ABSTRACT

Website risk management at PT XYZ faces various problems that can affect the sustainability of its operations. There are possibilities that can occur in the results of website penetration, namely DoS/DDoS attacks, Phishing, Malware, Ransomware, and SQL Injection. To overcome these problems, this study uses the ISO 31000:2018 framework as a guideline in the risk management process, which provides a systematic approach to identifying, assessing, and managing risks with the aim of minimizing negative impacts. The results of the implementation of this framework show comprehensive solutions, such as the implementation of a Web Application Firewall (WAF) to protect against DoS/DDoS and SQL Injection attacks, the implementation of antivirus and anti-malware to prevent malware infections, and routine data backups and periodic cybersecurity checks to reduce the risk of ransomware and other cybersecurity threats. The results of the analysis provide a solution for PT XYZ, because it allows the company to better understand the various possible risks and determine appropriate handling actions, thereby increasing the operational resilience of the company's website and reducing the potential losses that may arise from these risks. The implementation of the ISO 31000:2018 framework is expected to provide long-term benefits for companies in maintaining the integrity, security, and availability of the information systems used.

Keywords: Cybercrime, ISO 31000:2018, Risk Management, Penetration, Website.