Abstract

Purpose: The aim of the study was to assess the influence of cybersecurity training programs on employee behavior in corporate environments in Kenya.

Methodology: This study adopted a desk methodology. A desk study research design is commonly known as secondary data collection. This is basically collecting data from existing resources preferably because of its low cost advantage as compared to a field research. Our current study looked into already published studies and reports as the data was easily accessed through online journals and libraries.

Findings: The research demonstrated that comprehensive training initiatives positively impacted employees' cybersecurity awareness and adherence to best practices. These programs not only increased knowledge of potential threats but also instilled a sense of responsibility among employees regarding their role in safeguarding sensitive information. Moreover, the study highlighted the importance of continuous reinforcement and practical application of learned skills in real world scenarios to ensure long-term behavioral changes. Additionally, the effectiveness of training was found to be contingent upon the program's relevance, engagement strategies, and integration with organizational policies. Overall, the findings underscored the critical role of cybersecurity training in mitigating risks and fostering a culture of security within corporate settings.

Implications to Theory, Practice and Policy: Social learning theory, protection motivation theory and cognitive dissonance theory may be used to anchor future studies on assessing the influence of cybersecurity training programs on employee behavior in corporate environments in Kenya. Develop personalized training modules tailored to individual roles and risk profiles within the organization. Advocate for regulatory mandates requiring organizations to implement regular cybersecurity training programs for employees.