Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 4 No. 3 (2025) pp: 8108-8114
P-ISSN: 2963-9298, e-ISSN: 2963-914X

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

Vinsent Brilian Adiguna, Sekar Farahdila Inabah, Rona Rachel
Faculty of Economics and Business, Universitas 17 Agustus 1945 Semarang, Indonesia
vinsentbrilian@untagsmg.ac.id, sekarfarahdila@gmail.com, ronacahyani21@gmail.com

Abstract

Digital transformation has profoundly reshaped business ecosystems by embedding advanced technologies into operations, customer engagement, and decision-making processes. However, this transformation simultaneously amplifies cybersecurity vulnerabilities that endanger organizational resilience, data integrity, and consumer trust. This study provides a comprehensive analysis of cybersecurity vulnerabilities in digital business environments based on an extensive review of open-access literature and real-world case studies. The findings indicate that 89% of companies face web application vulnerabilities, 93% experience hosting and configuration issues, and 46% of employees reuse breached passwords—revealing persistent weaknesses in digital infrastructures. These vulnerabilities result in financial losses, reputational damage, and regulatory non-compliance that may threaten long-term business continuity. Artificial Intelligence (AI) has emerged as both a catalyst for advanced cyberattacks and a strategic defense enabler. AI-driven threat intelligence, anomaly detection, and automated response mechanisms significantly enhance organizational capacity to predict, prevent, and mitigate cyber incidents. The case of SAP NetWeaver zero-day exploitation (CVE-2025-31324) demonstrates the urgency of adaptive defense frameworks, while the implementation of AI-based zero-trust architectures highlights the importance of continuous verification and risk-based access control. This research recommends adopting AI-augmented cybersecurity solutions, strengthening supply chain security, and fostering cyber-aware organizational cultures to ensure sustainable digital resilience. Additionally, it underscores the necessity of aligning cybersecurity with business strategies through cross-disciplinary collaboration that integrates technology, management, human behavior, and policy. By linking cyber resilience directly with organizational performance and strategic competitiveness, this study contributes a holistic framework for maintaining trust and stability in the rapidly evolving landscape of digital business.

Keywords: Cybersecurity Vulnerabilities, Digital Business, Cyber Resilience, AI-Driven Security, Zero-Trust Architecture.

1. Introduction

Digital transformation (DT) has revolutionized business models by embedding advanced information technologies into core operations, customer engagement, and supply chain integration. However, this transformation expands the attack surface, amplifying cybersecurity vulnerabilities that threaten business continuity and data integrity (Rodríguez et al., 2023) [1]. Cybersecurity vulnerabilities in digital business environments manifest in multiple forms, including software flaws, misconfigured infrastructures, and human-related weaknesses.

1.1. Core Vulnerability Types

a. Web Application Vulnerabilities: These include injection flaws, cross-site scripting (XSS), and authentication bypasses that enable attackers to exploit publicly accessible services. According to a recent study, 89% of analyzed companies exhibited web application security issues, revealing a critical vector for data breaches (Cybernews, 2025) [2].
b. System Hosting and Infrastructure Misconfigurations: Poorly configured servers, outdated software, and insecure cloud deployments contribute to 93% of hosting-related vulnerabilities, increasing the risk of unauthorized access and service disruption (Cybernews, 2025) [2].
c. Human Factors – Credential Management: Alarmingly, 46% of employees in trusted US companies reuse breached passwords, significantly increasing susceptibility to credential-stuffing attacks (Cybernews, 2025) [2].

d. Supply Chain Vulnerabilities: The software and hardware supply chains introduce additional risks, with attackers targeting third-party providers to infiltrate otherwise secure organizations (Akinsola et al., 2024) [3].

1.2. Business Risks and Implications

Cybersecurity vulnerabilities translate into direct financial losses, reputational damage, regulatory penalties, and operational disruptions. The National Cyber Security Alliance estimates that 60% of small businesses subjected to cyberattacks cease operations within six months, underscoring the existential threat posed by cyber risks (Smajic, 2025) [4]. For large enterprises, breaches erode consumer trust and can impact stock valuations, necessitating robust resilience strategies that intertwine technical, organizational, and strategic layers (Rodríguez et al., 2023) [1].

