International Journal of Economics and Management Research

E-ISSN: 2830-2508
P-ISSN: 2830-2664

Research Article

Recent Developments in Cyber Security Research within Information Systems: A Systematic Literature Review (2021–2025)

Haya Fadiyah Hanin[1*], Sambas Ade Kesuma[2], Keulana Erwin[3], Fahmi Natigor Nasution[4]

[1] Universitas Sumatera Utara, Indonesia, haninfdy@gmail.com
[2] Universitas Sumatera Utara, Indonesia, sambas@usu.ac.id
[3] Universitas Sumatera Utara, Indonesia, keulana@usu.ac.id
[4] Universitas Sumatera Utara, Indonesia, fahmi.natigor@usu.ac.id

*** Corresponding Author:** haninfdy@gmail.com

Abstract: Cybersecurity has become a critical concern for organizations as digital transformation accelerates across all sectors, exposing information systems to increasingly sophisticated threats. This studi aims to analyze and systhesize the dispersed academis literature on cybersecurity in the context of information systems, eith particular focus on the business and accounting domain. A systematic review (SLR) approach was adopted following the PRISMA framework. A total of 28 open-access articles published between 2024 and 2025 were selected from the Scopus database, applying strict inclusion creiteria covering subject area, document type, languange, and source type. Analysis reveals five dominant research themes: AI and security technology, policy, governance, and framework, security behavior and culture, cybersecurity in business context, and digital risk management. Publications are concentrated in 23 journals across 23 countries, with the United States as the leading contributor. Quantitative methods dominate the research landscape while the individual level emerges as the most frequently explored unit of analysis. The findings indicate that effective cybersecurity in informations systems is inherently socio-technical, requiring the simultaneous advancement of AI-based defenses, sound governance frameworks, and human-centered security behavior. This study provides an up-to-date overview of the cybersecurity research landscape in information systems for 2024-2025, identifies emerging trend, and proposes a future reseacrh agenda, particularly for developing country contexts that remain underrepresented in the literature.

Keywords: Business Accounting Cybersecurity; Cybersecurity; Digital Risk Management; Information Systems; Systematic Literature Review.

Received: March 17, 2026
Revised: March 25, 2026
Received: April 12, 2026
Published: April 20, 2026
Current version: April 20, 2026

1. Introduction

Cybersecurity is broadly defined as the practices, processes, and technologies designed to protect computer systems, networks, devices, and data from attack, damage, or unauthorized access (NIST, 2023). In the context of information systems, cybersecurity is not only concerned with hardware and software protection, but also encompasses aspects of information confidentiality, integrity, and availability, widely known as the CIA triad. These three pillars serve as the foundation for designing information security architectures across various organizational contexts, from financial institutions and governments to healthcare and global supply chains (Casino, 2025; Galinec et al., 2025).

The growing attention to cybersecurity is inextricably linked to the massive acceleration of digital transformation that has occurred over the past decade. The adoption of cloud services, the proliferation of Internet of Things (IoT) devices, the expansion of remote work, and the integration of artificial intelligence into business processes have created an increasingly complex digital ecosystem, while expanding the attack surface that can be exploited. A significant inflection point occurred when the COVID-19 pandemic forced an unprecedented acceleration

of digitalization, leading to a sharp Spike in cyber incidents globally. The IBM Cost of Data Breach Report (2024) recorded the average global cost of a data breach reaching USD 4.88 million, a record high in the report's history and a 10% increase from the previous year. Cybersecurity Ventures (2025) projected global economic losses from cybercrime to reach USD 10.5 trillion in 2025 (up from USD 3 trillion in 2015) and is expected to continue growing to USD 12.2 trillion by 2031.

At the national level, the National Cyber and Crypto Agency (2025) recorded more than 330 million cyber traffic anomalies throughout 2024, with the Mirai Botnet being the top threat targeting IoT devices. This combination of high digital dependency, financial motivation of criminals, and the ever-evolving sophistication of attack vectors makes cybersecurity one of the most critical issues of the contemporary era.

