ABSTRACT

In the era of digital transformation, information security is a major challenge for the banking sector in Indonesia. Digital technology adopted by banks creates operational efficiency and improves service quality, but on the other hand opens up opportunities for cyber threats such as phishing, ransomware, and malware. One concrete example is the cyberattack that paralysed Bank Syariah Indonesia (BSI) in May 2023, resulting in financial service disruption and customer data leakage.

In addition to maintaining operational continuity, bank employees also have an important responsibility in protecting customers' personal data, which is vulnerable to misuse. The low level of employee awareness, training and understanding of information security practices is one of the factors that increase the risk to data security. As the first line of defense for ensuring the security of data and banking systems, it is crucial to assess the elements that affect bank employees' information security behavior.

This investigation intends to analyze the elements—password management, infrastructure security management, email management, organizational security policy, organizational support and training, and perception of security—that impact the information security behavior of Indonesian bank employees. The Theory of Planned Behavior (TPB), which explains how three primary factors—attitudes toward behavior, subjective norms, and perceived behavioral control—influence human behavior, is the theory that is employed.

This study uses a quantitative methodology with a questionnaire survey approach to bank employees in Indonesia with a sample of 258 respondents. Data analysis uses the Partial Least Squares-Structural Equation Modeling (PLS-SEM) method with the help of SmartPLS software.

The findings show that five of the six independent variables significantly influence information security behaviour. These variables include password management, infrastructure security management, email management, and organisational support and training, and perception of security. Meanwhile, organisational security policies showed no significant impact.

Keywords: *information security, digital transformation, employee behaviour, password management, organisational security policy, SmartPLS.*