**Article Review 1**

Michael Opoku-Arthur

CYSE 201s

Dr. Armistead

September 27, 2023

**Article 1:** Developing Metrics to access the effectiveness of Cybersecurity Awareness Programs

This article begins with the statement, “Cybersecurity is not just about technology, but it also includes the people who interact with technology and are responsible for properly implementing and operating it.” (Chaudhary et al., 2022)**.** As I read this statement, I felt that it summed up what this course has been teaching us so far- that Cybersecurity is an interdisciplinary field comprised of many different components.

This article focuses on Cyber Security Awareness, which can be defined as knowing risks and behaviors that could potentially damage systems, data, and other information. When educated on cyber awareness, users protect themselves, their employer, and any other confidential information. There are programs called CSA Programs that educate users on cyber knowledge; the goal is not to put a person through in-depth training but to allow them to learn the foundation. As technology constantly evolves, so will CSA Awareness Programs; these programs will constantly need to be improved and updated to keep up with the times. This article mentioned that there were many methods for evaluating CSA Programs, but the researchers wanted to show the correct methodologies for evaluating a CSA Program to determine its effectiveness. The goal was to examine every paper (32 total papers) on CSA programs and create a method that would “make the evaluation process of CSA program as inclusive, complete, and unbiased as possible and, more importantly, make it replicable so that everyone should be able to conduct the same evaluation and get similar results” (Chaudhary et al., 2022). Making a universal evaluation like this would have to be **parsimonious** to allow all cyber professionals to understand and utilize it for assessing their programs.

As stated previously, this research aimed to come up with the correct approach to evaluating CSA Programs. The scientists measured “the factors to be measured” and their “measuring methods” (Chaudhary et al., 2022)**.** After reviewing papers, factors used in other CSA Programs were noted. The factors measured were behavior (measuring the behavior of an individual after participating in the CSA program), attitude (looking for positive changes in attitude after participation), knowledge and competence (measuring the retention of information after participation), interest (measuring how an individual interacts while participating in the programs), reachability (making sure to reach the target audience), touchability, value-added, usability, and overall feedback (recording audience feedback). Various data collection methods were used to measure these factors; surveys (pre and post) and observation were performed to examine the attitude, interest, reachability, and touchability. Usability and value-added would be examined through data collection. Cyber professionals could also conduct simulated attacks and scenarios to test the intelligence and performance of their employees to examine behavior and knowledge. Through the examination, knowledge, attitude, and behavior were the most commonly evaluated factors, and the common methods were surveys, tests, and passive data, with Surveys being used in 26 papers (over ¾ of all research papers).

To conclude, it was noticed that the evaluation of CSA programs is necessary after implementation to note “how effective and successful the program was” (Chaudhary et al., 2022). Before the article, there was no universal consensus on how to evaluate a CSA Program; because of this, the writers reviewed 32 past studies and decided to create a consensus that comprised all the same information included in each study. Testing a CSA Program should be broken into different indicator categories. The first was the impact indicator; in this stage, the positive changes in cybersecurity knowledge attitude and behavior are measured. Next is the Sustainability indicator; in this stage, you measure the changes in policies, framework, and organizational arrangement after CSA. This is followed by Accessibility, which measures the “relevancy of topics, quality of materials, and appropriateness of delivery channels using methods like surveys, the percentage of relevant topics covered, and statistical analysis of relevant passive data like audience interest in the awareness program.” Lastly was the Monitoring indicator, which measures interest and participation in the CSA Program. Through thorough research, the writers believed they had created the best measurement system for evaluating CSA Programs. Not only did they create a metric that all could use, but they also helped narrow down all the different methods into one.

As I sat and reflected on this article, I thought about how I could relate this in a social science lens. This article takes a psychological approach to Social Science, emphasizing studying human behavior and interaction to improve Cybersecurity Awareness. Once again, it reminded me that Cybersecurity is not just technology but all other disciplinary factors that tie into the field. When I think of CSA Programs, I instantly think back to Maslow’s Hierarchy of Needs; companies want to emphasize their safety needs, ensuring that the best steps are implemented to enforce security and safety. Not only do we need to put the steps into place, but we also need to constantly update, evaluate, and engage in CSA Programs so that we are well protected in this cyber-dominant world in which we live. I believe that this article has done a great job of describing that.

**References**

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022, May 23). *Developing metrics to assess the effectiveness of cybersecurity awareness programs*. Journal of Cybersecurity, Volume 8, Issue 1. <https://doi.org/10.1093/cybsec/tyac006>