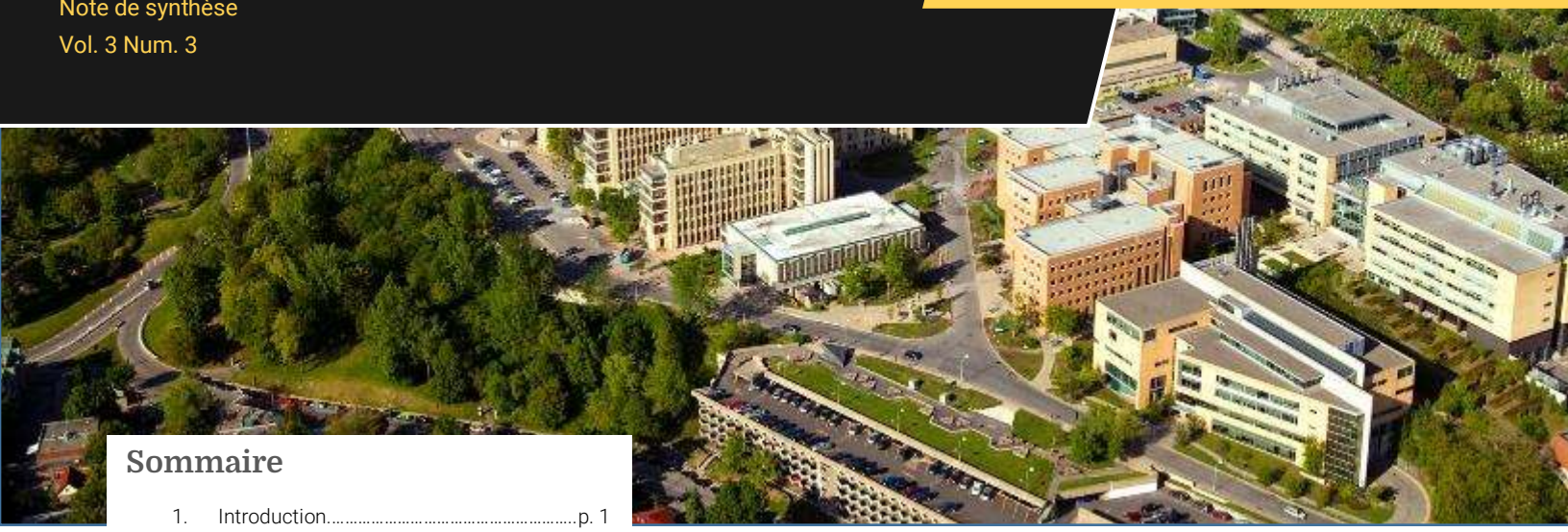
Communication des risques en cybersécurité et confiance

Marie-Pier Villeneuve-Dubuc, candidate à la maîtrise

Note de synthèse
Vol. 3 Num. 3

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

Les failles de sécurité et les brèches de données que subissent les organisations font drastiquement diminuer la confiance des clients envers ses dernières[1, 2, 3]. Les entreprises victimes de faille de sécurité se voient ainsi dans l'obligation de restaurer leur réputation et la confiance de leurs clients[4]. À cet effet, plusieurs études mettent en avant l'importance de la sensibilisation à la cybersécurité et une bonne communication des risques, afin que les entreprises puissent rétablir le lien de confiance avec leur clientèle[5, 6, 7, 8, 9]. Plus spécifiquement, la communication du risque (« risk communication » en anglais) est particulièrement pertinente lorsqu'il est question d'améliorer la confiance d'une clientèle envers une entreprise.

La communication des risques en cybersécurité

La communication du risque est un concept large qui représente le processus interactif d'échange d'informations relatif à un risque, que ce soit à propos de la nature de celui-ci, sa signification, ses conséquences, sa probabilité d'apparition et les options de réponse à ce risque[10]. Ce type de communication vise à informer les individus afin de leur permettre de porter des jugements éclairés face au risque en question et de les motiver à agir[10,11]. De plus, elle peut servir à établir ou rétablir la confiance entre deux parties prenantes et les impliquer dans un dialogue afin de résoudre un différend

dans l'objectif de trouver un consensus[10, 12, 13]. La communication des risques s'applique principalement aux domaines de la santé et des sciences de la nature, notamment pour informer les patients de problèmes de santé graves ou bien encore avertir la population de dangers environnementaux ou de désastres naturels[8]. Devant la numérisation grandissante des entreprises, la communication des risques dans les activités organisationnelles de cybersécurité est indispensable pour améliorer, de manière continue, la sécurité des systèmes d'information[14].

