Article Review #1:

Study of the Most Effective Ways to Measure the Success of Cybersecurity Awareness Programs

Katherine Billy

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

September 28, 2025

This paper is about a research study completed to help create a more standardized form of cybersecurity awareness programs (CSA) that are more effective in helping people understand common cybersecurity threats and steps they can take to protect themselves. The research was performed by Sunil Chaudhary, Vasileios Gkioulos, and Sokratis Katsikas. Their goal was to find out the best ways to test a person's understanding after they attend or read some type of cyber-awareness material. Most companies and organizations know that they need to inform their workers about how to stay safe while working with technology, however, there hasn't been much research done about what the best ways to inform them are or how to make sure they have understood the information once they have been informed. This is what these researchers strived to find out.

Study and the Principles of Social Sciences

Outside of this study's original goals, one thing that it helps to reiterate is the concept that cybersecurity is a social science. The whole reason that cybersecurity awareness programs are needed is due to the cybersecurity risks that people cause, which demonstrates the social science principle of relativism. This particular study helps by relating to the principles of social sciences in a number of different ways. The principle of objectivity is shown in how the authors of the paper did their research without immediately excluding academic papers simply because of their age or the methods in which they describe teaching cyber awareness. Parsimony can be related to this topic due to the authors' desire to simplify the creation of CSA programs. This study uses empiricism in its research through results that can be seen about the impact that CSA programs have on their employees. Lastly, these authors stayed skeptical and continued to do further research as to why some of the methods of cybersecurity awareness teaching and testing work better than others.

Study's Elements

This was an exploratory study with the goal of finding out how to best determine how effective a cybersecurity awareness program is. Therefore, the question in hand is: what are the best methods for determining the comprehension of a CSA program? Due to the nature of this study and the vast number of variables, there is no specified hypothesis within the paper. The main independent variable is the method in which comprehension of the CSA material is obtained, and the second variable that is being changed, even though it is not the main focus of this study, is the type of education method. The dependent variable in this study is how well the information is understood.

Research Methods Used

The type of research method that took place within this project was archival research. The authors of the paper collected 78 academic papers that they painstakingly narrowed down to the final 32 papers that they then collected their research from (Chaudhary, Gkioulos, & Katsikas, 2022). Within these papers, contained numerous different types of research regarding how they examined how well the people receiving the cybersecurity awareness training retained and understood the information. Some of the many types of assessments involved surveys, tests (both question style tests and surprise simulation tests), observation of participants' attitude and engagement, and levels of attendance or viewing (Chaudhary, Gkioulos, & Katsikas, 2022).

Data and Analysis

A majority of the data involved in this study was actually qualitative data. The authors described how previous people who have tried to gather data on how well an audience understands a CSA program tend to have focused on quantitative data because they believed it to

be desirable for executives attempting to calculate the return on investments for these programs. While they do believe quantitative data to be important in this situation, they argue that qualitative data is equally as important. This is especially due to this being a topic pertaining to people and how they learn. They use quantitative data like test scores, attendance rates, and number of security incidents before vs after the training and qualitative data such as observation of participants' behavior, feedback, and surveys (Chaudhary, Gkioulos, & Katsikas, 2022).

How the Study Relates to Class Topics

There are countless class topics that can be connected to the topics in this study. For one, the whole point of this research paper is to improve cybersecurity awareness programs which act as a preventative measure for reducing cybercrime. This also relates to the topic of the "human factors" which is the cause for most cyber risks. Cybersecurity awareness programs use victim precipitation to help understand what types of risks need the most coverage in order to help prevent them in the future. Another class topic that relates to this study is the matter of victim behaviors as well as the risks some people may take in terms of cybersecurity due to optimism bias and low observability. Lastly, while most CSA programs are meant to help protect people while working for a company or organization, their goal is to prevent cyber victimization and therefore the psychological consequences of victimization as well.

How the Topics in this Study Relate to the Challenges, Concerns, and Contributions of Marginalized People

The issue that led to this study was that there were no standardized forms of cybersecurity awareness programs, with little to no information out there about how to create an effective one. This may not have been too big of an issue for companies or organizations with the

money to spend on different types of awareness programs and examination practices, but for smaller companies and organizations, or even perhaps underfunded public-school systems, this could have caused some serious issues. Without the knowledge and money required to create an effective CSA program, smaller companies and programs would be at a greater risk of falling victim to common cyber threats purely do to those involved not being able to be informed about what to look out for and safety measures they can take to stay safe. Part of what this study hoped to achieve though finding what methods of cyber awareness education work the best, was to improve the availability of CSA programs for all people and all companies no matter their financial capabilities.

Contributions of this Study to Society

This study helps to contribute to society in a few different ways. It works to streamline cybersecurity awareness programs helping to identify which educational forms and testing methods are most efficient and effective. Through this, it would also help to make these programs more accessible and cost efficient. This study was conducted in order to improve these CSA programs so that more people can stay safe while using technology and working on the internet.

Conclusion

No matter what, cybersecurity awareness programs will continue to require updating as technology and cyber risks both evolve. However, this study worked to improve the format of said CSA programs so that they are more effective in educating people on how to prevent becoming the victims of cyber-attacks. This study acts as yet another argument for why cybersecurity is a social science. While this study is not about why CSA programs are needed, it

does briefly discuss that their importance is mostly because one of the greatest risks in cybersecurity is the human factor. The authors of this study researched the different methods of CSA education and the ways in which the understanding of those programs was tested in order to determine the best course of action for the people creating these programs.

Works Cited

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity*, 19.

Web link: https://academic.oup.com/cybersecurity/article/8/1/tyac006/6590603?searchresult=1