Article #1 Review:

Examining the Relationships Between Age and Company Size on Individual Attitudes towards Cybersecurity and Risky Cybersecurity Behaviors

Bailey Williams

Department of Cybersecurity, Old Dominion University

CYSE 201s: Cybersecurity and the Social Sciences

Prof. Diwakar Yalpi

October 1, 2024

This study examines the impact of employee age and company size on the frequency of risky cybersecurity behaviors displayed by employees, as well as employee attitudes toward cybersecurity endeavors.

Relation to the Social Sciences

The study is related to the social science principles of relativism, objectivity, and parsimony. The study practices the principle of relativism by examining how age and company size influence risky cybersecurity behaviors and attitudes toward cybersecurity. Researchers also maintained objectivity throughout the study by not allowing any predisposed biases toward age groups to impact their analysis. Finally, the hypotheses, described below, obey the principle of parsimony by seeking a simple explanation for employee's risky cybersecurity behaviors and attitudes towards cybersecurity (Yalpi, n.d.-a, pp. 4, 7, 9).

Research Hypotheses

The study had two hypotheses that were tested through separate surveys. The first hypothesis anticipated that a participant's attitude toward cybersecurity would be influenced by their age and the size of the company they work for. The second hypothesis anticipated that the frequency of a respondent's risky cybersecurity behaviors would be influenced by their age and the size of the company they work for (Hadlington, 2018, p. 272).

Research Methods

Participants were selected via an online survey administered to U.K. residents. The final dataset had 515 people, ranging from 18-84 years of age, who were all employed full- or part-time. After collecting demographic information, participants completed two questionnaires: the Risky cyber security behaviours scale (RScB) and the Attitudes towards cyber security in business (ATC-IB) scale. The RScB asked participants to rate how frequently they engage in different risky cybersecurity behaviors on a 5-point Likert scale. The ATC-IB asked participants to rate different statements based on their attitudes toward cybersecurity and

their perceived responsibilities for cybersecurity within their company on a 4-point Likert scale (Hadlington, 2018, pp. 272–273).

Research Analysis

Responses for each survey were analyzed by calculating the mean and standard deviation for each, based on the age group of the respondent and the size of the company they work for. There were significant differences in scores on the RScB between age groups (18-34 and 35+), as well as between company sizes (51-250 employees and 250+ employees), with younger employees admitting to participating in more risky behaviors. There were also significant differences in scores on the ATC-IB between age and company size groups, with older employees having a more positive outlook on cybersecurity (Hadlington, 2018, pp. 273, 276, 277).

Connections to Course PowerPoint Presentations

The PowerPoint presentations highlight the value surveys have for social science researchers. While these surveys rely on respondents to be truthful and objective when answering, they provide an important snapshot of the respondent's behaviors (Yalpi, n.d.-b, p. 8). The concept of using surveys to collect data from the target demographic is applied to this study by allowing researchers to analyze how individuals view their own cybersecurity attitudes and practices.

Applications for Marginalized Groups

While the study does not directly address marginalized groups, further application of the research could be used to identify differences in risky cybersecurity behaviors and attitudes towards cybersecurity between employee demographics. Assuming there is a significant difference between groups, this could provide insight into how to adapt cybersecurity training programs to address identified differences.

Societal Applications

This study contributed to society by providing a baseline for future studies to further examine the factors that contribute to an employee's cybersecurity behaviors (Hadlington, 2018,

p. 279). In addition, the study has identified age as a potential factor for cybersecurity behaviors, which may suggest that current cybersecurity training programs are not well-designed for younger employees. By making changes to these programs, organizations may reduce their risk of cybersecurity incidents.

Conclusion

In conclusion, this study provides a baseline for future research into how organizations can better address non-malicious insider cybersecurity violations. This research helped prove the idea that there is a relationship between age and company size when examining an individual's attitudes toward cybersecurity responsibilities and their own risky cybersecurity behaviors.

References

Hadlington, L. (2018). Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the united kingdom. https://doi.org/10.5281/ZENODO.1467909

Yalpi, D. (n.d.-a). CYSE201S (Module 2): Principles of Social Sciences and Cybersecurity Diversity and Cybersecurity.

Yalpi, D. (n.d.-b). CYSE201S (Module 3): Strategies to Study Cybersecurity through an Interdisciplinary Social Sciences Lens.

Link to Social Science Cybersecurity Study: https://doi.org/10.5281/ZENODO.1467909