Novatio: Journal of Management Technology and Innovation
E-ISSN : 3030-8674
Volume. 3, Issue 4, October 2025
Page No: 194-205

Cybersecurity and Innovation Risk Management: Organizational Responses in the Digital Era

Henny Noviany[1], Karno Ganjar Prasetyo[2]
[1]Universitas An Nasher, Indonesia
[2]Politeknik Bisnis Digital Indonesia, Indonesia
Correspondent :hennynoviany@universitasannasher.ac.id[1]

Received : August 21, 2025
Accepted : October 2, 2025
Published : October 31, 2025

Citation: Noviany, H., Prasetyo, K, G. (2025). Cybersecurity and Innovation Risk Management: Organizational Responses in the Digital Era. Novatio: Journal of Management Technology and Innovation, 3(4), 194-205.

ABSTRACT: The rapid pace of digital transformation has reshaped healthcare, finance, and energy sectors, creating opportunities for innovation while amplifying vulnerabilities to cyber threats. This narrative review synthesizes organizational responses to cybersecurity and innovation risk management across global contexts. Literature was systematically collected from Scopus, Web of Science, PubMed, and Google Scholar using defined keywords and inclusion criteria, with thematic synthesis guided by review standards. Four central themes emerged: (1) the effectiveness of secure access and identity management in protecting sensitive data, (2) the integration of artificial intelligence and blockchain in predictive modeling and threat detection, (3) measurable improvements in resilience through advanced technological adoption, and (4) the influence of systemic and structural factors, including governance frameworks and international collaboration. Evidence highlights disparities between developed and developing regions, where resource and infrastructure limitations hinder adoption. The discussion links findings with resilience theory while noting limitations such as the neglect of SMEs, dominance of Western perspectives, and reliance on secondary data. Policy implications emphasize capacity-building, harmonized frameworks, and innovation-driven cultures. Comprehensive, collaborative, and context-sensitive approaches are essential for advancing cybersecurity resilience in the digital era.

Keywords: Cybersecurity risk management; digital transformation; artificial intelligence in security; blockchain and data protection; organizational resilience; healthcare cybersecurity; international policy frameworks.

INTRODUCTION

Rapid technological advancement and the integration of information and communication technologies (ICT) have reshaped sectors such as healthcare, energy, finance, and manufacturing. Digitalization creates opportunities for efficiency, innovation, and connectivity, but at the same time raises urgent concerns about cybersecurity.

The healthcare sector has seen rapid growth in digital health systems and medical devices, which improve efficiency but increase risks of data breaches (Keeley, 2024). Similarly, digitalization in the energy sector through the Internet of Things (IoT) demands robust infrastructure protection (Solaimalai et al., 2024). Financial institutions integrating blockchain and artificial intelligence enhance risk management but face new vulnerabilities (Anwar, 2025).

The global scale of these challenges is evident. In 2024, 94% of healthcare organizations reported cyber incidents (Keeley, 2024). Losses from cybercrime are projected to surpass $10 trillion annually by 2025 (Ullah et al., 2024). Regional analyses confirm severe financial damage in sectors such as banking (Kedarya & Elalouf, 2023), while the COVID-19 pandemic revealed gaps in telemedicine security (Gellert et al., 2022).

The growing sophistication of cyber threats, such as malware and denial-of-service attacks, demands comprehensive strategies (Dutta et al., 2024). For example, healthcare digitalization enhances outcomes but increases exposure to attacks (Babu et al., 2025). Likewise, blockchain and AI have introduced new vulnerabilities (Anwar, 2025).

One key barrier is the inadequacy of current risk management strategies, especially in small and medium-sized enterprises (SMEs), which often lack resources and expertise (Adriko & Nurse, 2024). This imbalance leaves SMEs disproportionately vulnerable, making them systemic weak points.

Gaps also exist in research, including reliance on secondary data (Ullah et al., 2024), underrepresentation of SMEs (Adriko & Nurse, 2024), and dominance of Western contexts. Addressing these gaps requires broader and more inclusive approaches.

The aim of this review is to examine organizational responses to cybersecurity and innovation risks across sectors and regions, focusing on systemic challenges, sector-specific vulnerabilities, and effectiveness of current strategies

METHOD

The methodology of this review was designed to ensure the systematic identification, evaluation, and synthesis of relevant literature on cybersecurity and innovation risk management across multiple sectors. The primary aim was to capture the breadth of research that addresses both technical and organizational responses to cybersecurity threats, while simultaneously maintaining methodological rigor in alignment with established review guidelines.