2. Research Methods

Advancements in cybersecurity research have expanded beyond simple vulnerability identification towards comprehensive risk management, resilience engineering, and proactive threat anticipation

2.1. Cyber Resilience Frameworks

Resilience in cybersecurity extends traditional defense paradigms by incorporating detection, response, and recovery capabilities into continuous risk management cycles (Dahal et al., 2024) [5]. The NIST Cybersecurity Framework 2.0 (CSF 2.0) exemplifies this approach, structuring activities into six functions: Govern, Identify, Protect, Detect, Respond, and Recover (VanLeuven, 2025) [6]. Organizations adopting this model benefit from a systematic governance structure, asset management, threat detection mechanisms, and recovery protocols that reduce downtime and data loss.

2.2. Simulation-Based Vulnerability Assessment

Simulation techniques have become pivotal in modeling cyberattack scenarios, evaluating system vulnerabilities, and testing mitigation strategies without real-world risks (Barrera et al., 2023) [7]. Simulation environments enable organizations to anticipate attacker behaviors, assess the impact of zero-day exploits, and optimize defense postures. Emerging research advocates for integrating AI-driven simulation frameworks that dynamically adapt to evolving threat landscapes, enhancing predictive capabilities (Barrera et al., 2023) [7].

2.3. Emerging Threats and AI-Enabled Attacks

The increasing sophistication of cyber threats is driven by AI-powered tools that lower the skill barrier for attackers. For instance, AI-powered phishing kits automate social engineering attacks, while botnets leverage hijacked infrastructure for large-scale intrusions (The Hacker News, 2025) [8]. The exploitation of a critical SAP NetWeaver vulnerability (CVE-2025-31324) illustrates how zero-day flaws are weaponized using advanced techniques like Heaven's Gate for endpoint evasion (The Hacker News, 2025) [8].

3. Results and Discussions

RESULTS

Table 1: Cybersecurity Vulnerability Prevalence Across Sector (2025)

	Retail & Consumer (%)	Financial Services (%)	Professional Services (%)
Data Breaches (Past 30 days)	25	25	25
Web Application Vulnerabilities	87	100	100
System Hosting Issues	93	96	96
Software Patching Deficiencies	59	43	43
Employee Password Reuse	46	46	46

Source: Cybernews (2025) [2]

DOI: https://doi.org/10.31004/riggs.v4i3.3200

Table 2: NIST CSF 2.0 Core Functions and Business Impact Correlation

NIST CSF Function	Description	Business Impact
GOVERN	Cybersecurity governance	Aligns security with business objectives
IDENTIFY	Asset and risk identification	Prioritizes critical assets and vulnerabilities
PROTECT	Safeguards implementation	Reduces attack surface and entry points
DETECT	Detection of cybersecurity events	Enables early threat identification
RESPOND	Response to incidents	Minimizes damage and operational downtime
RECOVER	Recovery of services	Restores normal operations quickly

Source: VanLeuven (2025) [6]

Table 3: Cybersecurity Risk Management Framework Adoption Rates (2024-2025)

Framework	Adoption Rate 2024 (%)	Adoption Rate 2025 (%)	CAGR
NIST CSF (all version)	48	61	26.4
ISO/IEC 27001	37	45	21.6
CIS Controls	29	40	37.9
Custom Enterprise Frameworks	22	28	27.3

Source: Iopex (2025) [12]

Table 4: Projected Growth of Cloud Security Market in Education Sector (USD Billion)

Years	Market Size (USD Billion)	CAGR (%) (2024-2030)
2022	2.68	-
2024	3.45	14.4
2026	4.83	14.4
2028	6.75	14.4
2030	7.75	14.4

Source: Verified Market Reports (2025) [16]

Sensitivity Analysis and Scenario Planning

Scenario planning incorporating probabilistic models reveals that:

a. Password Hygiene Improvement: Reducing password reuse by 50% can lower credential-stuffing attack success rates by up to 35%, substantially decreasing breach likelihood.
b. Patch Management Efficiency: Accelerating patch deployment cycles by 30% reduces exposure windows for zero-day exploits, decreasing successful attack incidents by approximately 25%.

DOI: https://doi.org/10.31004/riggs.v4i3.3200

AI Defense Integration: Adoption of AI-augmented detection systems improves incident detection rates by 40%, curtailing attack dwell time and reducing potential damage.

