Journal of Systemics, Cybernetics and Informatics (2025) 23(5), 11-16
https://doi.org/10.54808/JSCI.23.05.11

Aligning SME Critical Assets with Cyber Risks Using a Matrix Model to Develop a Cyber Resilience Framework

Alona BAHMANOVA
Faculty of Engineering Economics and Management, Riga Technical University
Riga, LV-1048, Latvia

Natalja LACE
Faculty of Engineering Economics and Management, Riga Technical University
Riga, LV-1048, Latvia

ABSTRACT

Digitalization has become an integral part of both private and business life, fundamentally transforming all sectors of society. In recent years, the rapid advancement of Artificial Intelligence (AI) has further reshaped the landscape of entrepreneurship by enhancing operational efficiency, streamlining customer interactions, and enabling more informed decision-making. These technological developments offer significant benefits, particularly for small and medium-sized enterprises (SMEs) seeking to remain competitive in a dynamic digital environment. At the same time, these advances introduce new and increasingly complex risks - most notably, the rising threat of cyberattacks. SMEs, which typically operate with constrained financial and human resources, often face significant difficulties in developing and maintaining robust cybersecurity systems. This lack of preparedness makes them particularly attractive targets for cybercriminals, especially in the context of AI-driven operations that introduce novel vulnerabilities.

To address these challenges, this paper proposes a matrix-based approach that systematically links critical SME assets to specific categories of cyber risks. Building on the authors' previous research, the study identifies and classifies essential assets and major threat types, integrating them into a comprehensive matrix framework. The proposed model serves as a practical tool for assessing vulnerability, prioritizing protective actions, and ultimately supporting SMEs in enhancing their overall cyber resilience.

Keywords: Cyber Resilience, Cyber Risks, Digital Transformation, Critical Assets, Matrix-Based Risk Assessment.

1. INTRODUCTION

Today, effective entrepreneurship is inextricably linked to digitalization. Technological advancements offer entrepreneurs a wide range of significant advantages: they facilitate access to existing markets and the development of new ones within specific niches, enable a deeper understanding of target audience preferences through continuous feedback, accelerate operational processes, allow for rapid responses to disruptions, support scalable business growth, and foster the integration of innovative solutions into daily operations.

Among these advancements, one of the most transformative is Artificial Intelligence (AI), which empowers entrepreneurs with automation capabilities, data-driven decision-making, and advanced tools for personalized marketing, customer engagement, and intelligent cybersecurity.

However, like any phenomenon, digitalization, including the widespread adoption of AI, also has its drawbacks. Entrepreneurs now face new threats and risks that have emerged with the rise of virtual business environments. Assets are exposed to dangers that were previously unimaginable. AI systems themselves can become targets of cyberattacks or sources of new vulnerabilities due to data dependency and algorithmic manipulation [2;3;4].

To safeguard these assets, companies invest considerable resources and time into protecting both their tangible and virtual properties. While large enterprises often have sufficient resources to ensure strong cybersecurity measures, small and medium-sized enterprises (SMEs) frequently struggle to implement reliable cybersecurity strategies due to limited resources. This vulnerability makes them attractive targets for cybercriminals [5;6].

To establish effective cyber protection and build cyber resilience, SME entrepreneurs must understand both the specific cyber risks relevant to their field of activity and the range of company assets that are potentially exposed to these risks. This includes recognizing the role of AI systems among critical assets, as well as the unique risks they introduce [7].The classification of risks and assets holds intrinsic value, as it enables the systematic identification of key threats and critical organizational resources. However, the true effectiveness in managing cyber resilience emerges when specific assets are strategically mapped to corresponding risk categories. Authors presume that addressing these challenges requires the development of a matrix-based approach tailored to the realities of modern businesses facing cyber threats. This paper builds on several previous studies conducted by the authors: one focused on identifying and categorizing the critical assets of SMEs, and another on classifying the main cyber risks they encounter [8;9].

In the present paper, the authors integrate these two frameworks into a comprehensive matrix that links key assets, including those related to AI, with corresponding categories of cyber risks. The objective is to develop an integrated matrix-based approach that connects critical SME assets with corresponding categories of cyber risks, thereby enabling a more structured and strategic approach to cyber resilience [10;11;12;13].

To achieve this goal, the paper sets out the following research tasks (RT):

RT1: To identify and classify the critical assets of SMEs, including technological, informational, and AI-related resources.