Les enjeux de la communication du risque

Les techniques de communication du risque sont généralement utilisées par les promoteurs de la cybersécurité (« cybersecurity advocates » en anglais), considérant qu'ils sont fréquemment des professionnels, dont le rôle est d'encourager et de faciliter l'adoption de comportements sécuritaires en matière de cybersécurité[8]. Cependant, pour que les communications soient efficaces, qu'elles soient reliées aux risques ou non, les promoteurs doivent déjouer les perceptions négatives que les individus ont envers la sécurité[8]. Considérant que la cybersécurité est très souvent perçue comme effrayante, floue, inintéressante ou bien encore non importante par les utilisateurs, il importe de mettre davantage d'efforts pour modifier les perceptions des individus pour que les messages soient bien reçus. En outre, la notion de confiance semble cruciale pour inciter les humains à agir, considérant que le manque de confiance envers la source même de l'information amène les individus à simplement ignorer le message[15].

Cependant, la communication du risque peut être controversée lorsqu'elle inclut la transmission de messages contenant des menaces pour la sécurité, ce qui peut causer des sentiments hostiles envers le communicateur et ainsi nuire davantage à la confiance qui lie les parties prenantes[16]. Ce phénomène s'explique par le « modèle des bruits mentaux » (« Mental Noise Model » en anglais). Ce modèle s'intéresse aux mécanismes que les individus utilisent pour traiter les informations lorsqu'ils sont dans une situation stressante et, comment cela influence leur manière de communiquer avec autrui[10, 17]. Ce modèle stipule que lorsque les individus subissent un stress important, leur capacité à bien traiter l'information qui leur est transmise est considérablement modifiée par des émotions négatives telles que la peur, l'anxiété et même la colère[18, 19] ce qui cause une agitation mentale créant ainsi des « bruits mentaux » et une diminution de la capacité de rationalisation[20].

Une communication efficace du risque

Plusieurs aspects doivent être considérés pour réaliser une bonne communication du risque. En effet, des études ont établi qu'il est important que les informations soient à la fois simples et spécifiques, d'éviter les ambiguïtés, d'adapter l'information en fonction du public cible, d'aider les gens à considérer les conséquences de leurs décisions, de fournir des pistes d'action précises, de renforcer l'auto-efficacité des individus, et ce, tout en présentant l'information de manière engageante et stimulante[8, 14, 21, 22, 23]. D'autant plus, les facteurs qui semblent influencer la réception positive d'une communication du risque dépendent de plusieurs éléments incluant : la présentation du message, son format, son degré de spécificité, la couverture complète du sujet, sa pertinence, son actualité, sa cohérence et sa crédibilité[22]. Afin d'éviter que le message envoyé soit perçu comme étant négatif et menaçant, causant ainsi la perte de confiance envers l'auteur du message, il faut que le message de nature négative soit transformé de manière positive[16]. De plus, il faut que les individus qui transmettent le message véhiculent de l'empathie, de l'honnêteté et de l'ouverture, en plus de démontrer une bonne écoute pour bien saisir les rétroactions et un dévouement à aider autrui[21, 24].

De nombreuses actions peuvent être mises en place pour s'assurer que les communications sont efficaces, par exemple, en établissant un plan de communication du risque, en rendant ces communications simples et claires, en choisissant

méticuleusement le moyen de communication, ce que ce soit verbal ou bien encore visuel, et en s'assurant de fournir de la documentation servant de référence pour le futur[15]. L'Annexe permet de résumer les dix principales recommandations établies par le chercheur Jason Nurse pouvant être appliquées par toute organisation de cybersécurité[15]. En bref, en cybersécurité, il est important de considérer la structure du message et comment ce dernier est envoyé[25].

Rétablir la confiance

Afin d'établir une bonne communication du risque et ainsi rétablir la confiance, la littérature scientifique préconise l'application du modèle de la détermination de la confiance (« Trust Determination Model » en anglais). Ce modèle justifie la pertinence d'impliquer une tierce partie, représentant une source de confiance élevée, afin d'établir ou de maintenir la confiance[26]. Cette tierce partie peut autant consister en des professionnels de la santé, des scientifiques ou des experts/professionnels de la sécurité[27]. Cependant, il est important que ces tierces parties incarnent quatre facteurs de la détermination de la confiance : le dévouement et l'engagement, la compétence et l'expertise, l'honnêteté et l'ouverture [26]. De plus, la confiance est nécessaire afin que la communication du risque soit bien reçue[28, 29]. La confiance, se créant sur une longue période, résulte d'un continuel effort d'écoute et d'habiletés de communication[29, 30]. Après un incident de cybersécurité ou lorsque le risque est imminent, il est important d'appliquer les facteurs reliés au modèle de la détermination de la confiance, et particulièrement, viser à avoir une bonne communication avec la clientèle, assumer les responsabilités de l'entreprise, démontrer de l'engagement, être cohérent dans les communications, être transparent et maintenir la confidentialité des victimes[31]. Néanmoins, une mauvaise communication du risque peut causer une diminution de la confiance [16, 32, 33]. Subséquemment, la communication du risque se doit d'être faite de manière complètement réfléchie pour contribuer à rétablir une confiance, car elle peut aussi causer l'effet inverse si elle est mal accomplie.

