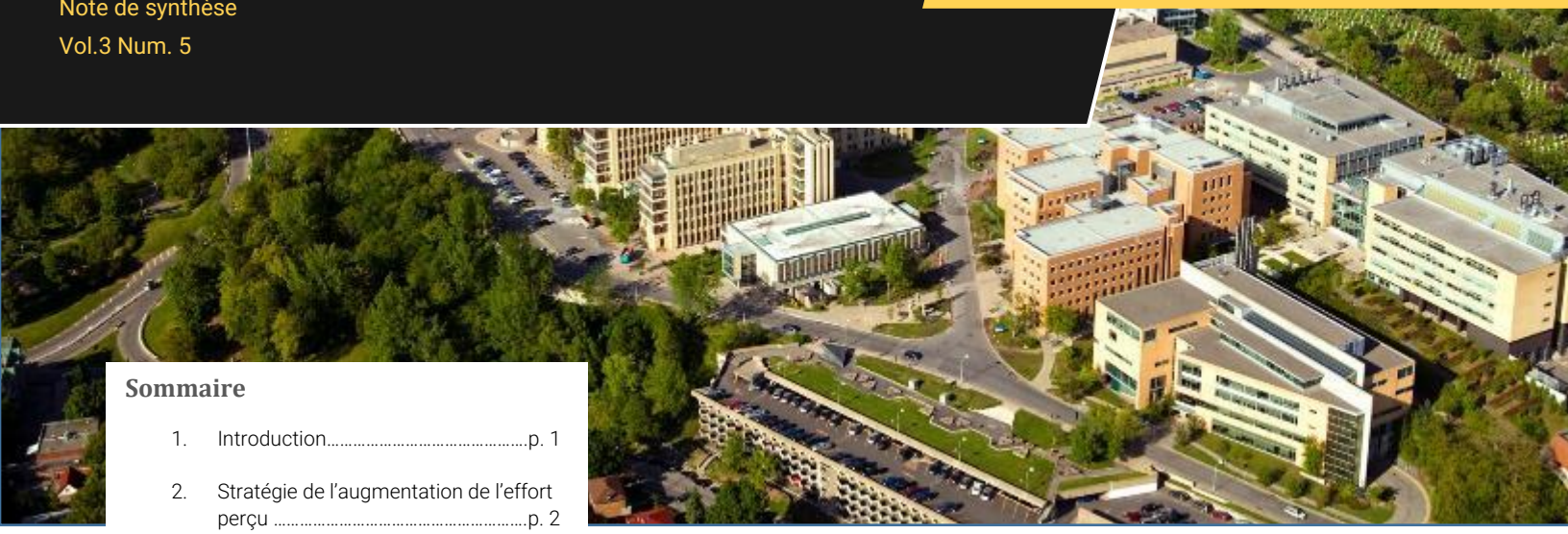
La prévention situationnelle appliquée à la cybercriminalité

Wassim Samy Azzoug, M.Sc.

Note de synthèse
Vol.3 Num. 5

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

La prévention situationnelle du crime (PSC) regroupe un ensemble de mesures de prévention visant des formes très spécifiques de criminalité, impliquant la gestion, la conception ou la manipulation de l'environnement immédiat de manière systématique et permanente afin de réduire les opportunités criminelles et augmenter les risques perçus par les délinquants[1]. La prévention situationnelle cible l'intervention sur l'acte délinquant et les situations de la vie quotidienne dans lesquelles il se produit. Elle part du postulat que pour arriver à des résultats, une intervention préventive doit cibler des problèmes très spécifiques, des personnes ou des espaces bien délimités, plutôt que de procéder à des changements importants dans une société, une communauté, un quartier[2].

Trois perspectives théoriques en criminologie s'alignent sur les principes de la PSC : (1) la théorie de l'activité routinière (TAR)[3] dont le postulat explique comment de vastes changements sociétaux créent des opportunités de criminalité au niveau macro ; (2) la théorie des modèles de criminalité[4], qui s'appuie sur les influences environnementales pour expliquer comment les facteurs de voisinage influencent les opportunités de criminalité ; et (3) la perspective du choix rationnel[5, 6] qui opère au niveau micro et explique comment la prise de décision au niveau individuel est conditionnée par le quartier et les situations environnementales qui donnent lieu aux événements criminels.

Ces trois théories offrent des informations très pertinentes pour comprendre les mécanismes de neutralisation des opportunités pertinents pour la prévention situationnelle[7]. Par exemple, la théorie du choix rationnel part du postulat que les délinquants prennent des décisions rationnelles sur quand, comment et où commettre des crimes lorsque la situation leur est favorable. La création de circonstances défavorables, qui est l'objectif de la prévention situationnelle, a donc pour but de dissuader les délinquants. En effet, « la règle cardinale des théories du choix rationnel est de ne jamais considérer un acte criminel comme gratuit, insensé ou irrationnel, mais plutôt de chercher à comprendre les objectifs du délinquant »[8].