RT2: To review and categorize the primary cyber risks that affect SMEs in the digital environment.

RT3: To design a matrix that links each asset category with relevant cyber risks, reflecting real-world conditions and challenges.

This study is guided by the following research questions(RQ):

RQ1: What are the critical assets of small and medium-sized enterprises (SMEs) that require protection in the context of growing cyber threats, particularly those emerging from AI-driven business operations?
RQ2: What are the most significant categories of cyber risks currently confronting SMEs in an increasingly digitalized business environment?
RQ3: In what ways can these critical assets be systematically linked to corresponding categories of cyber risks to enhance cyber resilience?
RQ4: To what extent can a matrix-based approach serve as an effective tool for SMEs in identifying, assessing, and managing cyber risks, particularly under conditions of limited resources?
The structure of the paper is organized as follows. The Methodology section outlines the research design, including the literature review process and the development of the asset and risk typologies. The Results section presents bibliometric findings and identifies key categories of cyber risks and SME assets. In the Discussion, the matrix model is introduced as a conceptual tool that enables the visualization of asset–risk relationships. It is important to note that the current paper offers only a generalized matrix framework without specific risk scoring or quantitative evaluation. The proposed model serves as a template for further development and application, which should be tailored to the context and informed by expert assessments and sector-specific data.

2. METHODOLOGY

This study employs a structured, multi-step methodological approach that integrates prior research by the authors and relevant academic literature sourced from the Scopus database. The goal is to develop a matrix-based tool that links critical SME assets with specific categories of cyber risks in order to support effective decision-making and strengthen cyber resilience.
Literature review
To ensure a comprehensive and up-to-date theoretical foundation, a structured literature search was conducted using Scopus, one of the largest and most reputable abstract and citation databases of peer-reviewed literature. A combination of the following keywords was used in the search among article titles, abstracts, and keywords: “cyber risk”, “assets”, and “cyber resilience”. This search yielded 169 documents, of which 33 were available in open access.
The selection was refined to include only peer-reviewed journal articles, conference papers, and review articles that focused on topics such as SMEs, cyber risk, AI-related threats, and digital assets. All selected publications were in English. Documents that lacked empirical or theoretical relevance, as well as duplicates and non-reviewed materials, were excluded from the final dataset.
Utilization of an established typology of cyber risks and classification of SME assets
The first step involves adopting a previously developed classification of cyber risks. This typology includes categories such as cyber attacks, external and insider threats, human related risks, data breaches, financial and reputational risks, operational and technological risks, and other threats commonly faced by SMEs in digital environments. The typology is refined and supplemented using up-to-date findings from peer-reviewed Scopus-indexed publications.
SME asset categorization includes tangible and intangible assets such as IT infrastructure, sensitive information, cyberphysical (CPS) systems, third-party risks, AI and machine learning (ML) systems, Internet of Things (IoT), company reputation, intellectual property, blockchain and smart contracts. These asset categories reflect the most valuable and vulnerable components of an SME in a digitalized context, including AI-enabled systems.

3. RESULTS

Scopus identified a total of 33 scientific publications spanning the period from 2016 to 2025. A notable increase in publication frequency has been observed in recent years, with a peak in 2024 (9 articles), followed by 2023 (7 articles), and 2025 (5 articles either in early access or accepted for publication).
The analyzed publications are categorized as follows:

- 23 journal articles,
- 6 conference papers
- 3 review articles, and
- 2 book chapters.

The most frequently cited publication, “Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations”, has received 112 citations, underscoring its foundational role in the field. Other highly cited works include:

- A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience (59 citations),
- Using Self-Organizing Architectures to Mitigate the Impacts of Denial-of-Service Attacks on Voltage Control Schemes (52 citations),
- Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects (48 citations), and
- Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks (43 citations).

An analysis of author keywords reveals dominant themes and research priorities across the selected publications. The most frequently occurring terms include:

- cybersecurity - 10,
- cyber resilience - 4,
- risk assessment - 3,
- machine learning, security, cyber security, risk management, risk analysis, industry 4.0,
- cyber-physical attacks occurred 2 times.