Conclusion

En conclusion, il importe de mettre en pratique et de maintenir une bonne communication du risque afin de non seulement, prévenir les cybermenaces mais également de maintenir une bonne relation et un lien de confiance fort avec sa clientèle, particulièrement après une faille de sécurité. Cette note de synthèse démontre que les recommandations des experts et la littérature scientifique reliée à la psychologie, aux politiques publiques, aux communications, et aux sciences de la nature comme la biologie et la santé, permettent de mieux comprendre les principes de la communication du risque, son origine et comment cette dernière s'applique en cybersécurité. Les recommandations à l'Annexe permettent d'outiller les praticiens en cybersécurité afin d'assurer que leurs communications du risque soient faites de manière réfléchie et éclairée.

Références

[1]. Campbell, K., Gordon, L. A., Loeb, M.P. et Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431-448.

[2]. Acquisti, A., Friedman, A. et Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 94.

[3]. Curtis, S., Carre, J. et Jones, D. (2018). Consumer security behaviors and trust following a data breach. *Managerial Auditing Journal*, *33*(4). DOI: 10.1108/MAJ-11-2017-1692

[4].Knight, R. et Nurse, RC. J. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, 99.

[5]. Beach, K. S. (2014). Usable Cybersecurity: Human Factors in Cybersecurity Education Curricula. *National Cybersecurity Institute Journal*, *1*(1), 5-21.

[6]. Bada, M. et Nurse, RC. J. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393-410. DOI 10.1108/ICS-07-2018-0080

[7]. Bada, M., Sasse, D. et Nurse, RC. J. (2015). Cyber Security Awareness Campaings: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*. ISSN 2052-8604.

[8]. Haney, J. M. et Lutters, W. G. (2018). « It's Scary...It's Confusing...It's Dull »: How Cybersecurity Advocates Overcome Negative Perceptions of Security. Proceedings of the Fourteenth Symposium on Usable Privacy and Security.

[9]. Boletsis, C., Halvorsrud, R., Pickering, J., Phillips, S. et Surridge, M. (2021). Cybersecurity for SMEs: Introducing the Human Element into Socio-

technical Cybersecurity Risk Assessment. *Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications - IVAPP*, (p. 266-274).

[10]. National Research Council (1989). Improving Risk Communication. National Academy of Sciences.

[11]. Kasperson, R., Golding, D. et Tuler, S. (1992). Social Distrust as a Factor in Siting Hazardous Facilities and Communicating Risks. *Journal of Social Issues*, *48*(4), 161-187.

[12]. Morgan, G., Fischhoff, B., Bostrom, A., Lave, L. et Atman, CJ. (1992). Communicating risk to the public. *Environ Science Technology*, *26*(11), 2048–2056.

[13]. Covello, VT. (1998). Risk perception, risk communication, and EMF exposure: tools and techniques for communicating risk information. Dans R. Matthes, JH, Bernhardt et MH, Repacholi, (dir), *Risk Perception, Risk Communication, and Its Application to EMF Exposure*: Proceedings of the World Health Organization/ICNRP International Conference (ICNIRP 5/98), (p. 179–214). International Commission on Non-Ionizing Radiation Protection.

[14]. Nurse, J. R. C., Creese, S., Goldsmith, M., et Lamberts, K. (2011a): Trustworthy and effective communication of cybersecurity risks: A review. *Proceedings of the 2011 Workshop on Socio-Technical Aspects in Security and Trust (STAST) at 5th International Conference on Network and System Security (NSS)*, IEEE, 60-68.

[15]. Nurse, J. R. C. (2013). Effective Communication of Cyber Security Risks. *7th International Scientific Conference on Security and Protection of Information*.

[16]. Rowan, K. E. (1994). Why rules for risk communication are not enough: A problem solving approach to risk communication. *Risk Analysis*, *14*(3), 365–374.

[17]. Baron, J., Hershey, JC. et Kunreuther, H. (2000). Determinants of priority for risk reduction: the role of worry. *Risk Anal*, *20*(4), 413–428.