Recent research shows that AI and machine learning have become central components in information system cybersecurity, ranging from network anomaly detection achieving accuracy of over 97% (Fadya & Utama, 2025), the development of interpretive threat hunting systems (Owen et al., 2024; Sharma & McHaney, 2025), to IoT security frameworks with a threat prevention rate of 97.1% (Hoxha et al., 2025). On the policy and governance side, several studies have identified significant regulatory gaps, including gaps in the UK NIS framework in addressing global supply chain risks (Gokkaya et al., 2025), the lack of coverage of Operational Technology in the EU 2023 regulation (North & Riskas, 2025), and the need for a standardized IS security maturity evaluation model (Alyami et al., 2024; Galinec et al., 2025). The behavioral dimension has also been shown to be critical: optimism bias drives unsafe behavior toward phishing (Ćirković & Milošević, 2025), and individual risk propensity significantly influences security policy compliance (Toftegaard et al., 2024). In a business context, cybersecurity has been shown to act as a strategic enabler supporting sustainable green practices in SMEs (Pham & Vu, 2025), enhancing the innovation capabilities of ecosystems (Singh et al., 2025), and facilitating the adoption of digital accounting systems (Gu & Wang, 2025).

This research employed a Systematic Literature Review (SLR) approach, an organized and transparent literature review technique to mitigate the risk of bias through the process of identifying, selecting, and synthesizing evidence from a large body of existing, replicable research (Kitchenham & Charters, 2007). Unlike narrative literature reviews, which tend to be subjective, SLR provides a clear search protocol, including keywords, databases used, inclusion and exclusion criteria, and quality assessment procedures, enabling other researchers to validate and replicate the process. This method has been widely used in information systems research to produce comprehensive, evidence-based knowledge syntheses (Okoli & Schabram, 2010). In this study, the SLR protocol was applied to 28 peer-reviewed journal articles selected from a systematic search of the Scopus database, covering the publication period from 2024 to 2025. The purpose of this study is to provide a comprehensive overview of cybersecurity research by answering two key questions:

RQ1. What is the growth trend of cybersecurity research publications in information systems during the period 2024-2025 based on Scopus data?

RQ2. What are the dominant research themes in the field of cybersecurity in information systems during the period 2024-2025?

Answering these questions will provide objective and reliable results on cybersecurity based on SLR findings.

2. Research Methods

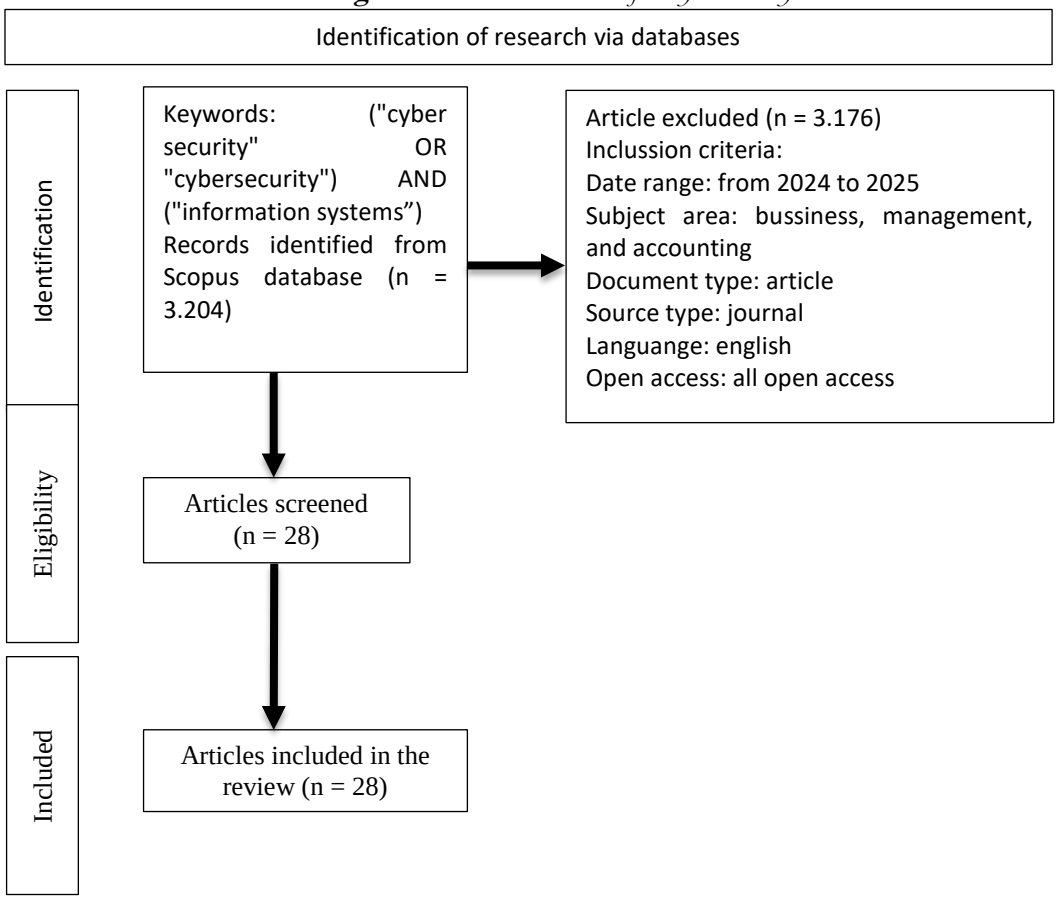
This study follows the PRISMA process to improve the quality of the Systematic Literature Review (SLR) as recommended by Martiny et al. (2024). The authors conducted an information search using article titles, abstracts, and keywords from the Scopus database. Keywords were carefully designed to improve search results. Using the keywords: ("cyber security" OR "cybersecurity") AND ("information systems"), the Scopus database returned 3,204 results. The following criteria were then applied to filter the results:

a. Date range: 2024-2025
b. Subject area: Business, Management, and Accounting
c. Document type: Article

d. Source type: Article
e. Languange: English
f. Open access: All open access

These criteria were applied to improve data quality, in line with recommendations from SLR studies (Martiny et al., 2024). The remaining results comprised 28 articles.

Figure 1. *PRISMA Process for Cybersecurity*



In line with Schaltegger et al. (2022) recommendations, the distribution of articles published by year, journal, and country is described to provide a comprehensive overview of cybersecurity research.

3. Results And Discussion

The following sections present the SLR analysis results using 28 related articles.

Research Status on Cybersecurity

Publications by year

Based on the recommendations of Lennox and Wu (2018), cybersecurity publications are presented by year. Table 1 shows that the distribution of cybersecurity research publications indicates an increase in the number of studies over the past two years. In 2024, a total of 9 publications were recorded by various researchers. Meanwhile, in 2025, the number of publications increased significantly to 19 studies. Overall, up to 2025, there are a total of 28 studies analyzed in this research, indicating that academic interest in cybersecurity within the field of information systems continues to grow in recent years.

Table 1. *Number of Publications per Year*

Year	Author(s)	No. of publication
2024	Owen et al. (2024); Toftegaard et al. (2024); Alyami et al. (2024); Ampel et al. (2024); Gupta et al. (2024); Barnes & Daim (2024); Solaimani et al. (2024); Ferrante (2024); Holbel et al.(2024)	9
2025	Pham & Vu (2025); Gokkaya et al. (2025); Casino (2025); Saadallah et al. (2025); Ilany-tzur & Fink (2025); Long & Rai (2026); Singh et al. (2025); Savchenko et al. (2025), Hoxha et al.	19

	(2025); Sharma & McHaney (2025); Orken et al. (2025); Kumar et al. (2025); Galinec et al. (2025); Gu & Wang (2025); Fadya & Utama (2025); Morshed & Khrais (2025); Ćirković & Milošević (2025); North & Riskas (2025); Shevchenko et al. (2025)	
Total		28

Publications by Journal

Table 2 presents cybersecurity studies published in journals. Of the 28 articles identified, publications are spread across 23 different journals. The journals appearing more than once are Issues in Information Systems (2 articles in 2024 and 2 articles in 2025), IEEE Transactions on Engineering Management (2 articles in 2024), and Information and Computer Security (2 articles in 2024), while all other journals contributed only 1 article each.