DISCUSSION

Challenges in Achieving Cybersecurity Resilience in Digital Business

Despite technological progress, several persistent challenges impede effective cybersecurity resilience in digital business contexts.

Complexity and Integration Issues

Digital ecosystems often comprise heterogeneous systems, cloud services, and IoT devices, complicating unified security management (Junior et al., 2023) [9]. Inconsistent security controls, legacy system vulnerabilities, and lack of interoperability diminish the efficacy of defense mechanisms.

Human Factor and Organizational Culture

Poor cybersecurity hygiene, including password reuse and insufficient training, remains a significant vulnerability vector (Cybernews, 2025) [2]. Organizational inertia and lack of cyber risk awareness hinder the adoption of best practices and timely incident response

Regulatory and Compliance Pressures

The evolving regulatory landscape, including frameworks such as GDPR, HIPAA, and NIS2, imposes stringent compliance requirements. Organizations struggle to balance compliance with operational flexibility and technological innovation (Darktrace, 2025) [10].

Supply Chain and Third-Party Risks

Supply chain attacks have surged, exploiting weak security practices among vendors and service providers. Transparency and trust deficits challenge the establishment of effective supply chain resilience (Akinsola et al., 2024) [3]

Case Studies: Real-World Vulnerabilities and Resilience Strategies

Exploitation of SAP NetWeaver Zero-Day Vulnerability (CVE-2025-31324)

In April 2025, threat actors exploited a critical zero-day flaw in SAP NetWeaver, assigned a CVSS base score of 10.0, enabling unauthorized file uploads and remote code execution (The Hacker News, 2025) [8]. The attack leveraged advanced post- exploitation frameworks (Brute Ratel C4) and evasion techniques (Heaven's Gate) to bypass endpoint protections. The incident underscores the need for rapid vulnerability disclosure, patch management, and adaptive defense mechanisms in enterprise software ecosystems.

Key Lessons:

a. Importance of timely patch deployment and vulnerability scanning.
b. Necessity of layered defense strategies, including behavioral analytics and endpoint detection.
c. Criticality of threat intelligence sharing across industry sectors.

DigitalXForce X-ROC Cyber Risk Management Solution Deployment

DigitalXForce introduced the X-ROC platform in early 2025, combining AI and big data analytics to provide real-time cyber risk management tailored to complex digital business environments (CBS42, 2025) [15]. The solution integrates threat intelligence feeds, vulnerability assessments, and compliance monitoring, facilitating proactive decision-making, to get Outcomes:

DOI: https://doi.org/10.31004/riggs.v4i3.3200

a. Improved risk visibility across multi-cloud infrastructures.
b. Enhanced incident detection and response times.
c. Streamlined compliance with evolving regulatory frameworks.

This case exemplifies the potential of cutting-edge risk management tools to elevate organizational resilience.

Cybersecurity Challenges in SME Digital Transformation

Small and medium-sized enterprises (SMEs) face acute challenges in cybersecurity resilience owing to limited resources and awareness (Junior et al., 2023) [9]. A systematic review revealed critical gaps in risk identification, workforce training, and integration of cybersecurity into business strategies.

Recommendations:

a. Development of accessible cybersecurity frameworks tailored for SMEs.
b. Increased investment in awareness campaigns and affordable security technologies.

Leveraging managed security service providers (MSSPs) to augment defenses.

Directions for Enhancing Cyber Resilience in Digital Business

Emerging research and industry practices converge towards innovative strategies to fortify resilience and mitigate evolving cyber risks.

AI-Driven Cybersecurity Solutions

Integrating AI for threat detection, anomaly analysis, and automated response is redefining cybersecurity paradigms (Brandefense, 2025) [11]. Zero Trust Architectures augmented with AI enable dynamic access control and continuous verification, reducing reliance on perimeter defenses (The Hacker News, 2025) [8].

Advanced Risk Management Frameworks

Contemporary frameworks emphasize continuous risk assessment, incorporating real-time threat intelligence, vulnerability scanning, and simulation-based scenario planning (Iopex, 2025) [12]. The inclusion of probabilistic reasoning and sensitivity analyses aids in prioritizing mitigation efforts and resource allocation.

