Article Review #1

Exploring the Psychological Profile of Cybercriminals: A Comprehensive Review for Improved Cybercrime Prevention

Kevin A. Loarca

Old Dominion University

CYSE 201S: Cybersecurity as a Social Science

Professor Woodbury

February 19, 2026

Article Review #1

The article written by the authors Trinh et al. explores several different topics in providing a comprehensive review of the research question of improvement in cybercrime prevention. The methodology used for this is a systematic review where the objective is to: provide a comprehensive analysis of cybersecurity crimes, examining their various types, impacts, and prevention strategies (Trinh et al., n.d., p.2). In addition, the article includes both technical and psychological aspects of cybercrime, which will aid in developing more effective policies, mitigating risks, and ensuring a more secure digital landscape (Trinh et al., n.d., p.2). The author's criteria are provided within the article to ensure relevance and quality of the studies. For example, the author lists a publication range of 2010 to 2023 to ensure relevance and recent advancements. In addition, the authors also exclude non-peer-reviewed sources, such as blogs or opinion pieces, to maintain focus and coherence of the review (Trinh et al., n.d., p.3). Examples of data and analysis done in the article are three case studies that the author provides context to, impact and consequences, response and mitigation, and the overall lesson learned from cyberattacks (Trinh et al., n.d., pp. 7-8).

The focus of the article aligns well with some of the principles of social sciences that were mentioned in class. These principles consist of objectivity, determinism, and relativism. Before starting the paper, the authors express objectivity as they avoid promoting an opinion and focus on an informative approach. This is seen in their search strategies and inclusion and exclusion of criteria. As for determinism, the authors mention a theory, known as Routine Activity Theory, which suggests crime occurs when three elements converge. These elements are a motivated offender, a suitable target, and the absence of capable guardianship (Trinh et al., n.d., p.5). The theory provides the explanation that cybercrimes are done by motivation rather

than by randomness. For relativism, its basic understanding is that all things are related in some way. To relate this principle to the article, it is shown how the impact of cyberattacks can affect several different areas that are related to the same conflict. For example, the first case study of Sony's security breach had financial, reputational, and political impact, which came from the data breach. The impact had an estimated $35 million for IT repairs and did not include lost revenue and legal costs (Trinh et al., n.d., p.7). The reputation of the company had raised concerns about their security practice as the attack leaked emails, revealing sensitive and embarrassing communications. As a response from the U.S. government, they would impose sanctions on North Korea, responsible for the attack (Trinh et al., n.d., p.7).

Discussed topics in class that relate to the article consisted of victim precipitation, cyberpsychology, the psychological profile, and Maslow's Hierarchy of Needs. For victim precipitation, this is seen in the second case study of Target's security breach. The company's behavior contributed to cyber victimization as they failed to consider third-party security access and maintain good network security (Trinh et al., n.d., pp. 7-8). The events were taken into consideration as they would secure third-party access and adhere to better security practices. Next, for cyberpsychology, the impacts of cyberattacks affect victims negatively. Attacks such as privacy breaches inflict significant emotional and psychological distress. Victims will experience anxiety, fear, and an extreme sense of vulnerability knowing the private information is in the hands of cybercriminals (Trinh et al., n.d., p.12). A psychological profile is seen with the third case study of the Colonial Pipeline Ransomware Attack of 2021. The cyber criminals disrespected legal norms and infiltrated the company's network to encrypt their data and demanded ransom payment. The attackers rebelled against symbols and authorities as the company would work closely with the FBI to investigate and recover from the breach. General

knowledge about the programs is included as they managed to break into the company's IT infrastructure and used software to encrypt data (Trinh et al., n.d., p.8). Lastly, Maslow's Hierarchy of Needs is seen through the actions of the attackers. The attackers in case study one showed physiological needs and safety needs as the group retaliated because Sony depicted the assassination of the North Korean leader. The stage of belongingness and esteem needs of the attackers is assumed to be a protective response towards their leader's reputation, as they were depicted in a violent death, which they found appalling. Lastly, self-actualization is seen when they accomplish their attack against Sony's infrastructure (Trinh et al., n.d., p.7).

The concern for marginalized groups can be impacted by cyberattacks mentioned in the article. Specifically, a privacy breach can affect marginalized groups such as low-income individuals or the elderly. Privacy breaches can expose individuals to identity theft, financial fraud, and emotional distress (Trinh et al., n.d., p. 12). An assumption about the two marginalized groups can be made. Attackers having their information could make it easier for the two to be susceptible to social engineering attacks. For low-income individuals, an attacker can take advantage of their financial situation and could trick them into giving them money. The elderly could be taken advantage of, as they may not be familiar with the technology that attackers may use. Overall, the article provides several societal contributions which are raising awareness in reducing human error and developing regulations. By educating employees in common cyber threats such as phishing and social engineering, they can recognize and respond to the threat (Trinh et al., n.d., pp. 14-15). This could reduce attacks, like the privacy breach, if they respond to the threat accordingly. As for developing regulations, the article emphasizes the importance of establishing legal standards for data protection, privacy, cybercrime prevention, and providing a basis for enforcing security measures (Trinh et al., n.d., p.15). By having these

regulations, it could reduce the chances of people's information being compromised, as companies would need to follow strict guidelines to implement appropriate security standards.

References

Trinh, D. T., Dinh, T. C., & Tran, T. N. (n.d.). Exploring the Psychological Profile of Cybercriminals: A Comprehensive Review for Improved Cybercrime Prevention. International Journal of Cyber Criminology. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/452/133