Table 2. *Number of Publications per Jornal*

Journal	2024	2025
ACM Transactions on Management Information Systems		1
Big Data and Cognitive Computing		1
Computer Law and Security Review	1	
Decision Sciences Journal of Innovative Education		1
Decision Support Systems		1
Eastern European Journal of Enterprise Technologies		1
IEEE Transactions on Engineering Management	2	
Information and Computer Security	2	
International Journal of Business Information Systems	1	
International Journal of Industrial Engineering and Management		1
International Journal of Information Management		1
International Journal of Information Management Data Insights		1
Issues in Information Systems	2	2
Journal of Management Information Systems	1	
Journal of Risk and Financial Management		1
Management and Accounting Review		1
Proceedings on Engineering Sciences		1
Scientific Bulletin of Mukachevo State University Series Economics		1
Techmology in Society		1
Technology Audit and Production Reserves		1
Technovation		1
TEM Journal		1
Wseas Transactions on Business and Economics		1
Jumlah	9	19
Total	28	

This wide distribution across 23 journals reflects the multidisciplinary nature of cybersecurity research in information systems, spanning the domains of information management, computer security, engineering, accounting, and business. The absence of a single dominant journal suggests that this topic has yet to establish a well-defined publication home, while also indicating an opportunity for specific journals to strengthen their focus on cybersecurity issues in information systems going forward.

Publications by Country

Table 3 presents cybersecurity studies categorized by country. The United States is the largest contributor with 11 articles (5 articles in 2024 and 6 articles in 2025), far exceeding other countries. The United Kingdom ranks second with 4 articles, followed by France with 3 articles. India, the Netherlands, and Ukraine each contributed 1 article.

Table 3. *Number of Publications per Country*

Country	2024	2025	Total
Albania		1	1
Azerbaijan		1	1
China		1	1
Croatia		1	1
France	1	2	3
India	1	1	2
Netherlands	1	1	2
Ukraine		2	2
United Kingdom	2	2	4
United States	5	6	11
			28

The dominance of the United States and Western European countries in cybersecurity research reflects the high levels of regulatory pressure and cyber threats in the region, as well as the availability of more mature research infrastructure. This also highlights a significant research gap from the perspective of developing countries, including Southeast Asia, which is experiencing rapid digitalization but has limited cybersecurity research capacity.

Cybersecurity Research Themes in Information Systems

A thematic analysis of the 28 articles identifies five dominant themes in cybersecurity research within information systems for the 2024–2025 period. Table 4 presents the distribution of articles across these themes.

Table 4. *Distribution of Research Themes*

No.	Research Theme	Quantity	% of Total
1	AI and Security Technology	8	32%
2	Policy, Governance, dan Framework	7	25%
3	Security Behavior and Culture	6	21%
4	Cybersecurity in the Business Context	4	14%
5	Digital Risk Management	3	14%
	Total	28	100%

Based on a synthesis of 28 articles, cybersecurity research in information systems for the 2024–2025 period covers five main themes. The first and most dominant theme is AI and Security Technologies, represented by eight articles. Research in this theme demonstrates that AI has become a core component of modern cyber defense, ranging from a layered security framework for IoT-based power grids that achieved a 97.9% threat detection rate (Orken et al., 2025), to the development of interpretive threat hunting systems such as DeepSecure (Kumar et al., 2025) and ATT&CK-Link, which connects hacker threats to the MITRE ATT&CK framework (Ampel et al., 2024). Benchmark studies also confirm the superiority of the XGBoost and Random Forest algorithms, with network anomaly detection accuracy exceeding 97% (Ćirković & Milošević, 2025).

The second theme, Policy, Governance, and Framework, includes seven articles that reveal a significant gap between existing regulations and actual needs on the ground. The UK NIS framework has been shown to have gaps in addressing global supply chain risks (Gokkaya et al., 2025), while the EU 2023 delegated act is deemed inadequate in covering Operational Technology security in the electricity sector (Toftegaard et al., 2024). At the organizational level, cybersecurity leadership has been shown to drive security policy compliance, although excessive IT complexity can undermine this influence (Gu & Wang, 2025).

The third theme, Security Behavior and Culture, is represented by six articles that confirm that the human factor remains a critical risk vector. Mobile users have been shown to be more wary of phishing than desktop users (Ilany-tzur & Fink, 2025), while optimism bias drives unsafe behavior among employees of financial organizations in South Africa (Owen et al., 2024). Another study identified 11 critical success factors for designing effective Security Education, Training, and Awareness (SETA) programs (Alyami et al., 2024).