The literature search was conducted across four primary databases that are widely recognized for their comprehensive coverage and reliability: Scopus, Web of Science, PubMed, and Google Scholar. Each of these databases was selected for its distinctive scope and strengths. Scopus and Web of Science were prioritized because of their rigorous indexing standards and extensive coverage of peer-reviewed journals in scientific, engineering, and social science fields. These

databases ensured the inclusion of high-quality articles published in internationally recognized journals, which is particularly critical in addressing the rapidly evolving nature of cybersecurity research (Ullah et al., 2024). PubMed was incorporated due to its specialization in biomedical and health-related literature, which is essential for exploring cybersecurity risks specific to medical devices, electronic health records, and digital healthcare delivery systems (Keeley, 2024). Google Scholar was used as a supplementary source to access a broader range of materials, including dissertations, technical reports, and conference proceedings. While the breadth of Google Scholar is advantageous for capturing diverse perspectives, careful evaluation was employed to account for variability in quality and peer-review standards.

To ensure the identification of relevant literature, carefully constructed keywords and Boolean search strings were employed across all databases. Keywords included "cybersecurity risk management," "cyber threats," "medical device cybersecurity," "information security policies," "data breach management," "blockchain security," and "artificial intelligence in cybersecurity." These terms were chosen based on their recurrent use in existing systematic reviews and empirical studies within the domain of cybersecurity (Ullah et al., 2024; Keeley, 2024). The use of Boolean operators allowed for greater precision, with combinations such as "cybersecurity AND healthcare," "blockchain OR AI AND information security," and "cyber threats AND financial sector." By applying such variations, the search strategy was able to capture literature spanning different sectors, technological applications, and organizational contexts.

The inclusion and exclusion criteria were carefully defined to refine the scope of this review. Only articles published within the last five years were included, ensuring that the findings reflected the most current trends, technologies, and risks in the cybersecurity landscape. This timeframe was chosen due to the rapid pace of change in both cyber threats and innovation strategies, making older studies less applicable to present conditions. Eligible studies were required to be peer-reviewed and published in English, to guarantee academic quality and accessibility. Methodologically, the review included empirical studies such as randomized controlled trials, cohort studies, case studies, and cross-sectional analyses, as well as systematic reviews and meta-analyses that synthesized broader bodies of evidence. The inclusion of multiple study types was intended to provide a comprehensive understanding of both granular case-based insights and higher-level trends.

Conversely, exclusion criteria were applied to filter out articles that lacked peer review, were published outside the defined timeframe, or had minimal relevance to the research objectives. Studies focusing on outdated technologies or presenting incomplete datasets were excluded to avoid drawing conclusions from obsolete or unreliable evidence. Non-English publications were also omitted, acknowledging a limitation in capturing perspectives from non-English speaking contexts. Nonetheless, this criterion was necessary to maintain consistency and reliability in the synthesis process.

The process of literature selection followed a structured approach consistent with the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework (Etemadi et al., 2021; Ullah et al., 2024). Initially, the database searches generated a large pool of records, which were then imported into a reference management system to facilitate screening and organization.

Duplicate records were removed prior to the screening process. Titles and abstracts were reviewed against the inclusion and exclusion criteria to identify potentially relevant studies. Full-text screening was subsequently performed on the shortlisted articles to ensure they met the methodological and topical requirements of the review. At each stage, the screening process was independently verified by multiple reviewers to minimize bias and enhance the reliability of study selection.

Following the selection process, the included studies were subjected to a comprehensive evaluation to assess quality and relevance. Quality appraisal tools appropriate to the study design were employed, ensuring that only methodologically sound studies were integrated into the review. For example, randomized controlled trials were evaluated using standardized risk-of-bias tools, while case studies and qualitative analyses were examined for methodological transparency and rigor. Systematic reviews included in the study were assessed against PRISMA guidelines to confirm adherence to established standards of reporting. This multi-layered quality assessment ensured that the synthesis was grounded in robust and credible evidence.