Des chercheurs ont proposé cinq stratégies générales de PSC à savoir « Augmenter l'effort », « Augmenter les risques », « Réduire les récompenses », « Réduire les incitations » et « Supprimer les excuses »[2]. Chacune de ces stratégies a été opérationnalisée à travers une série de techniques de PSC dans un objectif de réduction du crime.

Stratégie de l'augmentation de l'effort perçu

L'augmentation de l'effort perçu comprend des stratégies conçues pour rendre le crime plus difficile à réaliser[9]. Elle comprend les mesures suivantes : 1) la protection des cibles; 2) le contrôle des accès; 3) le contrôle des sorties; 4) l'orientation du public; 5) la régulation de la mise en circulation des armes et outils. Ces mesures visent à augmenter le niveau d'effort perçu pour commettre le crime, ce qui représente un élément de coût, c'est-à-dire que les coûts de la commission du crime viennent surpasser les bénéfices que le délinquant peut en tirer. Puisque la difficulté à réaliser une action influence l'attitude et la décision d'un individu à poursuivre son projet, augmenter les efforts perçus permettrait de prévenir le crime. Lorsqu'appliquée au cyberespace, cela signifie généralement qu'il faut s'assurer que les cybercriminels doivent déployer plus d'efforts lorsqu'ils souhaitent lancer une cyberattaque. Ainsi, des mesures de cybersécurité telles que les pare-feux, les mots de passe et les politiques de gestion des comptes (voir Annexe) font partie des stratégies ayant pour but d'augmenter les efforts perçus lors de la commission du délit.

Stratégie de l'augmentation du risque perçu

L'augmentation du risque perçu implique des stratégies qui font supposer au criminel que le risque associé au crime est supérieur au bénéfice qu'il pourrait en retirer[9]. Ces stratégies visent à réduire les récompenses anticipées du criminel. Les individus prennent en considération les conséquences de leurs actions avant de les commettre ; la mesure du risque influence alors leur attitude et leur décision concernant l'engagement dans une violation ou un crime[11]. Appliquée à la cybersécurité, cette stratégie vise à augmenter la possibilité de détection des cybercrimes grâce à la surveillance et au contrôle par des tiers dans le cyberespace[10]. En d'autres termes, l'augmentation du risque est associée à une probabilité accrue d'identification du délinquant, de détection de la violation par les autorités compétentes ou d'appréhension résultant d'un méfait[12].

Stratégie de la réduction de la récompense anticipée

La réduction de la récompense anticipée comprend des stratégies pour diminuer les récompenses obtenues par le criminel[9]. Les récompenses forment le cœur de la motivation extrinsèque du comportement des individus dans de nombreux cas en les encourageant à adopter un comportement particulier[13]. En cybersécurité, les mesures telles que le chiffrement- sont utiles pour empêcher les cybercriminels, notamment ceux s'adonnant au vol de données, d'exploiter leurs récompenses en rendant l'utilisation des données difficile, voire impossible (par exemple, des données). Il sera donc plus difficile pour eux de revendre ces données sur les marchés illicites du Darkweb par exemple, diminuant ainsi leur motivation à commettre un vol de donnée.

Stratégie de la réduction des incitations

La réduction des incitations comprend des stratégies visant à réduire les facteurs précipitants du crime[9]. L'incitation fait référence à l'action ou à l'événement qui amène un individu à passer à l'action. L'incitation agit comme un stimulus sur le comportement des individus et peut conduire à un comportement négatif et agressif dans certaines conditions[14]. En réduisant les incitations, l'objectif est de réduire les causes émotionnelles et la motivation pour commettre une infraction. Gérer les problèmes négatifs et prévenir les conflits dans l'environnement de travail, diminuer l'excitation émotionnelle, la frustration et le stress, décourager l'imitation et neutraliser la pression des pairs sont des exemples de techniques de réduction des incitations dans les organisations[15]. Ces mesures ne sont pas techniques, mais visent à prévenir toute situation pouvant créer des émotions négatives chez les employés des organisations. Par exemple, le eSafety Commissioner, un organisme australien dont la fonction est de favoriser la sécurité en ligne, a recommandé d'avoir un dialogue ouvert sans porter de jugement avec les enfants qui ont été victimes de cyberintimidation[10].