The fourth theme, Cybersecurity in a Business Context, includes four articles that demonstrate the strategic role of cybersecurity in supporting business performance. Green

cybersecurity has been shown to drive sustainable business practices in Vietnamese SMEs (Pham & Vu, 2025), while in the Arab Gulf region, a combination of robust cybersecurity, AI-based threat detection, and employee training significantly facilitated the adoption of digital accounting systems among 324 GCC professionals (Morshed & Khrais, 2025).

The fifth theme, Digital Risk Management, is represented by three articles that explore innovative approaches to measuring risk. The use of neural networks to analyze corporate annual reports yields a measure of digital risk from three perspectives—presence, intensity, and diversity—with the finding that risk diversity is of greater importance to investors than intensity (Ilany-tzur & Fink, 2025). A Kolmogorov-Gabor polynomial-based optimization model was also developed to help organizations allocate security budgets more effectively under resource constraints (Shevchenko et al., 2025).

Background Theory and Research Methods on Cybersecurity

Table 4 provides an overview of the research methods used in cybersecurity studies from 2024 to 2025. Of the 28 articles identified, the distribution of research methods is as follows.

Table 5. *Research Methods and Theoretical Framework*

Metodologi	2025	2024	Total
Metode			
Kuantitatif (SEM, PLS, survei, regresi)	7	3	10
Eksperimental/Simulasi	4	1	5
Design Science (artefak IT)	1	1	2
Kualitatif (wawancara, studi kasus)	2	3	5
Literature Review/Analisis Kebijakan	4		4
Mixed Methods		1	1
Model Matematis/Optimasi	1		1
Teori/Framework yang Digunakan			
SEM/PLS-SEM	3	1	4
NIST CSF/COBIT/CMMI	1		1
Machine Learning/Deep Learning	5	1	6
Paradox Theory	1		1
Model Matematis (Kolmogrov-Gabor)	1		1
Tidak disebutkan/konseptual	8	7	15

Four articles used literature review and policy analysis methods kebijakan (Casino, 2025; Galinec et al., 2025; Gokkaya et al., 2025; North & Riskas, 2025), two articles used design science (Ampel et al., 2024; Kumar et al., 2025), and one article each used mixed methods (Solaimani et al., 2024) and mathematical/optimization modeling (Shevchenko et al., 2025). The remaining 10 articles used quantitative approaches using SEM, PLS, surveys, and regression, followed by experimental/simulation methods with 5 articles, and qualitative methods with interviews and case studies with 5 articles.

Of the 28 studies analyzed, 15 did not mention background theory. The remaining 13 studies used a variety of background theories, including SEM/PLS-SEM, NIST CSF/COBIT/CMMI, machine learning/deep learning, paradox theory, and mathematical models.

Units of Analysis in Cybersecurity Research

Table 5 provides insight into the units of analysis used in cybersecurity studies from 2024 to 2025. Of the 28 studies analyzed, two did not specify the unit of analysis used.

Table 6. *Unit of Analysis*

Unit analisis	2025	2024	Total
Level individu (pengguna, karyawan, mahasiswa)	5	5	10
Level organisasi (perusahaan, instansi, SMEs)	7	1	8
Level nasional/kebijakan	2	1	3
Teknis/Sistem (jaringan, IoT, algoritma)	3	2	5
Tidak disebutkan/konseptual	2		2
Total			28

The individual level dominates as the unit of analysis, with 10 studies focusing on users, employees, and students. This is followed by the organizational level with 8 studies covering corporations, public agencies, and SMEs; the technical/systems level with 5 studies analyzing networks, IoT, and algorithms; and the national/policy level with 3 studies. This diversification in units of analysis highlights the evolving cybersecurity research landscape, encompassing federal employees, students, supply chain professionals, the dairy industry, and university networks.