The analysis of the selected literature involved a thematic synthesis approach. Studies were categorized according to thematic domains such as healthcare cybersecurity, financial sector vulnerabilities, technological innovations like blockchain and AI, and organizational resilience strategies. Within each domain, evidence was examined for recurring patterns, sector-specific challenges, and proposed mitigation measures. Thematic synthesis facilitated the identification of cross-cutting issues, such as the role of governance frameworks and resource availability, while also allowing for sectoral comparisons. In particular, the analysis aimed to highlight how cybersecurity risks and responses manifest differently in small and medium-sized enterprises (SMEs) compared to larger organizations, given the disparity in resources and technical expertise (Adriko & Nurse, 2024).

An additional analytical focus was placed on the geographical and contextual scope of the literature. Studies were examined for their representation of Western and non-Western contexts, enabling an evaluation of the global generalizability of cybersecurity strategies. This was particularly important given the identified literature gap in non-Western perspectives, which often remain underrepresented in high-impact journals (Adriko & Nurse, 2024). By considering geographical diversity, the review sought to generate insights applicable across varied cultural, political, and economic environments, rather than narrowly focusing on a single regional context.

Throughout the review process, efforts were made to ensure transparency, replicability, and comprehensiveness. Documentation was maintained at every stage of the methodology, from database search strategies and keyword development to screening procedures and thematic coding. This documentation serves as an audit trail, ensuring that the methodology can be replicated or scrutinized in future research. By aligning the methodological approach with established systematic review standards, the study contributes not only to the synthesis of knowledge on cybersecurity and innovation risk management but also to the methodological rigor of the field itself.

In conclusion, the methodology of this review reflects a deliberate balance between breadth and depth, combining multiple databases, carefully constructed search strategies, and rigorous

inclusion criteria with a transparent and systematic selection process. By employing thematic synthesis and quality appraisal, the review ensures that its findings are both comprehensive and credible, addressing sector-specific issues while also providing cross-sectoral insights. This approach not only supports the objectives of the study but also lays the groundwork for advancing future research methodologies in the evolving domain of cybersecurity.

RESULT AND DISCUSSION

The findings of this narrative review are organized around four key themes that emerged from the literature: the establishment of cybersecurity and the influence of enabling factors on outcomes; the implications of adopting new technologies for cybersecurity development; the impact of advanced technological factors on security outcomes; and the role of systemic and structural elements in shaping cybersecurity resilience. These themes collectively provide insights into how different factors contribute to organizational readiness and resilience against cyber threats across diverse sectors and geographical contexts.

The first theme highlights the establishment of cybersecurity systems and the role of specific enabling factors in improving outcomes. Evidence consistently underscores that the application of secure digital access technologies plays a crucial role in strengthening hospital information systems. For instance, Gellert et al. (2022) demonstrated that effective digital access management significantly enhanced patient information security during the COVID-19 pandemic, leading to improved institutional responses against cyber threats. This finding emphasizes how identity and access management systems contribute to preserving the integrity of patient data in high-risk environments. Complementarily, Keeley (2024) stressed the importance of implementing risk management standards for medical devices, noting that such measures reduce the incidence of security breaches and strengthen the trustworthiness of healthcare systems. These studies provide empirical evidence that carefully designed access and management technologies can substantially improve security outcomes across healthcare organizations.

The variation in these outcomes is strongly influenced by geographical and infrastructural contexts. In advanced economies, particularly Western Europe, sophisticated information security technologies and stringent regulatory measures have enabled more effective implementation of digital access systems, contributing to stronger cybersecurity performance (Keeley, 2024). Conversely, regions with underdeveloped digital infrastructures, such as parts of the Middle East and Africa, face significant challenges in implementing comparable measures, often resulting in lower preparedness and weaker protection against breaches (Gellert et al., 2022; Keeley, 2024). This disparity underscores the centrality of national infrastructure development and policy enforcement in shaping the effectiveness of organizational cybersecurity practices.

The second theme examines the implications of adopting and integrating new technologies, particularly artificial intelligence (AI) and blockchain, for cybersecurity. Usman et al. (2024) argued that the role of internal auditors is particularly critical in financial organizations, where knowledge of advanced technologies allows for the identification of vulnerabilities and the development of proactive strategies to mitigate risks. Their findings highlight the necessity of equipping auditors

with the skills and expertise required to navigate emerging technologies. Similarly, Movahed et al. (2025) revealed that the integration of AI and IoT into organizational systems enhances resilience by enabling predictive risk modeling and continuous monitoring. These innovations contribute to reducing exposure to cyberattacks by strengthening the capacity of organizations to detect and address risks proactively.

