Towards A Comparison of Training Methodologies on Employee’s Cybersecurity Countermeasures Awareness and Skills in Traditional vs. Socio-Technical Programs

Jodi Goode
Nova Southeastern University, jp1587@nova.edu

Follow this and additional works at: http://digitalcommons.kennesaw.edu/ccerp
Part of the Information Security Commons, Management Information Systems Commons, and the Technology and Innovation Commons

http://digitalcommons.kennesaw.edu/ccerp/2016/Student/2
Abstract
Organizations, which have established an effective technical layer of security, continue to experience difficulties triggered by cyber threats. Ultimately, the cybersecurity posture of an organization depends on appropriate actions taken by employees whose naive cybersecurity practices have been found to represent 72% to 95% of cybersecurity threats and vulnerabilities. However, employees cannot be held responsible for cybersecurity practices if they are not provided the education and training to acquire skills which allow for identification of security threats along with the proper course of action. This work-in-progress study addresses the first phase of a larger project to empirically assess if there are any significant differences on employees’ cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) based on the use of two security education, training, and awareness (SETA) program types (traditional vs. socio-technical) and three SETA delivery methods (face-to-face, hybrid, & online). In the first phase, a panel of subject matter experts (SMEs) will review SETA program topics and the measurement criteria for CCA and CyS per the Delphi methodology. The SMEs’ responses will be incorporated into the development of two SETA program types with integrated vignette-based assessment to be delivered via three methods.

Disciplines
Information Security | Management Information Systems | Technology and Innovation
SUMMARY

Concern over cybersecurity breaches continues to grow as organizations gain a greater understanding of the financial impact, loss of company information assets, and harm to business reputation that can transpire from cyber threats. Employees’ naive cybersecurity practices have been found to represent 72% to 95% of cybersecurity threats and vulnerabilities to organizations. This revelation has initiated research concentrated on technological solutions to secure systems, motivation of attackers, profile aspects, and loss which can result from the impact of breaches. However, focus on technical aspects alone against cyber threats is not enough. Organizations, which have established an effective technical layer of security, continue to experience difficulties triggered by cyber threats.

As technology becomes increasingly critical for achieving business objectives, state of the art security systems can provide a false sense of protection to organizations. Research must encompass the human-centric lens, as employees are often the potential targets or unintentional facilitators in cyber-attacks. Previous research has found raising employee awareness of security policies, as well as the implementation of security education, training, and awareness (SETA) programs to be beneficial in mitigating cybersecurity threats. SETA programs can be used to empower employees, who are often cited as the weakest link in information systems security due to limited knowledge and lacking skillsets.

This study will seek to address the lack of theoretically grounded empirical studies related to the design and effectiveness of SETA programs and will explore the differences in cybersecurity countermeasures awareness and cybersecurity skill based on SETA program type and delivery method. The first phase of this work-in-progress study will develop a validated measurement tool to properly assess the cybersecurity countermeasures awareness and cybersecurity skill level of employees due to the limitations of construct measurement in previous research. To address this need, the first four specific research questions of this work-in-progress study will focus on use of the Delphi methodology to determine subject matter experts’ approved measurement criteria for cybersecurity countermeasures awareness and cybersecurity skill, as well as the development of two SETA programs with integrated vignette-based assessment. Additional research questions and hypotheses will be addressed in the second and third phases of the study which are considered future research.