International Journal of Cybersecurity Intelligence & Cybercrime

Volume 3 | Issue 2 Article 1

11-3-2020

Toward Mitigating, Minimizing, and Preventing Cybercrimes and Cybersecurity Risks

cybercrime, cybersecurity, prevention, assessment

Recommended Citation

Lee, C. S. (2020). Toward mitigating, minimizing, and preventing cybercrimes and cybersecurity risks. International Journal of Cybersecurity Intelligence and Cybercrime, 3(2), 1-3. https://www.doi.org/10.52306/03020120JOFX1754

IJCIC Center for Cybercrime Investigation & Cybersecurity

Toward Mitigating, Minimizing, and Preventing Cybercrimes and Cybersecurity Risks

Claire Seungeun Lee*, University of Massachusetts Lowell, U.S.A

Keywords; cybercrime, cybersecurity, prevention, assessment

Abstract:

Cybercrime and cybersecurity are emerging fields of research, shaped by technological developments. Scholars in these interconnected fields have studied different types of cybercrimes as well as victimization and offending. Increasingly, some of these scholars have focused on the ways in which cybercrimes can be mitigated, minimized, and even prevented. However, such strategies are often difficult to achieve in reality due to the human and technical factors surrounding cybercrimes. In this issue of the *International Journal of Cybersecurity Intelligence and Cybercrime*, three papers adequately address such challenges using college student samples and nationally representative samples, as well as a framework through which cybersecurity can be better managed. Theoretically speaking, these studies use traditional criminological theories to explore different types of cybercrimes and cybersecurity while enhancing our understandings of both. The issue is concluded with a book review of a work about computer crime that was published before the Internet age and offers useful insights for current and future cybercrime studies.

Introduction

In the emerging fields of cybercrime and cybersecurity, scholars have studied cases of cybercrime victimization and cybersecurity breaches, as well as the correlations between them. This current issue of IJCIC makes a contribution to the extant literature by shedding light on the prevention and assessment of cybercrime and cybersecurity, and by examining the often neglected and understudied yet important "canon" of cybercrime-related book reviews. This issue includes the following three articles on 1) the effects of self-control on the cybercrime victim-offender overlap, 2) the cyber-situational prevention of cybercrimes, and 3) developing a cybersecurity assessment for a technologized global public health domain, and closes with a book review of *Tales of Electronic Thievery, Embezzlement, and Fraud.*

*Corresponding author

Claire Seungeun Lee, Ph.D., School of Criminology and Justice Studies, University of Massachusetts Lowell, 113 Wilder Street, Lowell, MA, 01854, U.S.A.

Email: claire_lee@uml.edu

Overview

Brooke Nodeland's paper "The Effects of Self-control on the Cybercrime Victim-Offender Overlap" (2020, this issue) is a meaningful addition to the existing literature on the victim-offender overlap in cybercrimes, which is one of the areas currently growing within cybercrime studies. The author utilized a survey of American college students to explore how self-control affects cyber offending, cyber victimization, and the cyber victim-offender overlap. A low level of self-control is highly associated with cyber offending and cyber victim-offending, yet, by contrast, this is not the case with cyber victimization. The author also found that having a peer who exhibits deviant behavior plays an important role in the likelihood of another individual becoming involved in cyber offending, cyber victim-offending, and cyber victimization. This paper's results are important because one of the challenging tasks for researchers is finding ways to apply existing traditional criminological theories to the new realm of cybercrime.

The next paper, titled "Cyber-Situational Crime Prevention and the Breadth of Cybercrimes among Higher Education Institutions," written by Sinchul Back and Jennifer LaPrade (2020, this issue), examined a nationally representative dataset on cybercrime and cybersecurity in U.S. higher education institutions. The authors offer innovative insights through the framework of situational crime prevention. While the situational crime prevention theory is a well-known criminological theory, it is not often applied to cybercrime studies. In this paper, the authors used the theory convincingly to analyze the association between common cybersecurity measures, crime prevention activities, and cybercrimes. Their results show that cyber-SCP techniques of "target hardening, entry/exit screening, and reducing temptation" can be considered as preventive measures for cyber-threats as well. This paper has implications not only for the field but also for higher education institutions in America and elsewhere in mitigating cybersecurity threats and enhancing cybersecurity risks.

Next, Stanley Mierzaw and his colleagues' research, titled "Proposal for the Development and Addition of a Cybersecurity Assessment Section into Global Public Health Involving Technology" (2020, this issue), proposed cybersecurity assessment in the global public health realm. While cybersecurity for health domains has been discussed by media and academics anecdotally and on a case study basis, a relatively smaller body of cybersecurity research has used empirical evidence to analyze this cybersecurity health phenomenon. The author offered a framework for minimizing cybersecurity and information security risks for public, non-profit, and healthcare organizations. At the same time, he opened up the discussion on public health as a field warranting potential cybersecurity risks. Such discussions are highly important as we are all in the COVID-19 pandemic together.

Lastly, Brian Nussbaum offers a book review on one of the forgotten classics of cybersecurity, Whiteside's (1978) *Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud*. The author brings our attention to this book, which he argues is an important and valuable yet lesser-known resource in the fields of cybersecurity and cybercrime competing against the numerous recent books written by journalists and academics. While the field is changing rapidly with technological advancements, the author emphasized that we need to go back to basics. Interestingly, the book was set and published before the Internet age. Computer crimes described in the book can be linked to the later Computer Fraud and Abuse Act, among other legal measures.

Computer Capers gives us insights about not only types of attacks but also attackers' characteristics and their motives. In his book review, Nussbaum also links "old" computer crimes to recent cybercrimes and cybersecurity breaches. The book, as well as the book review, will be useful for researchers and students in the field, particularly those who were born after this book was published.

Concluding Remarks

Like universities and schools, public health institutions not only hold enormous value, but they also hold sensitive data on people's personal information, their social security numbers, family backgrounds, and biometrics. While datafication of such data itself may only pose concerns for a select few who highly value their privacy (Lee, 2019), datafication and data are, unfortunately, a gold mine for cybercriminals. This aggregated context that facilitates datafication makes the mitigation, minimization, and prevention of cybercrimes and cybersecurity risks even more difficult to tackle, underscoring the necessity of cybercrime and cybersecurity studies. In this vein, I cordially invite scholars in the fields of cybercrime and cybersecurity to read this issue and consider these papers in light of related themes, hopefully inspiring new insights and fomenting new scholarships for future issues.

References

Back, S. & LaPrade, J. (2020). Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions. *International Journal of Cybersecurity Intelligence and Cybercrime*, *3*(2), 25-47.

Lee, C. S. (2019). Datafication, dataveillance, and the social credit system as China's new normal. *Online Information Review*, *43*(6), 952-970.

Mierzwa, S., RamaRao, S., Yun, J. A., & Jeong, B. G. (2020). Proposal for the development and addition of a cybersecurity assessment section into technology involving global public health. International Journal of Cybersecurity Intelligence and Cybercrime, *3*(2), 48-61.

Nodeland, B. (2020). The effects of self-control on the cybercrime victim-offender overlap. *International Journal of Cybersecurity Intelligence and Cybercrime*, *3*(2), 4-24.

Nussbaum, B. (2020). Book review of Whiteside, Thomas. (1978) *Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud.* New York: Thomas Y. Crowell Company. *International Journal of Cybersecurity Intelligence and Cybercrime*, *3*(2), 62-66.

Whiteside, T. (1978). *Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud.* New York: Thomas Y. Crowell Company.