Cybersecurity as a Business Enabler

Cybersecurity integration is increasingly recognized as a competitive advantage. Demonstrating robust cyber resilience can unlock new market opportunities, enhance customer trust, and foster innovation (Forbes Tech Council, 2025) [13]. Linking cybersecurity metrics directly to business outcomes facilitates executive engagement and strategic investment.

Supply Chain Transparency and Security

Novel approaches advocate leveraging blockchain and distributed ledger technologies to enhance supply chain transparency and integrity, fostering trust and reducing vulnerabilities (Akinsola et al., 2024) [3].

Workforce Training and Culture Change

Investing in continuous employee cybersecurity education and fostering a culture of vigilance are critical. Programs that combine simulation-based training with behavioral analytics improve human factor resilience (The BCI, 2025) [14].

DOI: https://doi.org/10.31004/riggs.v4i3.3200

Technical Deep Dive: AI-Augmented Cybersecurity Architectures

The convergence of AI and cybersecurity has led to architectures that integrate machine learning models for real-time anomaly detection, automated threat hunting, and adaptive access control. Key technological components include:

a. Behavioral Analytics Engines: Utilizing supervised and unsupervised learning to detect deviations from baseline user and network behaviors
b. AI-Powered Simulation Platforms: Enabling dynamic modeling of attack vectors and defense mechanisms to inform proactive security strategies (Barrera et al., 2023)[7].
c. Zero Trust Network Access (ZTNA): AI-enhanced ZTNA continuously validates user identities and device health, reducing the effectiveness of AI- driven attacks (The Hacker News, 2025)[8].

FP8 Quantization and Model Optimization: Emerging optimization pathways such as FP8 quantization reduce AI model memory footprints by 50%, enabling deployment on resource-constrained environments without performance loss (Meta AI Research, 2024) [17].

Contrarian Perspectives and Limitations

While AI integration in cybersecurity presents vast potential, critics highlight:

a. Complexity and Cost: AI systems require substantial investment and skilled personnel, potentially placing them beyond reach for SMEs (Junior et al., 2023)[9].
b. Adversarial AI Risks: Attackers may exploit the same AI technologies to craft sophisticated evasion techniques, necessitating an ongoing arms race in AI security (The Hacker News, 2025)[8].
c. Data Privacy Concerns: Extensive monitoring and behavioral analytics may raise privacy and ethical issues, requiring careful governance frameworks (Darktrace, 2025)[10].

Addressing these limitations requires balanced approaches combining technology, policy, and human factors.

Cross-Diciplinary Insights

Cybersecurity vulnerabilities in digital business are not solely technical issues but intersect with business strategy, human behavior, and regulatory policy.

a. Technological and Business Integration: Cybersecurity must be embedded within business processes to align risk management with organizational objectives, optimizing investment and operational effectiveness (Forbes Tech Council, 2025) [13].
b. Scientific Methodologies: Advances in simulation, AI, and probabilistic modeling enhance the predictive accuracy of threat assessments, offering scalable solutions applicable across industries (Barrera et al., 2023) [7].
c. Human Factors and Arts: Behavioral sciences and training methodologies derived from arts and communication domains improve employee engagement and cybersecurity culture, reducing human-related vulnerabilities (The BCI, 2025) [14].

Policy and Compliance: Regulatory evolution influences technology adoption curves, necessitating agile compliance strategies that balance security imperatives with innovation (Darktrace, 2025) [10].

Emerging Trends and Future Directions

a. Quantum-Resistant Cryptography: With quantum computing's advent, research is accelerating into quantum-resistant encryption to safeguard future digital business communications.
b. Decentralized Identity Management: Blockchain-based identity frameworks promise enhanced control and security over digital identities, reducing centralized attack risks.
c. Cybersecurity Mesh Architectures: Distributed security mechanisms that provide flexible, scalable, and composable security services aligned with business needs.

DOI: https://doi.org/10.31004/riggs.v4i3.3200

Regulatory Harmonization: Global efforts to unify cybersecurity regulations will facilitate streamlined compliance and foster cross-border cooperation.