The degree to which these technologies contribute to security outcomes varies between developed and developing regions. In the United States and Europe, where digital infrastructures are advanced, organizations are better positioned to leverage AI and blockchain technologies to gain competitive advantages while managing cybersecurity threats more effectively (Movahed et al., 2025). In contrast, developing regions in Africa and Southeast Asia face considerable barriers, including limited financial resources, insufficient training, and lack of technical expertise, which reduce their ability to adopt these technologies at scale (Usman et al., 2024; Movahed et al., 2025). Consequently, organizations in these regions remain more vulnerable to cyberattacks, highlighting the necessity of targeted capacity-building initiatives to address disparities in technological readiness.

The third theme investigates the impact of advanced technological adoption, such as AI-driven systems, on cybersecurity outcomes. Quantitative and qualitative evidence supports the potential of AI in improving accountability and the overall effectiveness of cybersecurity frameworks. Anwar (2025) reported that AI-driven systems increased the accuracy of threat detection by an average of 10% compared to traditional rule-based methods, illustrating the tangible benefits of employing machine learning models in real-world contexts. Furthermore, Movahed et al. (2025) highlighted the role of AI and IoT in enhancing predictive capabilities, thereby enabling organizations to strengthen resilience by identifying and addressing potential vulnerabilities in advance. These findings point to the transformative role of advanced technologies in establishing proactive cybersecurity frameworks.

Comparative studies further illuminate global differences in the application of these technologies. Ullah et al. (2024) found that developed countries tend to implement mature initiatives supported by well-defined security policies, while developing nations struggle with limited infrastructure and inadequate policy enforcement. Jaloliddin (2023) added that these disparities are further compounded by shortages of skilled personnel and financial resources. Similarly, Priya et al. (2025) showed how the integration of digital technologies significantly enhanced supply chain resilience in developed economies, whereas adoption remained at an early stage in developing countries. These comparative insights underscore the importance of contextualizing cybersecurity strategies, ensuring that resource and infrastructure limitations are explicitly considered when designing solutions for diverse global environments.

The fourth theme centers on systemic and structural factors, such as policies and institutional frameworks, that shape the effectiveness of cybersecurity strategies. Gellert et al. (2022) found that the implementation of digital identity management policies in hospitals significantly improved security practices and response mechanisms during times of crisis. Similarly, Keeley (2024) emphasized that stricter standards for risk management in healthcare not only enhanced patient data protection but also contributed to the establishment of robust institutional frameworks that

ensured resilience over time. These findings underscore the vital role of systemic governance in embedding sustainable cybersecurity practices across sectors.

International case studies provide further evidence of the value of systemic approaches. Research by Kedarya and Elalouf (2023) demonstrated how proactive cybersecurity policies in the banking sector of the United States reduced financial losses and increased institutional resilience. Anwar (2025) highlighted the necessity of international collaboration, noting that shared frameworks and cross-border cooperation are essential for tackling globally interconnected cyber threats. Similarly, Ullah et al. (2024) stressed that systematic alignment with established frameworks, such as the NIST Cybersecurity Framework and ISO standards, strengthens organizational preparedness and resilience across industries. These examples illustrate how international experiences and best practices can be adapted to diverse local contexts, providing valuable lessons for improving cybersecurity governance globally.

Taken together, the findings across these four themes reveal a complex but interrelated set of factors that shape organizational responses to cybersecurity challenges. Secure access technologies and digital identity management provide the foundation for strong cybersecurity practices, but their effectiveness is closely tied to the infrastructural and policy contexts in which they are implemented. The adoption of advanced technologies, including AI and blockchain, enhances resilience but requires significant resource investment and expertise that are not equally distributed across regions. Quantitative evidence demonstrates the measurable benefits of AI-driven solutions, while comparative analyses underscore the persistent disparities between developed and developing contexts. Finally, systemic and structural factors, including governance frameworks and international collaboration, play a decisive role in embedding long-term resilience.

The global perspective that emerges from this review indicates that while developed countries have achieved notable progress in integrating advanced technologies and governance frameworks, developing regions continue to face substantial challenges in achieving comparable outcomes. These findings not only highlight the uneven landscape of cybersecurity readiness but also stress the importance of global knowledge-sharing, capacity-building, and policy development to address disparities. Ultimately, the results affirm that the interplay between technological innovation, organizational practices, and systemic governance determines the success of cybersecurity strategies, underscoring the need for comprehensive and context-sensitive approaches.