Stratégie de la suppression des excuses

Finalement, la suppression des excuses reconnaît que les délinquants portent des jugements moraux sur leur comportement et qu'ils rationalisent souvent leur conduite pour « neutraliser » tout sentiment de culpabilité ou de honte[9]. Ces stratégies visent à supprimer les excuses potentielles du criminel (justification, rationalisation) pour avoir commis le crime[9]. La rationalisation et la justification de l'inconduite jouent un rôle important dans l'apparition du crime. La rationalisation ou la recherche d'excuses est un mécanisme de défense pour justifier et expliquer une violation de manière logique et rationnelle. Empêcher cette justification permettrait de prévenir les passages à l'acte criminel[16]. Fournir des documents clairs, contrôler et surveiller, et appliquer systématiquement les politiques sont des approches qui peuvent inhiber la pratique consistant à présenter de telles excuses par les individus. La clarification des règles et politiques de sécurité de l'information, la sensibilisation à la cybersécurité et l'aide aux employés pour se conformer aux règlements sont d'autres exemples de cette approche pour retirer les excuses du personnel lorsqu'ils dérogent aux règles de sécurité[14].

Résultats d'études PSC appliquées à la cybercriminalité

Des chercheurs ont démontré comment la théorie des activités routinières peut être utilisée pour modéliser l'incidence de la fraude sur Internet[17]. Les auteurs expliquent que la forme de prévention la plus efficace contre la fraude passe par la méthode de réduction de l'exposition c'est-à-dire que le fait de changer ses habitudes en ligne en réduisant son exposition, à travers l'utilisation de serveurs sécuritaires ou de logiciel antivirus, permettrait de prévenir efficacement les risques de fraude. Toutefois, un autre chercheur, dans une étude similaire sur les tentatives d'hameçonnage, a abouti à des résultats différents[18]. S'appuyant sur la théorie des activités routinières, le chercheur a démontré qu'augmenter la présence de gardiens, par exemple, les banques, en bloquant les transactions suspectées comme étant frauduleuses, permet de réduire les taux de victimisation à l'hameçonnage. Ainsi, selon cette étude, le succès des mesures de préventions contre l'hameçonnage dépend d'une surveillance efficace des transactions bancaires des potentielles victimes et de l'analyse des cas suspects, conduisant à réduire les bénéfices du crime pour les cybercriminels[18]. Dans le cas du cyberharcèlement, augmenter le risque de détection semble également efficace pour en limiter les occurrences, notamment par la présence de modérateurs de plateformes puisqu'ils peuvent manipuler l'environnement virtuel de sorte à limiter les opportunités criminelles[19]. Bien qu'encore peu nombreuses, les résultats de ces différentes études appliquant les principes de la prévention situationnelle à la cybercriminalité fournissent des résultats prometteurs quant à son efficacité.

Conclusion

L'étude de l'application des cinq stratégies générales de PSC et leurs techniques pourrait entraîner des changements dans la manière, dont les experts en cybersécurité et les organismes chargés de l'application de la loi créent des moyens plus efficaces d'augmenter l'effort requis et les risques pour les cybercriminels et, par conséquent, de réduire leurs récompenses et leurs motivations à commettre des cybercrimes. Les mesures préventives donnent aux entreprises un moyen proactif de réduire leurs expositions aux cybermenaces au lieu d'y répondre une fois l'incident passé.

Cependant, il est important de comprendre l'impact et l'effet des stratégies de prévention mises en place afin de juger de leurs pertinences. En s'attaquant directement aux motivations et facteurs situationnels des cybercriminels dans un objectif de dissuasion, les retombées seront plus pertinentes au niveau de la réduction des risques. L'objectif ultime de la PSC est de créer des interventions qui éliminent toute possibilité de commettre une certaine forme de crime ou du moins, de réduire la prévalence d'un crime spécifique. Il est important de noter que d'autres interventions de PSC ne cherchent pas à réduire ou à éliminer l'occurrence d'un crime spécifique, mais plutôt à réduire les dommages qu'il cause, ce qui pourrait mieux s'appliquer en cybersécurité où le risque zéro n'existe pas.