4. Conclusion

The conclusion of this study are as follows: a). Cybersecurity vulnerabilities in digital business are multifaceted, encompassing technical flaws, human factors, and supply chain risks, b). State-of-the-art research promotes simulation, AI augmentation, and resilience frameworks such as NIST CSF 2.0 for holistic risk management, c). Persistent challenges include complexity, cultural inertia, and evolving regulatory demands, d). Novel directions emphasize AI-driven zero trust models, enhanced risk management, and cybersecurity as a strategic business enabler, e). Real-world incidents highlight the urgency of rapid patching, threat intelligence sharing, and adaptive defense architectures, f). Cross-disciplinary approaches integrating technology, business strategy, science, and human factors are essential for sustainable cyber resilience.

Reference

[1] Akinsola, A., et al. (2024). Enhancing Software Supply Chain Resilience. arXiv preprint arXiv:2407.13785. https://arxiv.org/pdf/2407.13785
[2] Barrera, J., et al. (2023). Simulation for Cybersecurity: State of the Art and Future Directions. Cybersecurity, 7(1), tyab005. https://academic.oup.com/cybersecurity/article/7/1/tyab005/6170701
[3] Brandefense. (2025). Building Cyber Resilience: Strategies for Navigating Complex Threats. https://brandefense.io/blog/drps/strategies-for- navigating-complex-threats/
[4] CBS42. (2025). DigitalXForce to Launch X-ROC and Cutting-Edge Risk Management Solutions. https://www.cbs42.com/business/press-releases/ein-presswire/800782365/digitalxforce-to-launch-x-roc-and- cutting-edge-risk-management-solutions-at-gisec-rsa-blackhat-and-gartner-conferences/
[5] Cybernews Research Team. (2025, April 28). 46% of the Most Trusted US Companies' Employees Reuse Breached Passwords. https://www.globenewswire.com/news- release/2025/04/28/3069317/0/en/46-of-the-most-trusted-US-companies- employees-reuse-breached-passwords.html
[6] Dahal, K., et al. (2024). Resilience in the Context of Cyber Security: A Review of the State of the Art. Applied Sciences, 14(5), 2116. https://www.mdpi.com/2076-3417/14/5/2116
[7] Darktrace. (2025). NIS2 Compliance: Interpreting 'State-of-the-Art' for Organisations. https://www.darktrace.com/blog/nis2-compliance-interpreting-state-of-the-art-for-organisations
[8] Forbes Tech Council. (2025). The Art Of Risk Management And Navigating Uncertainty. https://www.forbes.com/councils/forbestechcouncil/2025/03/13/the-art-of- risk-management-and-navigating-uncertainty/
[9] Iopex. (2025). Cybersecurity Risk Management: Frameworks and Best Practice. https://www.iopex.com/blog/cybersecurity-risk-management
[10] Junior, C. R., et al. (2023). A Systematic Review of SME Cybersecurity. arXiv preprint arXiv:2309.17186. https://arxiv.org/pdf/2309.17186
[11] Meta AI Research. (2024). FP8 Quantization for Efficient AI Model Deployment. Meta Research Publications.
[12] Rodríguez, M., et al. (2023). Digital Transformation and Cybersecurity Challenges for Businesses: A Systematic Literature Review. Sensors, 23(15), 6666. https://www.mdpi.com/1424-8220/23/15/6666
[13] Smajic, N. (2025). The True Cost of Ignoring Cybersecurity. Medium. https://medium.com/@nermiX/the-true-cost-of-ignoring-cybersecurity- 5d91e5ebbcb4
[14] The BCI. (2025). Staying Resilient in 2025: ESAs Warn of Rising Cyber Attacks and Global Instability. https://www.thebci.org/news/staying-resilient-in-2025- esas-warn-of-rising-cyber-attacks-and-global-instability.html
[15] The Hacker News. (2025, April). Weekly Recap: Critical SAP Exploit, AI-Powered Phishing, Major Breaches, New CVEs & More. https://thehackernews.com/2025/04/weekly-recap-critical-sap-exploit- ai.html
[16] VanLeuven, S. (2025). The Imperative of Cybersecurity Assessments in the Modern Corporate Environment. GitHub. https://raw.githubusercontent.com/VanLeu22/Imperative-of-Cybersecurity-Assessments/main/README.md
[17] Verified Market Reports. (2025). Cloud Security for Education Market Drivers and Trends. https://raw.githubusercontent.com/Arth489/CrossAppHub/main/Cloud%20Security%20for%20Education%20Market%20Key%20Drivers%20and%20 Forecast%202025-2032.md

DOI: https://doi.org/10.31004/riggs.v4i3.3200