4. FINDINGS

Based on the authors’ previous research on cyber risk typologies and critical assets, six primary categories of cyber risks have been identified [2;7;14;15;16]:

- External Threats & Cyberattacks
    - Malware (viruses, ransomware)
    - Phishing, Business Email Compromise (BEC)
    - DDoS/DoS attacks, Zero-day exploits
    - SQL/code injection, DNS spoofing
- Insider and Human-related Risks
    - Malicious insiders, data leaks
    - Social engineering, credential stuffing
    - Shadow IT, weak passwords
- Data Vulnerabilities & Information Security Risks

    - Data manipulation/integrity attacks
    - Third-party/supply chain breaches
    - Cloud security flaws, unsecured sensitive data
- Reputational and Financial Risks
    - Regulatory non-compliance (GDPR, PCI DSS)
    - Financial fraud, scams
    - Reputational damage from incidents
- Emerging and Advanced Cyber Threats
    - AI-powered attacks
    - Deepfakes, synthetic identity fraud
    - Quantum computing threats, IoT exploits
- Operational & Technological Weaknesses
    - BYOD, outdated software, weak patching
    - Remote work vulnerabilities
    - Endpoint and infrastructure security gaps

The following categories represent the key SME assets to be protected [4;8;17;18]:

- Customer and Client Data
    - Personal data, purchase history, preferences
    - Loyalty programs, CRM records
- Operational and Business Processes
    - Internal workflows, production processes
    - Service delivery mechanisms
- IT Infrastructure and Digital Systems
    - Networks, servers, databases
    - Cloud-based services, ERP and CRM systems
- Employee Knowledge and Human Capital
    - Skills, expertise, access rights
    - Internal know-how, informal procedures
- Brand and Reputation
    - Market image, customer trust
    - Online presence, public perception
- Artificial Intelligence Systems and Algorithms
    - ML models, training data, automation tools
    - AI decision-support systems
- Financial Assets and Transactions
    - Online banking platforms
    - Digital wallets, e-invoicing tools

5. DISCUSSION

In this paper, the authors employ the concept of a matrix model as an analytical tool to evaluate the cyber resilience of small and medium-sized enterprises (SMEs) operating in environments where organizational assets are simultaneously exposed to multiple categories of cyber risks [3;5;8;19;20;21]. This approach enables a structured visualization of risk exposure, allowing decision-makers to clearly identify which critical assets require prioritization and enhanced protective measures [6;9;11;22;23].

Analogous to classical strategic matrices such as the SWOT or Ansoff Matrix, the proposed model adopts a two-dimensional structure: cyber risk categories are positioned along the horizontal axis, while critical SME assets are mapped along the vertical axis [28;29;30]. This framework facilitates the systematic cross-referencing of assets with the specific risks they face [11;14;24;25;26].

The matrix serves as a diagnostic instrument to detect correlations between assets and vulnerabilities, highlight protection priorities, and uncover gaps or inefficiencies in the current cybersecurity strategy [4;5;17;27;28]. By doing so, it provides SMEs with a practical and adaptable tool for strengthening cyber resilience through more informed, asset-specific decision-making [3;8;9;10;29].

To illustrate the application of the matrix-based approach, the authors selected the financial sector as a representative example. This decision was based on the sector's high level of digital integration, its critical dependence on secure financial transactions, and its frequent exposure to advanced and financially motivated cyber threats. Financial SMEs—such as fintech companies, digital lenders, and small-scale payment service providers—are increasingly reliant on digital infrastructures and AI-powered tools, making them highly vulnerable to a range of threats including fraud, data breaches, and reputational attacks [1;5;6;10;12;27;31;36]. Moreover, the regulatory pressure faced by this sector (e.g., GDPR) reinforces the need for a structured approach to cyber risk assessment and mitigation [11;19;28;34].

Our matrix utilizes six broad categories of cyber risks commonly affecting SMEs. External Threats & Cyberattacks encompass direct intrusions such as malware, phishing, DDoS attacks, and technical exploits (e.g., SQL injection). Insider and Human-related Risks include threats arising from employees or internal users—both intentional and accidental—such as social engineering, weak credentials, or shadow IT [8;9;12;15;26;30]. Data Vulnerabilities & Information Security Risks refer to breaches in data integrity, third-party exposures, and weaknesses in cloud environments. Reputational and Financial Risks involve consequences like regulatory non-compliance, financial fraud, and loss of customer trust. Emerging and Advanced Cyber Threats represent evolving risks from AI-driven attacks, synthetic fraud, and quantum or IoT vulnerabilities. Finally, Operational & Technological Weaknesses focus on structural deficiencies such as outdated software, unsecured remote work environments, and poor endpoint protection [1;6;19;22;31;32].

