International Journal of Cybersecurity Intelligence & Cybercrime

Volume 2 | Issue 2 Article 1

9-6-2019

The Future of Cybercrime Prevention Strategies: Human Factors and A Holistic Approach to Cyber Intelligence

cybercrime, prevention, human factor, holistic approach, cyber-intelligence

Recommended Citation

Back, S., & LaPrade, J. (2019). The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence. International Journal of Cybersecurity Intelligence & Cybercrime, 2(2), 1-4. https://www.doi.org/10.52306/02020119KDHZ8339

IJCIC Center for Cybercrime Investigation & Cybersecurity

Back, S., & LaPrade, J. (2019). *International Journal of Cybersecurity Intelligence and Cybercrime, 2* (2), 1-4.

The Future of Cybercrime Prevention Strategies: Human Factors and A Holistic Approach to Cyber Intelligence

Sinchul Back*, University of Scranton, USA

Jennifer LaPrade, University of Texas at Dallas, USA

Keywords; cybercrime, prevention, human factor, holistic approach, cyber-intelligence

Abstract:
New technology is rapidly emerging to fight increasing cybercrime threats, however, there is one important component of a cybercrime that technology cannot always impact and that is human behavior. Unfortunately, humans can be vulnerable and easily deceived making technological advances alone inadequate in the cybercrime fight. Instead, we must take a more holistic approach by using technology and better understanding the human factors that make cybercrime possible. In this issue of the International Journal of Cybersecurity Intelligence and Cybercrime, three studies contribute to our knowledge of human factors and emerging cybercrime technology so that more effective comprehensive cybercrime prevention strategies can be developed.

Introduction

The evolution of cutting-edge technologies, such as the Internet of Things and the 5th Generation (5G) wireless telecommunications networks influence how we communicate, operate our critical infrastrucure, and conduct economic activity (Krebs, 2019). As such, these emerging technologies create the future of internet innovation and connectivity that build online life eco-enviornments (Ahmad et., 2019). Therefore, people are expected to be more likely to engage in online activities from social media to the Internet of Things (e.g., power autonomous vehicles, refrigerators, and medical/healthcare devices). Because our real world heavily intertwines with online systems, these innovations can provide additional cybercrime eco-friendly environments where criminals have more opportunities.

New innovations to make online environments more secure are also being developed such as blockchain technology, which can enhance "the trustworthiness and integrity of transcative energy data by supporting multifactor verification through a distributed ledger" (Mylrea & Gourisetti, 2017, p. 19). However, a European Cyber Security Perspective 2019 report states that state-of-the-art technology cannot be the only remedy to mitigate cybersecurity risks, in fact, the human element is also

*Corresponding author

Department of Sociology, Criminal Justice, & Criminology, University of Scranton, 800 Linden St, Scranton, PA, 18510, USA.
Email: sinchul.back@scranton.edu

a very crucial component to disrupt cyber threats. Accordingly, U.S. Federal Chief Information Officer Suzette Kuhlow Kent emphasized that humans are still one of the most significant factors to mitigate cybercrime. At the same time, humans are considered to be the weakest link in cybercrime prevention because many are easy to manipulate and remain highy vulnerable to deception (Conteh & Royer, 2016). In short, as a holistic approach, people's behavior and preventative action are every bit as important as implementing robust cybersecurity structures in order to effectively mitigate cyber threats.

Human Factors and Technologies

To date, many scholars have attempted to identify the cause of cybercrime and cybercrime victimization, including causes related to human factors. In line with previous studies, this issue of IJCIC contributes to the literature by exploring human behaviors and mindsets pertaining to cybercrime, as well as a look at new technology that works to make online environments safer and more secure. This issue includes three articles regarding 1) fear of cybercrime in social media and 2) perceptions of sharing intimate images, and 3) an emerging technology called blockchain systems.

