Article Review #2: Developing metrics to assess the effectiveness of cybersecurity awareness program

Logan Gutierrez

Old Dominion University

CYSE 201s: Cybersecurity and the Social Sciences

November 14th, 2025

Professor Diwakar Yalpi

Overview

This article examines how organizations evaluate the effectiveness of cybersecurity awareness programs. Through a literature review of 32 studies, the authors find that most programs rely on self reported surveys and knowledge tests, while fewer measure real world changes such as phishing or password habits (Chaudhary et al., 2022). They argue that cybersecurity improvement requires standardized metrics that focus on actual user behavior, rather than attitudes. The article provides new ways for evaluating awareness programs and shows the need for behavior based assessments.

Relation to Social Science

This article relates to many of the social sciences, including psychology, sociology, and behavioral science. Cybersecurity behavior like clinking random links, adopting risky habits, or following security instructions are all human behaviors shaped by attitude, knowledge, culture, and even social norms. By focusing on knowledge, attitudes, and behavior change, the authors form social science themes such as risk perception and behavioral changes(Chaudhary et al., 2022). The authors also argue that cybersecurity cannot fully be understood through technical measures alone, as human factors must be taken into account.

Research Question, Hypothesis, Variables

The article has three implied research questions: what types of metrics are currently used in cybersecurity awareness evaluations, how effective are these metrics at capturing behavior change, what gaps exist in the current evaluation methods (Chaudhary et al., 2022). The authors do not state a clear hypothesis, but it does imply that existing evaluations overdo subjective and knowledge based metrics while underusing behavioral ones. The independent variable is a type

of awareness metric including knowledge, attitude, behavior and so on. The dependent variable is the effectiveness of the cybersecurity awareness programs

Research Methods and Data and Analysis

The authors use a systematic literature review of 32 papers that evaluated cybersecurity awareness programs. In order to do so, they performed a literature review initially identifying approximately 350 papers from Google Scholar and 400 from Microsoft Academic (Chaudhary et al., 2022). The data that was collected is from prior research findings, evaluation factors used in those studies, and metrics of them. The analysis involved extracting what was measured and how from selected studies. This approach relies on content analysis, which allows the authors to identify patterns used in other studies. The authors also mapped these findings to a framework based on European Literacy Policy Network's four indicators, that are impact, sustainability, accessibility, and monitoring (Chaudhary et al., 2022).

Relation to Course

This article also connects to the coursework in CYSE 201s. The article treats cybersecurity as a human centered and social issue, not just a technical one. The authors highlight that human factors are the weakest link in cybersecurity, which reflects the coursework as it focuses on how human behavior and social systems affect security outcomes (Chaudhary et al., 2022). It goes over psychology, sociology, and organizational behavior involved with cybersecurity that relates to the course.

Relation to Marginalized Groups

The article does not talk about marginalized groups but can be implied. Marginalized groups like people with disabilities, non-english speakers, or even low income individuals can be faced with many cybersecurity risks. These groups may not have the resources to learn or

understand cybersecurity risks. Making awareness programs that account for differences can help reduce risks.

Contributions to Society

The article helps organizations and society by proposing a framework that aims to improve how awareness programs are assessed, stating that “Without a proper evaluation, a mature CSA program is presumably unachievable” (Chaudhary et al., 2022). Awareness programs can reduce human related errors, protecting information and supporting cybersecurity. It also helps with academic research by finding gaps and building a foundation for future studies.

Conclusion

In conclusion, the article shows that cybersecurity awareness is a human and social issue that requires evaluation to be effective. By finding gaps in assessments and making frameworks, the authors show how organizations can help deal with human errors and long term impacts. In order to improve security, people must be understood too, not just technology.

References

Sunil Chaudhary, Vasileios Gkioulos, Sokratis Katsikas, Developing metrics to assess the effectiveness of cybersecurity awareness program, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac006, https://doi.org/10.1093/cybsec/tyac006