Deshanta Kearney

Article 1 Review

Cyse 201S

Developing Metrics to Access the Effectiveness of CSA

Developing metrics to assess the effectiveness of cybersecurity awareness program (CSA) relates to the principles of social science because the goal of the CSA is to measure the changes in the security awareness, attitude, and behavioral changes of people in the cybersecurity field. Understanding social science and how it can influence human behavior is an advantage to companies in order to grow and maintain a strong security infrastructure that reduces risks.

Raising security awareness is important when managing human factors. The CSA program target is to transform things that are learned into practice. Ideally, providing employees with resources and the right information will convince them to make the right choices. Unfortunately, providing standards and implementing mandatory trainings isn’t enough to assume employees will make the right decisions if they are told the right thing to do. Transitioning into finding ways to capture employees’ attention, motivating them to use security measures, and driving them to understand the importance of cybersecurity is Beneficial. Also, knowing that cyber risks and cyber threats challenge vulnerabilities is important. Communicating the information needed for security should be presented in a way that employees will develop a level of motivation to act when involved in unusual situations. Focused attention will distinguish interest, increase cognitive functioning, and persistent effort.

The CSA program can be unique and adjusted to each target group depending on a clear goal and objective. Evaluation checks the interest of awareness by the audience and identify other topics that’s interesting to learn about. Surveys, tests, passive data, face-to-face interaction, and observations are methods used for evaluation by the researchers. The questions used has effective meanings, doable suggestions, useful messages, and concise presentations. The author used charts to display such. This will determine if the message persuades or push away the recipients. Several measured factors have their respective measurement methods. Behavior factors are measured by an intrusive method such as questionnaire-based surveys, face-to-face meetings, semi-structured interviews, and group discussions. It is also measured by a non-intrusive method which is pre- and post-attacks where the responses to phishing emails is counted and silently observing compliance.

Behavior factors will either demonstrate what was learned through practice or avoidance to showing it. Attitude factors are also measured by questionnaire-based surveys through an intrusive method. Attitudes can either have a negative effect or a positive effect towards security. The effectiveness of a CSA program was collected by factors measured. Improvement in the behavior of cybersecurity reduced risky behavior, promotion of best practices with safe behavior, positive effect, and intended change. The attitude of the audience resulted in improvement in adaptability, willingness to learn about cybersecurity, and intentions to make positive changes. Cybersecurity knowledge and competence has gained and improved in learnability. Value has been added by the CSA which includes time and cost-saving.

I agree with the author of this article and the emphasis on including a CSA program and effective metrics for improvement. The article also relates to marginalized groups including those who interact with technology and who are responsible for properly operating it.

<https://academic.oup.com/cybersecurity/article/8/1/tyac006/6590603?searchresult=1#387384152>