

Article Review:

Cyberattacks, Cyberthreats, and Attitudes Towards Cybersecurity Policies

Jestina Hill

Old Dominion University

Cybersecurity 201s: Cybersecurity and Social Science

Professor Yalpi

2 October 2024

Attitudes Towards Cybersecurity Policies

How did the Article Relates to the Principles of Social Science

Social science is described as the study of individuals or groups, including organizations, cultures, and economies, and their actions, both individual and collective (Bhattacharjee, 2012). Social sciences encompass areas including psychology, sociology, and economics (Bhattacharjee, 2012). Upon reviewing the text, I concluded that it pertains to social science through its examination of human behavior, policy formulation, and societal impact and trust. It illustrates the responses of individuals and their community to threats and the manner in which these are conveyed.

Researched Question and Hypothesis

This article examines cybersecurity priorities following lethal and nonlethal cyberattacks (Snider et al., 2021). There is a lack of research examining how various forms of cyberattacks impact different cybersecurity policies (Snider et al., 2021). Their emphasis was on the consequences of cyberattacks rather than the identity of the assailant or the categorization of the attack. The hypothesis posits that more exclusive cyberattacks will ultimately result in greater support for the adoption of cybersecurity measures compared to those involving broader threats.

Types of Research Methods Used

The employed study approach is a controlled survey experiment that presented participants with simulated television news reports regarding significant cyberattacks. Both groups completed pre- and post-surveys by responding to inquiries regarding their personal attitudes towards cybersecurity and pertinent sociodemographic characteristics (Snider et al., 2021). The participants were divided into three groups: the fatal condition, the nonlethal condition, and the control group, including a total of one thousand twenty-two individuals (Snider et al., 2021).

Types of data and analysis done

The information that was provided came from the participant surveys. It included the following three variables: the dependent variable, which supports cybersecurity policies; the mediator variable, which is threat perception; and the predictor variable, which was exposure to cyberattacks (Snider et al., 2021). Furthermore, gathered was the sociodemographic measure (Snider et al., 2021).

How Concepts from the PowerPoint Relates to the Article

The first thing that comes to me when I think of the modules is the CIA triad, which stands for confidentiality, integrity, and availability. This triad illustrates how the rules are organized to demonstrate that if we want to avoid the dangers, we need to make sure that we strike a balance between our privacy and our security. In addition to this, it utilized the research procedures including the research question, the variables, and the hypothesis. Through the utilization of those notions, the audience was provided with an awareness of how it influenced the field of cybersecurity.

How the Article Relates to the Challenges, Concerns, and Contributions of Marginalized Groups

In my view, this text does not explicitly address the objectives towards marginalized people, however it does contain some indirect references. However, groups may perceive themselves as targeted if they lack the necessary resources to mitigate the intrusions. It illustrates the extensive influence of cybersecurity regulations on individuals' privacy and civil liberties. Ultimately, the cybersecurity policies indicated that the excluded group was reticent to voice their opinions in certain discussions due to the prevailing views towards the policy, which was

Attitudes Towards Cybersecurity Policies

ostensibly more inclusive and considerate of their requirements. It enabled society to understand how the policy may be created to assist all groups effectively.

Overall Contributions of the Studies to Society

Through the use of cyberattacks, the articles demonstrate how the general public can influence the level of support for the cybersecurity policy. The greater the number of threats that individuals received, the more it demonstrated that people are eager to have more restrictions, even if it means that their privacy will be violated. It provides policymakers with a better understanding of how to build the policies for cybersecurity. Additionally, by highlighting the significance of the threat, the piece brought attention to the necessity of public awareness and education regarding matters pertaining to cybersecurity.

Conclusion

In conclusion of the article, Cyberattacks, Cyber Threats, and Perspectives on Cybersecurity Policies The society at large is vulnerable to cyber-attacks, prompting individuals to seek cybersecurity regulations. Media coverage of cyberattacks has shaped public opinion by leveraging facts to garner support for more rigorous cybersecurity policies (Snider et al., 2021). Overall, it indicates that the implementation of cybersecurity measures should take into account public views and vulnerability to cyber-attacks (Snider et al., 2021).

References

- Bhattacharjee, A. (2012). *Social Science Research: Principles, Methods, and Practices Social Science Research: Principles, Methods, and Practices*. Textbooks Collections. Retrieved September 30, 2024, from https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1002&context=oa_textbooks
- Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, 7(1). <https://doi.org/10.1093/cybsec/tyab019>