3. Conclusions And Suggestions

Conclusion

It is evident that cybersecurity research in the business and information systems domain experienced significant growth in the 2024-2025 period, with 28 articles meeting the inclusion criteria out of a total of 3,204 initial search results in Scopus. Answering RQ1, cybersecurity publications were concentrated in 2025 with 19 articles, while 9 articles were published in 2024. This increase indicates growing interest in cybersecurity as a research topic. Publications were spread across 23 different journals, with the United States being the largest contributor (11 articles), followed by the United Kingdom (4 articles), and France (3 articles). Cybersecurity research is clearly dominated by developed countries, reflecting the high level of regulatory pressure and cyber threats in the region. The individual level emerged as the primary unit of analysis, with 10 articles focusing on it. However, this trend changed in 2025, with 7 articles focusing on the organizational level, while only 5 articles explored the individual level.

To answer RQ2, thematic analysis identified five dominant themes in cybersecurity research for the 2024-2025 period. Theme 1 (AI & security technology) was the most researched, with 8 articles, reflecting AI's central role in strengthening cyber defenses. Theme 2 (policy, governance & framework) included 7 articles, demonstrating the urgency of strengthening governance at various levels. Theme 3 (security behavior & culture), with 6 articles, emphasized that the human factor remains a critical risk vector. Themes 4 (cybersecurity in a business context) and 5 (digital risk management) contributed 4 and 3 articles, respectively, highlighting cybersecurity as both a strategic business enabler and a growing risk measurement challenge.

In terms of research methods, quantitative approaches dominated, with 10 studies, followed by qualitative and experimental/simulation studies with 5 studies each. Cybersecurity research tends to utilize a wider variety of methods, including design science, mixed methods, and mathematical modeling.

Limitations and suggestions for future research

Expanding the scope of the literature review beyond Scopus to include Web of Science, IEEE Xplore, and Google Scholar could potentially enrich the findings of this study. Although the SLR offers a systematic and reproducible framework, some relevant articles may have been missed due to limitations in the search results. Furthermore, the subject area restriction to business, management, and accounting meant that cybersecurity articles from a purely computer science perspective were excluded, despite the close relationship between the two.

In-depth research on the role of AI and security technologies in the context of organizations in developing countries is highly recommended (theme 1). Existing studies are predominantly focused on developed country contexts, thus the relevance of findings to organizations in Southeast Asia, Africa, and Latin America is limited. Exploring how resource-constrained organizations adopt and optimize AI solutions for cybersecurity would provide more inclusive and applicable insights.

Continuing research on the factors influencing cybersecurity policy compliance (theme 2) is also a valuable direction. Existing studies indicate that leadership, IT complexity, and framework maturity have significant impacts, but research examining these three factors simultaneously is still very limited. Cross-country comparative studies on the effectiveness of regulatory frameworks such as NIST CSF, COBIT, and EU NIS2 in various organizational contexts would provide meaningful contributions to theory and practice.

Theme 3, which focuses on security behavior and culture, presents an interesting research opportunity. Demographic characteristics such as age, gender, and work experience should be

considered as moderators of individual security behavior, as they have been shown to be relevant in other technology adoption contexts (Van et al., 2025). Several studies in this SLR have addressed demographic characteristics, but have not explicitly considered them as moderating variables. Filling this gap will strengthen the design of more personalized and targeted SETA programs.

Quantitative research is recommended for future research to provide a stronger foundation for organizations in prioritizing cybersecurity investments. Furthermore, ensuring that background theory is interrogated within quantitative cybersecurity studies can enhance the robustness and theoretical foundation of research findings, while addressing limitations in the current literature. Longitudinal research on how organizational cybersecurity capabilities evolve over time, particularly in the era of widespread AI adoption, is still essential to understand the long-term dynamics of this issue.

References

Alyami, A., Sammon, D., Neville, K., & Mahony, C. (2024). Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness: An empirical comparison of practitioner perspectives. *Information & Computer Security, 32*(1), 53-73. https://doi.org/10.1108/ICS-08-2022-0133

Ampel, B. M., Samtani, S., Zhu, H., Chen, H., & Jay, F. (2024). Improving threat mitigation through a cybersecurity risk management framework: A computational design science approach. *Journal of Management Information Systems, 41*(1), 236-265. https://doi.org/10.1080/07421222.2023.2301178

Barnes, B., & Daim, T. (2024). Information security maturity model for healthcare organizations in the United States. *IEEE Transactions on Engineering Management, 71*, 928-939. https://doi.org/10.1109/TEM.2021.3139836

Casino, F. (2025). Unveiling the multifaceted concept of cognitive security: Trends, perspectives, and future challenges. *Technology in Society, 83*(April), 102956. https://doi.org/10.1016/j.techsoc.2025.102956

Ćirković, S., & Milošević, M. (2025). Anomaly detection in computer networks using AI techniques: A benchmark study. *Proceedings on Engineering, 07*(3), 1493-1500. https://doi.org/10.24874/PES07.03.011

Corporation, I. (2024). *Cost of data breach report 2024*.

