ABSTRACT

With the rapid development of digital technology, Bank X has implemented various innovations such as mobile banking, internet banking, and digital payment solutions to meet the diverse needs of its customers. However, on the internal side of the bank, this greater reliance on digital platforms also brings a higher risk of cyber threats. The issue of cybersecurity among employees is becoming increasingly important, given that the human factor is often the main cause of cyberattacks in an organization. In addition, many previous studies have focused more on the cybersecurity aspects of customers, while the role of employees as managers and those responsible for customer data and company assets is often overlooked.

This research focuses on analyzing the factors that influence cybersecurity awareness and attitudes and their impact on employee protective behaviors at Bank X, which is a representation of three large state-owned banks in Makassar, Indonesia. This research examines various factors that influence employees' cybersecurity compliance attitudes and behaviors, including perceived barriers, self-efficacy, and response efficacy, which contribute to their decision-making process in safeguarding information. In addition, the research also explored the effectiveness of cybersecurity awareness programs, such as the SETA program, and the implementation of comprehensive cybersecurity policies within banks. These factors are critical in shaping employees' understanding of security protocols and motivating them to engage in protective behaviors to mitigate potential cyber threats.

This study utilized a quantitative methodology where primary data was collected using a survey questionnaire distributed to employees of the three state-owned banks in Makassar. The collected data were then analyzed using the Partial Least Squares Structural Equation Modeling (PLS-SEM) approach. Through this approach, measurement validity and structural equation models are comprehensively assessed. The results of this study aim to provide valuable insights into improving cybersecurity practices in the banking sector, specifically by encouraging employee protective behavior. By understanding how factors such as policy provisions, SETA programs, and cybersecurity awareness impact compliance and security attitudes, this study contributes to the development of strategies that strengthen banks' defense mechanisms against cyberattacks. The findings are expected to serve as a model for other financial institutions in Indonesia and abroad to enhance their cybersecurity culture and ensure the integrity and security of their digital infrastructure.

Keywords: cybersecurity awareness, cybersecurity behavior, cybersecurity compliance attitude, protective behavior