Seong-Sik Lee, Kyung-Shick Choi, Sinyong Choi, and Elizabeth Englander (2019, this issue) discuss how social demographic factors, victimization experiences, opportunity factors, and social context factors are associated with the public's fear of crime on social networking sites (SNS). Four major theoretical frameworks - vulnerability model, victimization model, disorder and social integration models, and risk interpretation model – are applied to identify significant predictors of the fear of cybercrime victimization. Lee and his colleagues conclude that sociodemographic factors (i.e., age and gender), opportunity factors (i.e., target attractiveness and offending peers on SNS), and social context factors (i.e., bridging network and bonding-centric social networks) influenced the fear of cybercrime such as verbal abuse, sexual harassment, privacy infringement, hacking/malware, and property damage. The findings help explain how human interaction in virtual space and social environments substantially impact the nature of cybercrime victimization. Even though a large body of work has highlighted the significance of human and social factors on crime victimization or fear of crime in the physical world, there has been a lack of research on this relationship in the cyber world. Thus, this study contributes to the literature and provides an exploratory foundation upon which future studies can develop cybercrime prevention strategies based on human and social factors.

Jin Ree Lee and Steven Downing (2019, this issue)'s study is another article in IJCIC which received high ratings from reviewers. The study is one of the first to examine why individuals send intimate images to others through texting and social media. As such, Lee and Downing significantly contribute to this unveiled literature. Using mixed methods, the researchers conducted a perception analysis and found respondents were more likely to share images with romantic partners and preferred sending non-intimate images. Respondents also believed sharing intimate images without consent was motivated by bullying, revenge, or a desire to "show off" and could indicate or be signs of abusive behavior. Understanding the human motivations behind online image sharing can help lead to better protection and education for online users and their privacy. Furthermore, the authors provide directions for future research, such as considering how human factors (i.e., socially constructed norms) interact with held beliefs about close peers and romantic partners.

And, finally, Nicolas Blasco and Nicholas Fett (2019, this issue) investigate the strengths and potential weaknesses of emerging technology known as blockchain networks, which are designed to make online environments safer and more secure. Specifically, the authors examined the role of target hardening within the theoretical framework of situational crime prevention theory in relation to cybercrime. They tested the vulnerability of blockchain network architectures so that developers can have a better understanding of the strengths and weaknesses when creating security to combat against cybercrime. Understanding the ins and outs of this type of protective technology is critical in order to effectively fight increasing cyber threats. However, as these three papers show, it is only with a comprehensive and holistic approach that includes technology and consideration of human factors that a cybercrime prevention strategy can truly be effective.

Holistic Approach to Cyber Intelligence

How can we boost an online user's preventative behavior or harden our target environment as part of an effective cybercrime prevention strategy? In general, cybersecurity awareness training is considered to be an effective preventative measure in order to harden the softest component, human vulnerability. The studies in this issue suggest that cybercrime awareness campaigns and building socially constructed norms for online users will improve human vulnerabilities to cybercrime. Likewise, many cybersecurity experts and scholars assert that cybersecurity awareness education and training is one of the most significant aspects for individuals to effectively fight against cyber threats (Abawjy, Thatcher, & Kim, 2008; Back, LaPrade, Shehadeh, & Kim, 2019; Dodge, Carver, & Ferguson, 2007). As such, considering that human factors still play a significant role in the ongoing development of cybersecurity and protecting critical information infrastructures, it is important to note that cyber place management strategies along with implementing cybersecurity awareness training, and a resilient incident response system are all crucial means to effectively mitigate the likelihood of cybercrime victimization and minimize losses in an online setting.

