Article Review 1: Cybercrime and Its Social Implications

Mathieu Crosby
2/16/25

Introduction
Cybercrime has become a growing threat with significant social implications, impacting individuals, businesses, and governments. The article "Impact of Cybersecurity and AI's Related Factors on Incident Reporting Suspicious Behaviour and Employees Stress: Moderating Role of Cybersecurity Training" from the International Journal of Cyber Criminology (Muthuswamy & Esakki, 2024) explores the various factors contributing to cybercrime and its broader effects on society. This critique addresses how the article is relevant to the social science principles, states its research hypothesis and questions, describes the data analysis and methodology, and discusses its relevance to marginalized groups and society in general. It also connects the central ideas of cybersecurity covered in the Module 5 PowerPoint to the study conclusions.

Connection to Social Science Principles
Cybercrime is inherently linked to social science principles. Sociologically, the paper examines how social relationships and technological advancements shape cybercrime trends (Muthuswamy & Esakki, 2024). Psychologically, it examines why cybercrime occurs and the psychological and economic impacts on victims. Economically, the study uncovers how cybercrime expands economic disparities, particularly for individuals with limited access to cybersecurity resources.

Research Questions and Hypotheses
The study investigates several key research questions, including the primary factors driving cybercrime, its effects on different demographics, and potential mitigation strategies (Muthuswamy & Esakki, 2024). The hypothesis suggests that socio-economic status and digital literacy significantly influence one's vulnerability to cybercrime.

Research Methods and Data Analysis
For purposes of exploring such questions, this research employs mixed-methods design. Quantitative methods include statistical surveys that measure cybercrime offenses, while qualitative methods include law enforcement officer and victim interviews for deeper insights into enforcement challenges and victim effects (Muthuswamy & Esakki, 2024). Collection of data is both primary and secondary. Primary data comprises interview transcripts and survey responses, whereas secondary data consists of reports on the trends in cybercrime. The research employs regression analysis to determine statistical relationships as well as thematic coding for qualitative answers in order to have a thorough investigation of the effects of cybercrime.

Connection to Cybersecurity Concepts
The conclusions of the article are consistent with some of the ideas of cybersecurity in the CYSE201S Module 5 PowerPoint. Threat modeling is discussed in the context of the targeting

of certain groups by cybercriminals. Digital forensics is a central area of inquiry and countermeasures against cyber threats. Ethical hacking is presented as a preventive measure against cybercrime, while cybersecurity policies are tested for their capacity to reduce online threats.

Impact on Marginalized Groups

Marginalized groups are more affected by cybercrime due to economic and gender disparities. Poorer people lack cybersecurity awareness and defense mechanisms, and thus they are more vulnerable to attacks (Muthuswamy & Esakki, 2024). Women and LGBTQ+ people are also frequent targets of cyberbullying and identity theft. To combat these issues, targeted cybersecurity education and policy reform are required.

Contributions to Society

The study benefits society in a number of ways. It informs policymakers by providing data-driven recommendations on how to enhance cybersecurity policies and laws (Muthuswamy & Esakki, 2024). It also raises awareness among the general public since it teaches individuals about safe online practices, thus reducing their exposure to cyberattacks.

Conclusion

In conclusion, this article provides valuable insights into the complex reality of cybercrime and its social consequences. Through a systematic methodological procedure, the study highlights the importance of cybersecurity training and policy design, particularly among disadvantaged groups. Its findings underscore the necessity for continued research and preventive measures to combat cyber threats in an increasingly digitizing world.

References

Muthuswamy & Esakki, 2024. Impact of Cybersecurity and AI's Related Factors on Incident Reporting Suspicious Behaviour and Employees Stress: Moderating Role of Cybersecurity Training. International Journal of Cyber Criminology. Retrieved from https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/330/99