

Cybersecurity Vulnerabilities in Digital Business: Challenges, and Novel Directions for Resilience

Vinsent Brilian Adiguna^{1*}, Sekar Farahdila², Rona Rachel³

¹*Faculty Economics and Business, Universitas 17 Agustus Semarang, Indonesia,
vinsentbrilian@untagsmg.ac.id*

²*Faculty Economics and Business, Universitas 17 Agustus Semarang, Indonesia,
sekarfarahdila@gmail.com*

³*Faculty Economics and Business, Universitas 17 Agustus Semarang, Indonesia,
ronacahyani21@gmail.com*

Abstract

Digital transformation increases cybersecurity vulnerabilities that threaten organizational resilience and stakeholder trust. This study analyzes cybersecurity vulnerabilities in digital business through a review of current open access literature. Findings reveal 89% of companies experience web application vulnerabilities, 93% have hosting misconfigurations, and 46% of employees reuse breached passwords. Artificial Intelligence (AI) exacerbates threat sophistication but offers resilience strategies through advanced detection and dynamic risk management. Case studies of SAP NetWeaver zero-day exploitation (CVE-2025-31324) and zero-trust architecture implementation demonstrate the effectiveness of AI-based threat mitigation. The research recommends integrating AI-driven cybersecurity tools, enhancing supply chain security, and developing cyber-aware organizational cultures to maintain business resilience against increasingly complex cyber threats. The study emphasizes cross-disciplinary approaches integrating technology, business strategy, and human factors as essential for sustainable cyber resilience in digital business environments.

Keywords: cybersecurity vulnerabilities, digital business, cyber resilience, AI-driven security, zero-trust architecture.