non-technique » qui reconnait l'impossibilité d'atteindre une adéquation parfaite entre les compétences défensives des entreprises et celles offensives des entités malveillantes. Ce décalage peut être saisi de manière comparable au concept de « fracture numérique » (*digital divide*) qui renvoie à la répartition inégale des technologies de l'information et de la communication (TIC) dans la société[17]. Cependant, alors que son articulation initiale se rapporte au phénomène d'inégalité d'accès aux outils issus de l'ère digitale, le comprendre en termes d'asymétrie de capacités permet de l'étendre au domaine de la cybersécurité actuel. En effet, le cyberespace peut être compris comme un environnement dans lequel les menaces peuvent rapidement instrumentaliser l'innovation afin de tirer avantage des handicaps structurels des acteurs défensifs (intégration technologique plus lente, mises à jour de vastes systèmes, délais de *patching*, etc.). La culture est donc un mécanisme qui permet aux organisations de consolider leur sécurité sans qu'elles n'aient à constamment surmonter une forme de fossé numérique et concentrer une part trop significative de leurs ressources sur des dispositifs technologiques dont l'efficacité à long terme demeure incertaine[18].

La conformité

De nombreux ouvrages soulignent que même lorsque des politiques de sécurité sont en place au sein d'une organisation, il est possible que des employés ne satisfassent pas à ses exigences[19, 20]. Connue sous l'appellation de « conformité » (*compliance*), elle fait référence « **au fait d'honorer les règles et/ou les normes** », donc au principe d'adhérer aux politiques internes de sécurité[21]. Cette notion est particulièrement prépondérante dans la littérature, car elle est considérée comme **un élément qui a le pouvoir d'invalider tout stratégie de mitigation des risques si elle n'atteint pas un certain seuil minimal**. Cette problématique est généralement attribuée aux habitudes et aux expériences des individus, qui ont toujours le choix d'appliquer ou non les normes de sécurité. Ce libre arbitre explique notamment pourquoi la question est communément analysée par l'entremise de théories psycho-comportementales et criminologiques qui abordent la question du processus décisionnel ainsi que les paramètres le régissent.

Ainsi, **la théorie psychologique de la protection-motivation** (*Protection-motivation Theory; PMT*) proposée par Rogers en 1975 est abondamment reprise dans l'arène de la cybersécurité par de

nombreux auteurs[4, 8, 10, 15, 20, 21, 22, 23]. Outre le fait qu'elle jouisse d'une popularité croissante au sein du milieu académique, celle-ci se distingue par son traitement du concept de « motivation », qu'elle considère comme un état variable et intimement lié à des facteurs situationnels. Puisqu'elle sous-tend que la motivation est un paramètre qui fluctue d'une situation à l'autre, cela suggère que **nous pouvons être motivés à accomplir nos tâches avec la diligence et le soin nécessaires lorsque certaines conditions sont présentes**. Plutôt que de s'ensiler dans des facteurs aussi complexes que les traits de caractère et de personnalité, la PMT évoque des vecteurs d'action tangibles sur lesquels il est possible d'agir, ce qui accroît drastiquement sa portée et la facilité avec laquelle un acteur peut l'opérationnaliser. Ainsi, la théorie de la protection-motivation relaye l'idiosyncrasie au second plan, facilitant dès lors sa généralisation à l'ensemble de la force de travail et l'intervention ciblée des gestionnaires en sécurité de l'information.

Selon la PMT, qui s'intéresse aux processus cognitifs qui régissent le comportement face à la menace, les individus mènent habituellement **deux types de processus d'évaluation, l'un axé sur la menace elle-même** (*threat appraisal*) **et l'autre sur leur capacité à agir contre celle-ci** (*coping appraisal*)[8, 24, 25]. Au cours de l'évaluation de la menace, l'acteur estimerait les conséquences négatives que le risque occasionnerait (*perceived threat severity*; la gravité perçue) et la probabilité qu'il se concrétise (*perceived threat vulnerability*; la vulnérabilité perçue)[24]. Conformément à cet aspect de la théorie, un individu devra croire qu'il existe une menace sérieuse et que cette dernière est susceptible de se produire pour qu'il adopte un comportement sécuritaire. Au cours de l'évaluation de la « capacité d'action », la personne évaluera si le fait d'entreprendre l'action prévue par les normes éliminerait la menace (*response efficacy*; efficacité de la réponse) et son niveau de confiance quant à son aptitude à mener cette action à bien (*self-efficacy*; auto-efficacité)[4, 20]. Relativement à cet élément, les auteurs postulent que l'individu devra reconnaitre qu'il existe des actions qui mitigeraient efficacement la menace et être convaincu que réaliser cette action ne surpasse pas ses capacités personnelles. Certains chercheurs complémentent ce modèle d'un élément rationnel, ajoutant que pour se conformer aux protocoles, la personne doit se croire capable d'adopter le comportement requis sans que cela ne lui « coûte » un montant d'effort trop élevé (calcul coûts-bénéfices)[4, 19].