Fadya, M., & Utama, D. N. (2025). Towards secure information systems: Developing and implementing an information security evaluation model using NIST CSF and COBIT 2019. *Technology, Engineering, and Management, 14*(1), 182-191. https://doi.org/10.18421/TEM141-17

Ferrante, T. (2024). Risk-taking propensity and information security compliance behavior in government workers. *Journal of Information Security, 25*(3), 1-12.

Galinec, D., Steingartner, W., & Kozina, A. (2025). National cybersecurity strategy action plan implementation for cyber resilience: Qualitative exploration and achievements. *International Journal of Cybersecurity, 22*, 1290-1304. https://doi.org/10.37394/23207.2025.22.105

Gokkaya, B., Spanaki, K., & Karafili, E. (2025). Strengthening the UK regulatory framework: Enhancing cybersecurity in supply chains. *International Journal of Information Management Data Insights, 5*(2), 100370. https://doi.org/10.1016/j.jjimei.2025.100370

Gu, L., & Wang, J. (2025). The impact of leadership in cybersecurity risk management on information security policy compliance and perceived information security success: The moderating role of IT complexity. *Journal of Cybersecurity, 26*(3), 183-193.

Gupta, S., Modgil, S., Meissonier, R., & Dwivedi, Y. K. (2024). Artificial intelligence and information system resilience to cope with supply chain disruption. *IEEE Transactions on Engineering Management, 71*, 10496-10506. https://doi.org/10.1109/TEM.2021.3116770

Holbel, R., Yerby, J., & Smith, W. (2024). Utilizing virtualized honeypots for threat hunting, malware analysis, and reporting. *Journal of Cybersecurity Research, 25*(1), 265-278.

Hoxha, E., Angjeli, A., & Bombaj, F. (2025). Implementation of modern information systems for automating accounting processes in the public sector: The experience of Albania. *Modern Studies in Economics, 12*(1), 61-74. https://doi.org/10.52566/msu-econ1.2025.61

Ilany-Tzur, N., & Fink, L. (2025). Device and risk-avoidance behavior in the context of cybersecurity phishing attacks. *International Journal of Information Management, 84*(July), 102919. https://doi.org/10.1016/j.ijinfomgt.2025.102919

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering (Technical Report EBSE-2007-01). Keele University & Durham University.

Kumar, P., Javeed, D., Islam, A. K. M. N., & Robert, X. (2025). DeepSecure: A computational design science approach for interpretable threat hunting in cybersecurity decision making. *Decision Support Systems, 188*(October 2024), 114351. https://doi.org/10.1016/j.dss.2024.114351

Lennox, C., & Wu, X. (2018). A review of the archival literature on audit partners. *Accounting Horizons, 32*(2), 1-35. https://doi.org/10.2308/acch-51942

Long, Y., & Rai, A. (2026). Decoding digital risk from corporate disclosure: A neural network approach. *Journal of Corporate Risk Management, 16*(3). https://doi.org/10.1145/3728365

Martiny, A., Taglialatela, J., & Iraldo, F. (2024). Determinants of environmental social and governance (ESG) performance: A systematic literature review. *Journal of Cleaner Production, 456*, 142213. https://doi.org/10.2139/ssrn.1954824

Morgan, S. (2025). *2025 Official Cybercrime Report.* https://cybersecurityventures.com/official-cybercrime-report-2025/

Morshed, A., & Khrais, L. T. (2025). Cybersecurity in digital accounting systems: Challenges and solutions in the Arab Gulf region. *Journal of Risk and Financial Management, 18*(1). https://doi.org/10.3390/jrfm18010041

NIST. (2023). *National Institute of Standards and Technology cybersecurity framework 2.0*. https://doi.org/10.6028/NIST.CSWP.29

North, M., & Riskas, T. (2025). Assessing IS learning outcomes effectively in the age of GenAI. *Journal of Information Systems Education, 26*(2), 1-13.