The findings of this review demonstrate clear alignment between recent empirical studies and established theoretical frameworks on organizational resilience and information security. The integration of advanced technologies such as artificial intelligence (AI), blockchain, and digital identity management reflects the principles of resilience theory, which emphasizes the capacity of organizations to adapt and respond effectively to unexpected threats. López-López et al. (2022) argued that resilience is achieved not merely through preventive strategies but through the capacity to absorb shocks and maintain continuity of operations. This perspective resonates with the evidence provided by Gellert et al. (2022), who showed that digital identity management in hospitals during the COVID-19 pandemic not only strengthened information security but also enhanced crisis response and operational resilience. Similarly, Keeley (2024) highlighted the role of risk management standards for medical devices in reducing security breaches, providing empirical confirmation of theoretical claims that robust governance frameworks are essential for

enhancing organizational preparedness. However, earlier studies often relied on abstract theoretical models without fully engaging with practical applications and lessons derived from real-world contexts (Etemadi et al., 2021). This underscores the necessity of bridging the gap between theory and practice to ensure that frameworks remain relevant and actionable.

Systemic, cultural, and institutional factors emerged as decisive elements influencing the effectiveness of cybersecurity strategies. National policy environments and the availability of technological infrastructure play pivotal roles in shaping organizational readiness. In advanced economies, strong policy support and investments in digital infrastructure have facilitated the deployment of sophisticated cybersecurity technologies, enabling organizations to adopt advanced solutions such as blockchain-based authentication and AI-driven threat detection (Usman et al., 2024; Peralta et al., 2020). By contrast, developing countries often face structural limitations, including resource constraints, weak infrastructure, and uneven levels of digital literacy among employees, which collectively undermine their ability to achieve comparable outcomes (Adriko & Nurse, 2024). Organizational culture also acts as a mediating factor: institutions that prioritize training, awareness, and innovation are more likely to foster resilience, while those that neglect these elements remain vulnerable to cyberattacks. Keeley (2024) emphasized that the presence of supportive cultural practices that encourage collaboration between technical and managerial staff enhances the integration of effective security protocols, aligning with López-López et al.'s (2022) claim that organizational culture serves as a foundation for adaptive resilience.

The literature provides several potential solutions and interventions to overcome the barriers identified. One recurrent theme is the enhancement of professional competencies within organizations. Usman et al. (2024) recommended improving the skill sets of internal auditors, arguing that their ability to understand and assess emerging technologies is critical for detecting vulnerabilities and devising mitigation strategies. In healthcare, Keeley (2024) suggested that the comprehensive implementation of risk management standards for medical devices can substantially reduce patient data breaches, an approach widely regarded as effective in safeguarding sensitive health information. In the financial sector, Anwar (2025) demonstrated that AI-driven systems significantly improved threat detection accuracy compared to traditional rule-based models, indicating that technology-based interventions yield measurable improvements in cybersecurity outcomes. Collectively, these studies suggest that capacity-building efforts—whether through training, adoption of best practices, or integration of advanced technologies—represent a crucial pathway for improving resilience.

At the systemic level, broader policy interventions have been widely advocated. Ullah et al. (2024) and Etemadi et al. (2021) highlighted the importance of international cooperation in establishing harmonized cybersecurity frameworks, facilitating information sharing on emerging threats, and developing joint strategies to counter transnational cyber risks. These approaches are considered particularly effective given the globalized nature of cyber threats, which transcend national boundaries and require collective responses. However, the literature also stresses that the effectiveness of these measures depends heavily on the inclusivity of stakeholder engagement. Successful policy interventions necessitate collaboration across governments, private sector entities, and civil society to ensure comprehensive adoption and enforcement. Without such collaboration, policies risk remaining fragmented and less impactful, particularly in regions with weaker governance structures.

The discussion also brings into focus the limitations of existing research and the need for further exploration. A notable gap in the current literature is its disproportionate focus on large organizations, which has resulted in limited insights into the unique vulnerabilities faced by small and medium-sized enterprises (SMEs). Adriko and Nurse (2024) highlighted that SMEs often lack the financial and technical capacity to implement advanced security measures, making them disproportionately vulnerable to cyberattacks. Future research should thus extend its scope to include SMEs, particularly in non-Western contexts, to generate findings that are more globally representative. Another limitation lies in the reliance on secondary data in many reviews, which may not adequately capture the rapidly evolving nature of cyber threats (Ullah et al., 2024). The absence of timely primary data collection constrains the ability of researchers to provide real-time assessments of cybersecurity risks and organizational responses.