Policht (2019) points out that the majority of modern cybercrimes tend to rely on a multi-dimensional approach to establish persistence in the target environment by using the following sequence of steps: observe, orient, decide, and act. From the cyber adversary perspective, first, the cybercriminal needs to stick around and understand the suitable target's environment, making a decision on which cybercrime typology they will utilize. Afterwards, the cybercriminal commits cyber threats to the suitable target. From the defender's perspective, what is our objective? The key is to detect and interrupt malicious attacks or abnormal behavior (e.g., unauthorized access and phishing scams) through cyber threat intelligence tools such as Advanced Threat Analytics or Security Risk Detection before the criminal reaches the point of malicious actions. In this regard, information security officials can apply more agile real-time detection systems or behavioral-pattern threat detection systems for identifying the emerging phishing campaign or other types of emerging cybercrime. Because trends of cybercrime change and turn over so quickly, immediate notification of a cybercrime threat is necessary for online users. After several mass shootings at higher education institutions in the United States, many universities have proactively and reactively implemented an Internet-based message board to alert the campus about emergencies. Likewise, entities in collaboration with government agencies can apply this Internet-based alert systems to rapidly disseminate cybercrime information to online users as quickly as information security officials identify it before cybercriminals take more severe attacks to suitable targets.

In summary, our thinking, policies, and cybersecurity technology must progress at the same pace that technology and cybercrime trends are also progressing. The papers included in this issue provide support for the link between human factors, technology, and cybercrime. We have just begun to see how the holistic approach of the cyber intelligence framework along with human factors can be applied to suppress criminal opportunities and mitigate the cyber risk in our society. We hope this holistic approach of a cyber intelligence framework inspires readers with possible areas to focus their future research and policy implications. We look forward to receiving contributions from scholars, policy analysts, practitioners, and others on enhancing theory, methods, and practice within the field of cybersecurity and cybercrime on national, regional, and international dimensions.

References

Abawajy, J., Thatcher, K., & Kim, T. H. (2008, April). Investigation of stakeholder's commitment to information security awareness programs. In *2008 International Conference on Information Security and Assurance (ISA 2008)* (pp. 472-476). IEEE.

Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., & Ylianttila, M. (2019). Security for 5G and Beyond. *IEEE Communications Surveys & Tutorials.*

Back, S., LaPrade, J., Shehadeh, L., & Kim, M. (2019, June). Youth hackers and adult hackers in South Korea: An application of cybercriminal profiling. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 410-413). IEEE.

Blasco, N. J., & Fett, N. A. (2019). Blockchain security: Situational crime prevention theory and distributed cyber systems. *International Journal of Cybersecurity Intelligence & Cybercrime, 2*(2), 44-59.

Carter, W. (2018). Extending Federal Cybersecurity to the Endpoint. In *Center for Strategic and International Studies.* Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181010_Carter_FederalCybersecurity_FINAL_WEB.pdf?H403CdzCrPL3Asbc8MDU84VxbcVm_jCC

Conteh, N. Y., & Royer, M. D. (2016). The rise in cybercrime and the dynamics of exploiting the human vulnerability factor. *International Journal of Computer (IJC), 20*(1), 1-12.

Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *computers & security, 26*(1), 73-80.

Krebs, C. (2019). 5G: The impact on national security, intellectual property, and competition. In *United States Senate.* Retrieved from https://www.judiciary.senate.gov/imo/media/doc/Krebs%20Testimony.pdf.

Lee, J. R., & Downing, S. (2019). An exploratory perception analysis of consensual and nonconsensual image sharing. *International Journal of Cybersecurity Intelligence & Cybercrime, 2*(2), 23-43.

Lee, S., Choi, K., Choi, S., & Englander, E. (2019). A test of structural model for fear of crime in social networking sites. *International Journal of Cybersecurity Intelligence & Cybercrime, 2*(2), 5-22.

Mylrea, M., & Gourisetti, S. N. G. (2017, September). Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In *2017 Resilience Week (RWS)* (pp. 18-23). IEEE.

Policht, M. (2019). Threat detection Planning for a secure enterprise. In *EdX.* Retrieved from https://www.edx.org/course/threat-detection-planning-for-a-secure-enterprise-3