Journal Article Review

Article Title:
Security Education, Training, and Awareness Programs: Literature Review

Authors:
Siqi Hu, Carol Hsu, Zhongyun Zhou (Tongji University, Shanghai, China)

Publication:
Journal of Computer Information Systems, Volume 62, No. 4, Year 2022, Pages 752–764

DOI/URL:
https://doi.org/10.1080/08874417.2021.1913671

Selected Topic:
Security Training and Awareness Programs for Development Teams

Background

In an effort to maintain information security and mitigate the growing complexity of cyber threats, many organizations have implemented Security Education, Training, and Awareness (SETA) programs as part of their security governance strategies. These programs aim to enhance employees' knowledge and awareness—especially those in software development teams—about the importance of security in all aspects of their work. However, despite widespread adoption, the effectiveness of SETA programs is often questioned. One of the main challenges is the lack of deep, systematic understanding of how these programs actually influence employee attitudes, behaviors, and actions related to information security in the workplace. Many initiatives are carried out as mere formalities, without considering the psychological and organizational factors that support behavioral change. Therefore, a scientific approach through a comprehensive literature review is necessary to identify success patterns, implementation challenges, and key characteristics that make SETA programs truly effective. This study responds to that need and aims to provide valuable insights for organizations to design and implement targeted and impactful security training.

Research Objectives

This study aims to conduct a systematic literature review of 80 scholarly articles published between 1998 and 2020 that specifically examine Security Education, Training, and Awareness (SETA) programs. Through this comprehensive review, the authors seek to uncover and analyze the core characteristics of SETA initiatives, explain the mechanisms through which these programs influence employee behavior, and identify the key conditions and supporting factors that determine the success of SETA implementation. By understanding these elements, the study aspires to provide a strong conceptual and practical foundation for organizations to develop more effective and sustainable security training strategies.

Methodology

The research employs a **systematic literature review** approach, focusing on 80 peer-reviewed articles relevant to the topic of SETA. These articles were selected based on specific criteria such as thematic relevance, publication quality, and contributions to the field of information security. A thorough analysis was conducted to identify key findings from each study, evaluate existing research gaps, and formulate the factors that influence the success or failure of SETA programs within organizational settings. This method aims to construct a more structured and comprehensive understanding of security training effectiveness for both software development teams and general employees.

Key Findings

1. **Low Effectiveness of SETA Programs:**
   Only a small number of information security professionals consider the SETA programs in their organizations to be truly effective in changing employee behavior toward security.
2. **Lack of Understanding of SETA's Impact:**
   Many organizations do not fully comprehend how SETA programs affect employees' beliefs, attitudes, and intentions concerning information security.
3. **Need for a More Systematic Approach:**
   A more structured and evidence-based approach is needed in designing and evaluating SETA initiatives to ensure that the training programs have meaningful, long-term impacts and can foster a sustainable security culture in the workplace.

Relevance to Security Governance

This study provides a valuable contribution to the field of information security governance, especially in the area of developing more targeted and effective security training programs. By identifying the various factors that influence the success of SETA initiatives, organizations can design training strategies that are not only informative but also capable of driving positive behavioral change among employees. Well-designed training programs can strengthen the organization's security culture, increase awareness of potential risks, and help minimize long-term threats to information security in a sustainable manner.