Furthermore, interdisciplinary approaches remain underutilized in current cybersecurity research. While existing studies have offered valuable insights into technical and organizational aspects, the integration of perspectives from psychology, sociology, and political science could yield a more comprehensive understanding of cybersecurity dynamics. For instance, cultural studies could illuminate how differing attitudes toward technology influence organizational readiness, while political science frameworks could shed light on the role of governance and international relations in shaping cybersecurity collaboration. Movahed et al. (2025) advocated for such interdisciplinary integration, emphasizing that the complex and evolving nature of cyber threats necessitates perspectives that extend beyond purely technical considerations.

Finally, the comparative evidence between developed and developing countries underscores the urgent need for differentiated strategies. Whereas developed countries have achieved considerable progress in deploying advanced technologies and governance frameworks, developing nations face persistent challenges due to resource limitations and infrastructural deficits. Jaloliddin (2023) and Priya et al. (2025) noted that while developed economies have successfully leveraged digital technologies to enhance supply chain resilience, developing countries remain in the early stages of adoption, leaving them more exposed to cyber risks. This disparity highlights the importance of capacity-building initiatives that focus specifically on addressing the contextual challenges of resource-constrained environments. Tailored strategies that account for local conditions are more likely to succeed than blanket approaches that assume homogeneity across global contexts.

In sum, the discussion illustrates that while recent empirical evidence supports theoretical claims regarding resilience and information security, systemic and cultural factors remain critical determinants of cybersecurity effectiveness. The proposed solutions and interventions emphasize both organizational capacity-building and broader policy coordination, though limitations in the existing literature call for expanded scope, interdisciplinary engagement, and context-sensitive strategies in future research.

CONCLUSION

This review highlights the complex interplay between technological innovation, organizational practices, and systemic governance in shaping cybersecurity and innovation risk management across diverse sectors. The findings underscore that secure digital access technologies and identity

management frameworks are essential in enhancing patient data protection and organizational preparedness, particularly in the healthcare sector. Similarly, the integration of advanced technologies such as artificial intelligence and blockchain contributes significantly to improving threat detection, predictive risk modeling, and organizational resilience. However, disparities in technological adoption between developed and developing regions reveal critical challenges, with resource constraints and infrastructural deficits leaving many organizations vulnerable. Systemic and structural factors, including robust policy frameworks, institutional governance, and international collaboration, emerge as decisive in embedding long-term cybersecurity resilience.

The urgency of addressing cybersecurity challenges is reinforced by the growing frequency and sophistication of cyber threats, which impose significant economic and social costs globally. Effective responses require targeted interventions that combine organizational capacity-building, sector-specific standards, and coordinated international policy frameworks. Future research should address limitations in the current literature, particularly the underrepresentation of small and medium-sized enterprises, non-Western contexts, and interdisciplinary approaches that integrate social, cultural, and political dimensions. Expanding primary data collection and comparative studies will also be crucial in generating timely and context-sensitive insights. Strengthening training, awareness, and innovation-driven cultures within organizations remains a central strategy for mitigating risks. Ultimately, cybersecurity and innovation risk management demand comprehensive, context-aware, and collaborative approaches to secure the digital transformation of critical sectors.

REFERENCE

Adriko, R., & Nurse, J. (2024). Cybersecurity, cyber insurance and small-to-medium-sized enterprises: a systematic review. *Information and Computer Security, 32*(5), 691-710. https://doi.org/10.1108/ics-01-2024-0025

Anwar, S. (2025). Ai-driven risk management in online financial transactions: enhancing cybersecurity in the fintech era. *International Journal of Innovative Research and Scientific Studies, 8*(4), 328-335. https://doi.org/10.53894/ijirss.v8i4.7784

Babu, C., Logapadmini, B., Regash, K., & Biruntha, R. (2025). Cybersecurity and privacy concerns in digital health., 397-414. https://doi.org/10.4018/979-8-3693-8774-0.ch020

Dutta, P., Das, S., & Ganguly, D. (2024). Safeguarding business in the age of ai for organizational resilience and risk management., 78-101. https://doi.org/10.4018/979-8-3693-1198-1.ch005