Toutefois, certains reconnaissent qu'une des faiblesses de la PMT est son usage de « l'intention » comme indicateur principal, car ils défendent que la sécurité dépend avant tout des comportements, donc des actions que les employés prennent lorsqu'ils font face à la menace[10]. À cet effet, quelques études ont donc utilisé les actions concrètes comme variable dépendante et ont été en mesure d'inférer qu'en matière de protection de l'information, la sécurité repose sur le comportement plutôt que sur l'intention.[25, 26]

Conclusion

Cette note de synthèse offre une vision globale de la culture de sécurité et des facteurs de la théorie de la protection-motivation qui influencent le niveau de conformité des individus. Bien que ces deux dimensions puissent sembler indépendantes l'une de l'autre, les éléments relevés dans la littérature permettent au contraire d'observer leur complémentarité et leur renforcement mutuel. En effet, plusieurs aspects soulevés précédemment permettent d'avancer qu'une culture positive de cybersécurité peut être articulée autour des aspects centraux de la PMT pour assurer une protection efficace des systèmes informatiques d'une organisation tout en prenant en compte le facteur humain. Alors que la culture peut placer la sécurité au sommet des priorités d'une entreprise, la PMT permet aux gestionnaires de structurer cette culture de manière à exploiter les processus cognitifs qui déterminent la conformité. Leur conjonction pourrait faire en sorte que les gens soient conscients des risques liés à la

cybersécurité, qu'ils normalisent les comportements sûrs, qu'ils reconnaissent les actions de mitigation efficaces et qu'ils aient confiance en leur capacité à répondre aux menaces. Cette approche mixte permettrait aux entreprises d'évaluer leurs stratégies actuelles et de privilégier les pratiques qui s'immiscent aisément dans les deux dimensions discutées (p. ex. les campagnes de sensibilisation).

Par ailleurs, considérant l'attention qu'elle accorde aux facteurs situationnels, la PMT est un outil flexible qui permet de développer des stratégies cohérentes à n'importe quel contexte, dont celui du télétravail. Cette dernière qualité implique que les variables de la théorie pourraient être rapidement calibrées par les entreprises, leur permettant de prioriser les mesures efficaces et d'ajuster (ou d'abandonner) celles rendues désuètes. En ce sens, nonobstant les particularités de l'environnement dans lequel elle est mise en application, la PMT pourrait aider à motiver les individus à modifier leurs comportements et prémunir les entreprises qui manipulent des informations sensibles de la plupart des risques associés à l'humain.

Références

[1] Ertan, A., Crossland, G., Heath, C., Denny, D., & Jensen, R. (2020). *Cyber Security Behaviour in Organisations*. London: Royal Holloway University.

[2] Ponemon Institute (2018). *Cost of a Data Breach Report: Global Overview*. Ponemon Institute: Traverse City.

[3] Verizon Business RISK Team (2020). *2020 Data Breach Investigations Report*. Verizon Business.

[4] Boss, S., Galletta, D., Lowry, P., Moody, G., & 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.

[5] D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*.

[6] Da Veiga, A. (2016, July). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In *2016 SAI Computing Conference (SAI)* (pp. 1006-1015). IEEE.

[7] Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, *70*, 72-94.

[8] Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

[9] Gutzwiller, R. S., Fugate, S., Sawyer, B. D., & Hancock, P. A. (2015, September). The human factors of cyber network defense. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *59*(1), 322-326.

[10] Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach?. Journal of Management Information Systems, 29(3), 157-188.

[11] Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). Human Factors And Information Security: Individual, Culture and Security Environment (No. DSTO-TR-2484). *Defence Science and Technology Organisation: Command Control Communications and Intelligence Division*. Edinburgh: Australia.

[12] Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?.

[13] Becker, I., Islam, T., Posner, R., Ekblom, P., McGuire, M., Borrion, H., & Li, S. (2019, November). A socio-technical and co-evolutionary framework for reducing human-related risks in cyber security and cybercrime ecosystems. In *International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications* (pp. 277-293). Springer, Singapore.

[14] Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. Information & Management, *49*(2), 99-110.

[15] Cram, W. A., D'arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. MIS Quarterly, 43(2), 525-554.

[16] Karyda, M. (2017). Fostering Information Security Culture in Organizations: A Research Agenda. In MCIS (p. 28).

[17] Hoffman, D. L., Novak, T. P., & Schlosser, A. E. (2001). The evolution of the digital divide: Examining the relationship of race to Internet access and usage over time. *The digital divide: Facing a crisis or creating a myth*, 47-97.

[18] Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, p.102003.

[19] Beautement, A., Sasse, M. A., & Wonham, M. (2008, September). The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop* (pp. 47-58).

[20] Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69-79.

[21] Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In *Emerging Cyber Threats and Cognitive Vulnerabilities* (pp. 73-92). Academic Press.

[22] Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198.

23 Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2-16.

24 Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190-209.

25 Crossler, R. E. & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database for Advances in Information Systems*, *45*(4), 51-71.

26 Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & security*, *32*, 90-101.