[18]. Gould, L. et Walker, C. (1982). *Too Hot to Handle*. Yale University Press.

[19]. Neuwirth, K., Dunwoody, S. et Griffin, RJ. (2000). Protection motivation and risk communication. *Risk Anal*, *20*(5), 721–733.

[20]. Covello, V.T., Peters, R., Wojtecki, J. et Hyde, R. (2001). Risk Communication, the West Nile Virus Epidemic, and Bioterrorism: Responding to the Communication Challenges Posed by the Intentional or Unintentional Release of a Pathogen in an Urban Setting. *Journal of Urban Health: Bulletin of the New York Academy of Medicine*, *78*(2).

[21]. Covello, V. (1997). Risk communication. Dans H. Waldron et C. Edling (dir.), *Occupational Health Practice* (6). Arnold Publishers.

[22]. Nurse, J. R. C., Rahman, S. S., Creese, S., Goldsmith, M, et Lamberts, K. (2011b). Information quality and trustworthiness: A topical state-of-the-art review. *International Conference on Computer Applications and Network Security (ICCANS)*, IEEE, 492–500.

[23]. Dolata, M., Comes, T., Schenk, B. et Schwabe, G. (2016). Persuasive practices: Learning from home security advisory services. *International Conference on Persuasive Technology*, 176–188.

[24]. Slovic, P. (1987). Perception of risk. *Science*, 236(4799), 280–285.

[25]. Beard, H. P. (2016). Cybersecurity message framing. ProQuest Dissertations & Theses Global. https://www.proquest.com/dissertations-theses/cybersecurity-message-framing/docview/1849023455/se-2?accountid=12543

[26]. Peters, RG., Covello, VT. et McCallum, DB. (1997). The determinants of trust and credibility in environmental risk communication: an empirical study. *Risk Anal*, 17(1), 43–54.

[27]. US Environmental Protection Agency (1990). *Public Knowledge and Perceptions of Chemical Risks in Six Communities: Analysis of a Baseline Survey*. US Government Printing Office.

[28]. Renn, O. et Levine, D. (1991). Credibility and trust in risk communication. Dans R. Kasperson, et P. Stallen. (dir.), *Communicating Risks to the Public* (p.175-218). Kluwer Academic Publishers.

[29]. Slovic, P. (1999). Trust, emotion, sex, politics, and science: surveying the risk-assessment battlefield. *Risk Anal*, *19*(4), 689–701.

[30]. National Research Council (1996). *Understanding Risk: Informing Decisions in a Democratic Society*. National Academy Press.

[31]. Appiah, B. O. et Maharjan, R. (2020). Developing and Maintaining Trust Within Organizations: Tech One Global in Nepal [Mémoire de maîtrise, University of Gävle]. DiVA.

[32]. Covello, V., McCallum, DB. et Pavlova, MT. (1989). Principles and guidelines for improving risk communication. Dans VT, Covello., DB, McCallum. et MT, Pavlova (dir.), *Effective Risk Communication: the Role and Responsibility of Government and Nongovernment Organizations*, (p. 3-16). Plenum Press.

[33]. Chess, C., Salomone, KL., Hance, BJ. et Saville, A. (1995). Results of a national symposium on risk communication: next steps for government agencies. *Risk Anal*, *15*(2),115–125.

[34]. SPRITE+ (2022, janvier). SPRITE+ Community Building Event: Communicating Cybersecurity. mhttps://spritehub.org/2022/02/17/sprite-community-building-event-communicating-cybersecurity/

Annexe

Recommandations pratiques pour une communication efficace du risque en cybersécurité[15]

	Recommandations
1	Établir un plan préalable détaillant la manière dont les risques seront communiqués.
2	Concevoir les communications, tout en considérant que les humains possèdent une capacité de traitement de l'information limitée, en simplifiant l'information.
3	La signification des informations présentées dans les messages de risques de cybersécurité doit être claire.
4	Les utilisateurs ou clients doivent recevoir des directives d'actions claires et cohérentes en ce qui concerne les options de réponse au risque de sécurité.
5	Limiter l'utilisation de termes et de jargon techniques et trop spécifiques à la cybersécurité.
6	Être prudent lorsqu'il y a des communications qui impliquent des chiffres à propos des risques de cybersécurité.
7	Être attentif aux détails lorsque l'information est communiquée visuellement.
8	Être prudent lors des communications verbales sur les risques de cybersécurité, surtout en se concentrant sur les choix des mots.
9	Fournir de l'aide, des conseils et de la documentation sur la cybersécurité après chaque communication du risque.
10	Rendre les fonctionnalités de cybersécurité visibles et accessibles.