ABSTRACT

Cybersecurity has become a critical issue in the digital era, especially for Indonesia, which faces various cyber threats such as ransomware and trojans. This study aims to identify key parameters for measuring the cybersecurity maturity level of organizations using the Best-Worst Method (BWM) as an evaluation approach. The methodology integrates various frameworks, including COBIT 2019, the NIST Cybersecurity Framework (CSF), MITRE ATT&CK, and others, to develop a comprehensive cybersecurity readiness assessment tool. The framework developed in this study encompasses four main aspects: Data security, Application and endpoint security, Network and perimeter security, and the Human layer. Through BWM-based evaluation, the proposed framework provides strategic guidance to enhance organizational cybersecurity preparedness. The findings demonstrate that the framework is capable of offering actionable insights for improving cybersecurity readiness across organizations. The results of this study contribute to the development of proactive mitigation strategies and the improvement of cybersecurity risk management in various industries. The proposed cybersecurity readiness framework is expected to serve as a guideline for organizations to identify security gaps, prioritize mitigation efforts, and design effective strategies to address cyber threats. Furthermore, the framework is designed to be adaptable across various sectors, including government, healthcare, education, and financial industries, which have diverse cybersecurity needs.

Keywords - Cybersecurity, Maturity Level, Best-Worst Method, Integrated Framework, Data security