Exploring the Relationship Between Cybersecurity Culture and Cyber-Crime Prevention: A Systematic Review

Banuka DE SILVA
Faculty of Criminal Justice, General Sir John Kotelawala Defence University,
Ratmalana, Colombo, Sri Lanka
desilvakbn@kdu.ac.lk

Abstract

Cybercrime requires a multidimensional approach addressing technical, organisational, and human factors to prevent cyber-attacks. This systematic review highlights the significance of a strong cybersecurity culture in mitigating the risks of cyberattacks and enhancing an organisation's resilience. Implementing training and awareness programmes, establishing leadership support and accountability mechanisms, and fostering employee engagement are strategies for promoting a strong cybersecurity culture. However, fostering a robust culture of cybersecurity can be challenging and requires the participation of various stakeholders. Training and awareness programmes can significantly improve employee cybersecurity knowledge and behaviour, and leadership support is essential for establishing a cybersecurity culture. It is possible to enforce employee compliance with cybersecurity policies and procedures through accountability mechanisms, such as consequences for noncompliance and periodic security audits. Involving employees in the creation of cybersecurity policies and procedures, as well as recognising and rewarding responsible behaviour, can increase employee engagement and investment in cybersecurity. Although technical measures such as firewalls and encryption are essential for defending against cyber-attacks, a strong cybersecurity culture is necessary to mitigate cybercrime risks and enhance an organisation's resilience. Future research should identify and evaluate effective strategies for cultivating a robust cybersecurity culture in the context of preventing cybercrime. Cybersecurity should be a top priority for businesses and individuals, who must take preventative measures against cyber-attacks. By fostering a robust culture of cybersecurity, businesses can increase their resilience and reduce the risks of cybercrime.

Index terms: Cybercrime, cybersecurity culture, training and awareness programs, leadership support, accountability mechanisms, criminology

References

[1]. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101.

[2]. CASP. (2018). Critical Appraisal Skills Programme (CASP) Qualitative Checklist. Retrieved from https://casp-uk.net/wp-content/uploads/2018/03/CASP-Qualitative-Checklist-2018_fillable_form.pdf

[3]. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2019). The impact of culture on cybersecurity incident reporting. Information Systems Frontiers, 21(1), 55-69.

[4]. Eling, N., Heim, J., Kolokytha, S., & Renaud, K. (2018). Implementing a security culture in the workplace: An empirical study. Journal of Business Research, 89, 352-360.

[5]. Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2017). Cultivating a cybersecurity culture, in Advances in Accounting Behavioral Research, 20, 21-40.

[6]. Graf, D., & Borthick, A. F. (2018). Developing a cybersecurity culture: A review of the literature. Journal of Information Systems Education, 29(1), 35-45.

[7]. Kendall-Taylor, A., & Krause, J. (2018). Cybersecurity culture: A concept that works. Harvard Business Review Digital Articles, 2-5.

[8]. Kshetri, N. (2018). Cybercrime and cybersecurity: An introduction. Routledge.

[9]. Liao, Y., Hsu, C. L., & Chen, C. C. (2018). Developing an effective cybersecurity awareness training program: An empirical study. Computers & Security, 78, 398-408.

[10]. Marshall, A. (2019). A coordinated approach to fighting cybercrime. Computer Fraud & Security, 2019(1), 11-14.

[11]. McAfee. (2018). Economic impact of cybercrime: No slowing down. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/atr-economic-impact-cybercrime.pdf

[12]. Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & PRISMA Group. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. PLoS Med, 6(7), e1000097.

[13]. National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, version 1.1. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[14]. Nissenbaum, H., Shiffrin, S., & Johnson, D. G. (2018). Internet freedom and political trust: The role of contextual factors. The Information Society, 34(1), 1-13.

[15]. Peltier, J. A., Peltier, T. R., & Blackley, J. A. (2016). Information security fundamentals. CRC Press.

[16]. Rousseau, D. M., & Friedland, N. (2018). Reducing cybersecurity risk: An exploration of the role of organizational culture. Journal of Business Ethics, 152(1), 97-115.

[17]. Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

[18]. Van der Woude, M. (2018). Underreporting of cybercrime: Issues and challenges. European Journal of Criminology, 15(6), 723-739.