The vertical axis of the matrix incorporates seven categories of critical assets that SMEs must protect in the face of cyber threats. Customer and Client Data includes personal information, purchase histories, and CRM records, forming the basis of customer trust and compliance requirements [4;8;33]. Operational and Business Processes refer to core internal workflows and service mechanisms that ensure business continuity and value delivery [2;5;16;22;29;34]. IT Infrastructure and Digital Systems comprise hardware, networks, cloud platforms, and enterprise software critical to daily operations. Employee Knowledge and Human Capital encompass employee skills, institutional knowledge, and privileged access, all of which are vulnerable to insider-related risks. Brand and Reputation reflect a company's public image and trustworthiness, which are easily damaged by security incidents. Artificial Intelligence Systems and Algorithms include machine learning models and decision-support tools that are increasingly integral to innovation and automation [3;5;16;23;24;35]. Finally, Financial Assets and Transactions cover digital payment systems, banking platforms, and invoicing tools, making them prime targets for financial fraud and disruption [1;5;6;10;12;27;31;36].

Table 1: Cyber Risk–Asset Matrix for SMEs in the Financial Sector (Created by Authors)

	External Threats & Cyberattacks	Insider and Human-related Risks	Data Vulnerabilities & Information Security Risks	Reputational and Financial Risks	Emerging and Advanced Cyber Threats	Operational & Technological Weaknesses
Customer and Client Data	3	2	3	3	2	2
Operational and Business Processes	2	2	2	2	2	2
IT Infrastructure and Digital Systems	3	2	3	2	3	3
Employee Knowledge and Human Capital	2	3	2	2	2	2
Brand and Reputation	3	2	2	3	2	2
Artificial Intelligence Systems and Algorithms	2	2	2	2	3	2
Financial Assets and Transactions	3	2	3	3	2	2

Each cell in the matrix is evaluated using a three-point ordinal scale to indicate the level of vulnerability and potential impact of a given cyber risk on a specific asset:1=Low, 2=Medium, 3=High

A matrix was constructed based on two analytical dimensions:

- critical SME assets,
- cyber risk categories.

Each cell represents the assessed level of vulnerability and potential impact when a specific asset is exposed to a corresponding risk. The evaluation scale comprises three qualitative levels: Low, Medium, and High, determined through a combined assessment of the likelihood of occurrence and the severity of potential consequences:

- Low rating indicates minimal disruption or limited damage;
- Medium reflects moderate operational disturbance or recoverable loss; and
- High denotes significant impact, potentially resulting in serious operational, financial, or reputational harm.

For the development of the cyber risk–asset matrix, each intersection between a critical asset and a risk category has to be assigned a qualitative score based on expert judgment. For practical implementation, these values should be refined through expert input, industry reports, contextual risk assessments, or structured SME stakeholder workshops.

6. CONCLUSIONS

In this paper, the authors proposed a matrix-based approach to assessing the cyber resilience of SMEs by systematically linking critical organizational assets to relevant categories of cyber risks. The matrix model enables SMEs to visualize the interplay between asset vulnerabilities and cyber threats, serving as a structured tool for prioritizing protective actions and identifying deficiencies in existing cybersecurity strategies. This framework is adaptable and can be applied at various levels, across business sectors, within individual enterprises, or even among specific departments, reflecting functional roles and differential exposure to cyber threats. As such, the resulting matrices will vary by context, offering tailored strategies and priorities for asset protection.

In the current study, the matrix is presented as a conceptual diagram without assigning numerical assessment indicators. For practical application, these values must be determined by experts familiar with the specific operational environment, sectoral characteristics, and threats.

The developed matrix provides a tool for the systematic analysis of cyber resilience at the level of an industry sector, a specific enterprise, or even an individual department within an enterprise. However, the severity and relevance of cyber risks vary significantly depending on the characteristics of the sector and the criticality of specific asset categories. While all sectors are exposed to threats across the six identified risk categories, the degree of exposure and vulnerability is shaped by structural, operational, and technological factors.

Drawing upon the risks and challenges faced by entrepreneurs in various industries, as described in the relevant literature, the authors propose that the severity of risks should be modeled according to sector-specific contexts.