Etemadi, N., Gelder, P., & Strozzi, F. (2021). An ism modeling of barriers for blockchain/distributed ledger technology adoption in supply chains towards cybersecurity. *Sustainability, 13*(9), 4672. https://doi.org/10.3390/su13094672

Gellert, G., Kelly, S., Hsiao, A., Herrick, B., Weis, D., Lutz, J., … & Johnston, D. (2022). Covid-19 surge readiness: use cases demonstrating how hospitals leveraged digital identity access management for infection control and pandemic response. *BMJ Health & Care Informatics, 29*(1), e100680. https://doi.org/10.1136/bmjhci-2022-100680

Jaloliddin, R. (2023). Digitalization in global trade: opportunities and challenges for investment. *Global Trade and Customs Journal, 18*(10), 391-395. https://doi.org/10.54648/gtcj2023043

Karakaya, T. (2025). Securing digital transformation., 123-144. https://doi.org/10.4018/979-8-3693-6417-8.ch006

Kedarya, T., & Elalouf, A. (2023). Risk management strategies for the banking sector to cope with the emerging challenges. *Foresight and Sti Governance, 17*(3), 68-76. https://doi.org/10.17323/2500-2597.2023.3.68.76

Keeley, D. (2024). Healthcare providers' readiness to address medical device cybersecurity within the irish healthcare system. *Global Clinical Engineering Journal, 6*(2), 30-39. https://doi.org/10.31354/globalce.v6i2.158

López-López, Y., Martínez, N., García, V., & Martínez, F. (2022). Organizational resilience: 30 years of intellectual structure and future perspectives. *Iberoamerican Journal of Science Measurement and Communication, 2*(2). https://doi.org/10.47909/ijsmc.37

Movahed, A., Abyaneh, A., Khakbazan, M., & Movahed, A. (2025). Smart economy cybersecurity., 49-72. https://doi.org/10.4018/979-8-3693-4369-2.ch004

Peralta, F., Gorton, A., Watson, M., Bays, R., Boles, J., Gorton, B., … & Powers, F. (2020). Cybersecurity resiliency of marine renewable energy systems-part 1: identifying cybersecurity vulnerabilities and determining risk. *Marine Technology Society Journal, 54*(6), 97-107. https://doi.org/10.4031/mtsj.54.6.9

Priya, N., Masudin, I., & Zulfikarijah, F. (2025). The impact of cross-border logistics and e-commerce on sustainable supply chain management in the digital age., 309-336. https://doi.org/10.4018/979-8-3373-0528-8.ch014

Radvilė, E., & Urbonas, R. (2025). Digital transformation in energy systems: a comprehensive review of ai, iot, blockchain, and decentralised energy models. *Energetika, 71*(1). https://doi.org/10.6001/energetika.2025.71.1.1

Sabkara, M., Aliyari, M., & Lajevardi, M. (2025). Emerging technologies in financial process optimization and risk management., 17-32. https://doi.org/10.4018/979-8-3693-4369-2.ch002

Sayari, K., Firdouse, M., & Abri, F. (2025). Artificial intelligence and machine learning adoption in the financial sector: a holistic review. *IAES International Journal of Artificial Intelligence (IJ-AI), 14*(1), 19. https://doi.org/10.11591/ijai.v14.i1.pp19-31

Shobarani, R., Muthuveerappan, C., Priscilla, G., Suganthi, T., Santhi, S., & Surekha, R. (2023). Securing the future., 383-402. https://doi.org/10.4018/978-1-6684-9317-5.ch019

Solaimalai, G., Mary, S., Kamma, V., Malini, K., Karthikumar, K., & Sudhakar, M. (2024). Harnessing digitalization and internet of things for sustainable energy., 231-262. https://doi.org/10.4018/979-8-3693-2827-9.ch008

Ullah, M., Alam, M., Sultana, T., Rahman, M., Faraji, M., & Ahmed, M. (2024). A systematic review on information security policies in the usa banking system and global banking: risks, rewards, and future trends. *Edelweiss Applied Science and Technology, 8*(6), 8437-8453. https://doi.org/10.55214/25768484.v8i6.3816

Usman, A., Ahmad, A., & Abdulmalik, S. (2024). The role of internal auditors characteristics in cybersecurity risk assessment in financial-based business organisations: a conceptual review. *Revista De Gestão Social E Ambiental, 18*(6), e05691. https://doi.org/10.24857/rgsa.v18n6-008