ABSTRACT

The development of digitalization has encouraged the government sector to adopt information technology in various work processes and public services. However, this advancement also brings new challenges, particularly in the form of cybersecurity threats. Several hacking cases targeting government agencies indicate a low level of awareness regarding the importance of information security among employees. This condition negatively impacts public trust and threatens the safety of strategic national data.

This study aims to analyze the influence of information security management on employees' cybersecurity behavior in government institutions. The research focuses on several factors, including infrastructure management, organizational policy, support and training, password management, email management, and security perception. The research was conducted on employees of the Bandung City Government, specifically those working in the Department of Communication and Informatics and the Department of Population, Civil Registration, and Human Resource Development.

A quantitative approach was used with a survey method. Data were collected through questionnaires and analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM), which allows for comprehensive analysis of relationships between variables and produces relevant results. The findings show that most variables have a significant impact on cybersecurity behavior. Three key factors—Infrastructure Security Management, Password Management, and Email Management—are proven to encourage safer behavior when using information systems.

This study provides practical insights for government agencies in developing strategies to raise information security awareness. It is recommended that agencies strengthen infrastructure security management, improve employee education regarding secure password practices, and provide regular training to recognize and prevent email-based threats such as phishing. Future research can be conducted in other institutions with a larger sample size to obtain more generalizable results.

***Keywords**: Cybersecurity, Information Security Awareness, Data Leakage, Government, Cyber Threats, Information Security Management.*