Retail Sector
In the retail sector, customer data as well as financial assets and transactions receive the highest risk scores across several categories. This finding aligns with research indicating that retailers are frequent targets of phishing attacks, payment fraud, and customer data breaches due to their reliance on e-commerce platforms and digital payment systems. Brand reputation also emerges as a critical asset, as customer trust is easily compromised by high-profile data breaches. Literature further confirms that retail SMEs often operate with legacy systems and fragmented IT infrastructures, increasing their susceptibility to external threats and technological vulnerabilities.

Healthcare Sector
The healthcare sector consistently demonstrates elevated risk levels for customer and client data, IT infrastructure, and operational processes. These outcomes correspond with prior studies showing that healthcare organizations are particularly vulnerable to data manipulation, ransomware attacks, and regulatory compliance failures, especially in the context of HIPAA and GDPR frameworks. Insider threats are also of particular concern, given the sensitivity of medical records and the extensive workforce involved in care delivery. In addition, vulnerabilities related to AI are emerging in this sector, particularly due to the increasing deployment of diagnostic automation tools and patient data modeling systems.

Manufacturing Sector
Within the manufacturing sector, the highest levels of risk are observed in relation to operational and business processes, IT infrastructure, and AI systems. Literature sourced from the Scopus database emphasizes that the growing adoption of the Industrial Internet of Things (IIoT), machine learning for process optimization, and intelligent supply chains introduces complex cyber-physical vulnerabilities. These include endpoint device attacks, falsification of quality control data, and remote access exploits. In contrast to the retail and healthcare sectors, manufacturing places comparatively less emphasis on the protection of customer data and instead prioritizes the continuity of core processes and the integrity of supply chains. This orientation aligns with the heightened relevance of risks such as third-party data breaches and denial-of-service (DoS) attacks.

Based on the sectoral analysis presented above, the authors conclude that while the six categories of cyber risks and the seven types of critical assets are universally applicable, the prioritization of mitigation strategies must be tailored to the specific characteristics of each sector:

- The retail sector requires particular focus on data security, fraud prevention, and the preservation of customer trust.
- The healthcare sector demands heightened attention to regulatory compliance, management of insider threats, and protection against ransomware attacks.
- The manufacturing sector must emphasize business continuity, the security of Industrial IoT systems, and the reliability of AI-enabled operational tools.

Despite its practical utility, the proposed approach is subject to certain limitations. The assessment of risk severity levels remains qualitative and may rely on subjective expert judgment unless reinforced by empirical data or sector-specific benchmarks.
Future research should aim to refine and validate the model through empirical case studies and expert review, integrate quantitative risk metrics, and extend its application across diverse industries and regulatory contexts.

7. ACKNOWLEDGEMENT

This work has been supported by the EU Recovery and Resilience Facility within Project No. 5.2.1.1.i.0/2/24/I/CFLA/003 “Implementation of consolidation and management changes at Riga Technical University, Liepaja University, Rezekne Academy of Technology, Latvian Maritime Academy and Liepaja Maritime College for the progress towards excellence in higher education, science and innovation” academic career doctoral grant (ID 1038).