Références

[1] Clarke, R. V. (1983). Situational crime prevention: Its theoretical basis and practical scope. Crime and justice, 4, 225-256.
[2] Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators, and criminal decisions: A reply to Wortley's critique of situational crime prevention. Crime prevention studies, 16, 41-96.
[3] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American sociological review, 588-608.
[4] Brantingham, P. L., & Brantingham, P. J. (1993). Nodes, paths and edges: Considerations on the complexity of crime and the physical environment. Journal of environmental psychology, 13(1), 3-28.
[5] Clarke, R. V., & Cornish, D. B. (1985). Modelling offenders' decisions: A framework for research and policy. Crime and justice, 6, 147-185.
[6] Cornish, D. B., & Clarke, R. V. (1986). The Reasoning Criminal: Rational Choice Perspectives on Offending Springer-Verlag, New York. NY Google Scholar.
[7] Clarke, R. V. (2009). Situational crime prevention: Theoretical background and current practice. Dans *Handbook on crime and deviance* (pp. 259-276). Springer, New York, NY.
[8] Clarke, R. V., & Cornish, D. B. (2001). Explaining criminals and crime: Essays in contemporary criminological theory.
[9] Clarke, R. (1997). *A revied classification of situational crime prevention techniques. Crime prevention at a crossroads*. Cincinnati
[10] Ho, M. H., Ko, R., & Mazerolle, L. (2022). Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review. Computers & Security, 102611.
[11] Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. Decision Support Systems, 48(4), 635-645
[12] Yusop, Z. M., & Abawajy, J. (2014). Analysis of insiders attack mitigation strategies. Procedia-Social and Behavioral Sciences, 129, 581-591.
[13] Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. Computers in Human Behavior, 28(3), 1019-1027.
[14] Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M. (2019). Deterrence and prevention-based model to mitigate information security insider threats in organisations. Future Generation Computer Systems, 97, 587-597.
[15] Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers & Security, 39, 447-459.
[16] Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses. Discouraging neutralization to reduce IT policy violation. Computers & security, 39, 145-159.
[17] Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. Journal of research in crime and delinquency, 47(3), 267-296.
[18] Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. Cyberpsychology, Behavior, and Social Networking, 17(8), 551-555.
[19] Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. Crime Prevention and Community Safety, 12(2), 99-118.

Recommandations

La prévention situationnelle du crime possède des qualités applicables à la cybersécurité et la lutte contre la cybercriminalité. Il est donc important d'étudier ses effets et de la mettre en oeuvre au sein de programmes de cybersécurité. Plusieurs recommandations sont suggérées ici :

- Une plus grande synthèse et collaboration entre les différentes disciplines de la cybersécurité, de la criminologie, de la psychologie, du droit et des sciences informatiques qui peut conduire à l'adoption de normes, d'avis et de réglementations plus efficaces qui peuvent prévenir la cybercriminalité.
- Développer l'identification d'un ensemble de contrôles appropriés dans la SCP qui peuvent prévenir des formes spécifiques de cybercriminalité.
- Valider de manière empirique l'efficacité des contrôles qui peuvent être utilisés pour prévenir les cybercrimes.

Annexe

Techniques de prévention situationnelle appliquée à la cybersécurité.

Augmenter l'effort	Augmenter les risques	Réduire les récompenses	Réduire les incitations	Empêcher toute justification
1) Protection des cibles Logiciels de sécurité.	6) Surveillance mutuelle Surveiller et contrôler l'accès à distance depuis tous les terminaux	11) Dissimulation des cibles Restreindre les informations du domaine public	16) Réduction des frustrations et des situations de stress Environnement de travail agréable	21) Mise en place de règles Politiques de sécurité des informations.
2) Contrôle des accès Contrôle des accès privilèges	7) Promotion de la surveillance naturelle par l'aménagement urbain Programme formalisé contre les menaces internes	12) Retrait des cibles Segmentation des informations et du matériel	17) Prévention des conflits Anticiper et gérer les problèmes dans au travail	22) Affichage de signalisations/ règle d'utilisation Règles de comportement
3) Contrôle des sorties Surveillance de l'exfiltration de données non autorisée	8) Réduction de l'anonymat Utiliser un système de gestion des informations et des événements de sécurité (SIEM) pour enregistrer, surveiller et auditer les actions des employés	13) Mesures de marquage des biens Marquage de propriété, protection des droits d'auteur, étiquetage des données	18) Réduction des tentations et des tensions Attention/réponse immédiate aux violations	23) Conscientisation Rappels formels d'utilisation acceptable
4) Orientation du public Attribution des privilèges en fonction des besoins du poste.	9) Recours à des garants des lieux Surveillance par les administrateurs système	14) Perturbation des marchés Protection des droits intellectuels, logiciels gratuits	19) Neutralisation de la pression des pairs Mise en place e processus disciplinaires	24) Promotion du respect des règles Sensibilisation aux menaces internes dans la formation à la sécurité
5) Régulation de la mise en circulation des armes et des outils Désactivation des droits d'accès des anciens employés.	10) Renforcement de la surveillance formelle Vidéosurveillance dans les zones contenant des équipements ou des informations sensibles	15) Suppression des bénéfices du crime Chiffrement des données	20) Décourager les actes d'imitation Application de la politique de sécurité sur les incidents ou les procédures disciplinaires	25) Contrôle de la consommation des stupéfiants et d'alcool. Éducation à la cyber éthique,