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. *Sprouts: Working Papers on Information Systems, 10*(26). https://doi.org/10.2139/ssrn.1954824

Orken, M., Serikov, T., Aizat, K., Abdumauvlenovna, B. D., Mekebayev, N., Zhazira, S., & Tursynkanovna, Z. A. (2025). Cybersecurity framework for IoT-integrated electric power information systems. *International Journal of Information Engineering and Management, 16*(2), 124-137. https://doi.org/10.24867/IJIEM-376

Owen, M., Flowerday, S. V., & Van der Schyff, K. (2024). Optimism bias in susceptibility to phishing attacks: An empirical study. *Information and Computer Security, 32*(5), 656-675. https://doi.org/10.1108/ICS-02-2023-0023

Pham, Q. H., & Vu, K. P. (2025). Management accounting information system with green cybersecurity for sustainable green practices: Insight into the moderating role of government regulation. *Management Accounting Research, 24*(3). https://doi.org/10.24191/MAR.V24i03-17

Saadallah, M., Shahim, A., & Khapova, S. (2025). Reconciling tensions in security operations centers: A paradox theory approach. *Business Data Communications and Cloud Computing, 9*(11), 0278. https://doi.org/10.3390/bdcc9110278

Savchenko, T., Lutska, N., Vlasenko, L., Sashnova, M., Zahorulko, A., Minenko, S., Ibaiev, E., & Tytarenko, N. (2025). Risk analysis and cybersecurity enhancement of digital twins in dairy. *Digital Technologies, 2*(2), 37-49. https://doi.org/10.15587/2706-5448.2025.325422

Schaltegger, S., Christ, K., Wenzig, J., & Burritt, R. (2022). Corporate sustainability management accounting and multi-level links for sustainability: A systematic review. *International Journal of Management Reviews, 24*(4), 480-500. https://doi.org/10.1111/ijmr.12288

Sharma, M., & McHaney, R. (2025). Bots and insights: Combining perspectives of analytics and software development in systems analysis and design projects. *Decision Sciences Journal of Innovative Education, 23*(2), e70005. https://doi.org/10.1111/dsji.70005

Shevchenko, V., Syvytsky, Y., Derevianko, Y., Bakaiev, O., Korol, O., Pohasii, S., Laptiev, S., Laptieva, T., Rzayev, K., & Komar, O. (2025). Development of a model of the useful effect of the system at different levels of

subsystem interchangeability in the problem of optimizing the allocation of a limited resource. *Optimization and Control, 4*, 64-75. https://doi.org/10.15587/1729-4061.2025.342299

SIber, D. O. K. (2025). Lanskap keamanan siber Indonesia 2024. *Badan Siber dan Sandi Negara Indonesia*. https://bssn.go.id

Singh, K., Chatterjee, S., Mariani, M., & Fosso, S. (2025). Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic changes in the macroeconomic business environment. *Technovation, 143*(February), 103219. https://doi.org/10.1016/j.technovation.2025.103219

Solaimani, S., Dabestani, R., Harrison-Prentice, T., Ellis, E., Kerr, M., Choudhury, A., Bakhshi, N., Solaimani, S., Dabestani, R., Harrison-Prentice, T., & Ellis, E. (2024). Exploration and prioritisation of critical success factors in adoption of artificial intelligence: A mixed-methods study. *International Journal of Business Information Systems, 10*(26). https://doi.org/10.1504/IJBIS.2022.10053346

Toftegaard, Ø., Grøtterud, G., & Hämmerli, B. (2024). Operational technology resilience in the 2023 draft delegated act on cybersecurity for the power sector: An EU policy process analysis. *Computer Law & Security Review, 54*(August), 106034. https://doi.org/10.1016/j.clsr.2024.106034

Van, H. V., Afifa, M. A., Nguyen, N., & Bui, D. Van. (2025). Cloud accounting: A systematic literature review. *Global Knowledge, Memory and Communication*. https://doi.org/10.1108/GKMC-04-2024-0246