8. REFERENCES

[1] D. Herranz-Oliveros, M. Tejedor-Romero, J.M. Gimenez-Guzman, L. Cruz-Piris, "Unsupervised Learning for Lateral-Movement-Based Threat Mitigation in Active Directory Attack Graphs," **Electronics (Switzerland)**, vol. 13, no. 19.0, 2024 doi: 10.3390/electronics13193944.
[2] I.H. Sarker, H. Janicke, A. Mohsin, A. Gill, L. Maglaras, "Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects," **ICT Express**, vol. 10, no. 4.0, pp. 935.0-958.0, 2024, doi: 10.1016/j.icte.2024.05.007.
[3] K. Strandberg, T. Rosenstatter, R. Jolak, N. Nowdehi, T. Olovsson, "Resilient Shield: Reinforcing the Resilience of Vehicles against Security Threats," **IEEE Vehicular Technology Conference**, vol. 2021-April, , 2021, doi: 10.1109/VTC2021-Spring51267.2021.9449029.
[4] S.B.H. Youssef, N. Boudriga, "A resilient micro-payment infrastructure: An approach based on blockchain technology," **Kuwait Journal of Science**, vol. 49, no. 1.0, 2022, doi: 10.48129/KJS.V49I1.10578.
[5] S. Huda, M.R. Islam, J. Abawajy, V.N.V. Kottala, S. Ahmad, "A Cyber Risk Assessment Approach to Federated Identity Management Framework-Based Digital Healthcare System," **Sensors**, vol. 24, no. 16.0, 2024, doi: 10.3390/s24165282.
[6] D. Zelle, C. Plappert, R. Rieke, D. Scheuermann, C. Krauß, "ThreatSurf: A method for automated Threat Surface assessment in automotive cybersecurity engineering," **Microprocessors and Microsystems**, vol. 90, , 2022, 10.1016/j.micpro.2022.104461.
[7] E. Wai, C.K.M. Lee, "Seamless Industry 4.0 Integration: A Multilayered Cyber-Security Framework for Resilient SCADA Deployments in CPPS," **Applied Sciences (Switzerland)**, vol. 13, no. 21.0, 2023, 10.3390/app132112008.
[8] A. Bahmanova and N. Lace, "Types of Cyber Risks for SMEs: Classification and Business Impact," **Proceedings of the 15th International Scientific Conference “Business and Management 2025”**, 2025, doi: 10.3846/bm.2025.1556.
[9] A. Bahmanova and N. Lace, "The High Stakes of Cyber Resilience: What Key Business Assets Can SMEs Afford to Lose?," **Journal of Service, Innovation and Sustainable Development**, Vol 5, Issue 1, 2024, doi: 10.33168/SISD.2024.0102.
[10] H.I. Kure, A.O. Nwajana, "Protection of critical infrastructure using an integrated cybersecurity risk management (i-CSRM) framework," **5G Internet of Things and Changing Standards for Computing and Electronic Systems**, vol. , pp. 94.0-133.0, 2022, doi: 10.4018/978-1-6684-3855-8.ch004.
[11] S. Silvestri, S. Islam, D. Amelin, G. Weiler, S. Papastergiou, M. Ciampi, "Cyber threat assessment and management for

securing healthcare ecosystems using natural language processing," **International Journal of Information Security**, vol. 23, no. 1.0, pp. 31.0-50.0, 2024, 10.1007/s10207-023-00769-w.
[12] J. Rasmussen, "Risk management in a dynamic society: a modelling problem," **Safety Science**, vol. 27, no. 2–3, pp. 183–213, 1997, doi: 10.1016/S0925-7535(97)00052-0.
[13] S. Guerreiro, W. Guédria, R. Lagerstrõm, S. Van Kervel, "A meta model for interoperability of secure business transactions using BlockChain and DEMO," **IC3K 2017 - Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management**, vol. 2, pp. 253.0-260.0, 2017, doi: 10.5220/0006517502530260.
[14] A. Umunnakwe, A. Sahu, M.R. Narimani, K. Davis, S. Zonouz, "Cyber-physical component ranking for risk sensitivity analysis using betweenness centrality," **IET Cyber-Physical Systems: Theory and Applications**, vol. 6, no. 3.0, pp. 139.0-150.0, 2021, doi: 10.1049/cps2.12010.
[15] S. Saeed, S.A. Suayyid, M.S. Al-Ghamdi, H. Al-Muhaisen, A.M. Almuhaideb, "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience," **Sensors**, vol. 23, no. 16.0, 2023, doi: 10.3390/s23167273.
[16] S. Saeed, S.A. Altamimi, N.A. Alkayyal, E. Alshehri, D.A. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," **Sensors**, vol. 23, no. 15.0, 2023, doi: 10.3390/s23156666.
[17] Z. Liu, L. Wang, "A Distributionally Robust Scheme for Critical Component Identification to Bolster Cyber-Physical Resilience of Power Systems,," **IEEE Transactions on Smart Grid**, vol. 13, no. 3.0, pp. 2344.0-2356.0, 2022, doi: 10.1109/TSG.2022.3147421.
[18] N. AllahRakha, "Cybersecurity Regulations for Protection and Safeguarding Digital Assets (Data) in Today's Worlds," **Lex Scientia Law Review**, vol. 8, no. 1.0, pp. 405.0-432.0, 2024, 10.15294/LSLR.V8I1.2081.
[19] A. Veeramany, S.D. Unwin, G.A. Coles, J.E. Dagle, D.W. Millard, J. Yao, C.S. Glantz, S.N.G. Gourisetti, "Framework for modeling high-impact, low-frequency power grid events to support risk-informed decisions," **International Journal of Disaster Risk Reduction**, vol. 18, pp. 125.0-137.0, 2016, doi: 10.1016/j.ijdrr.2016.06.008.
[20] C. Cameron, C. Patsios, P.C. Taylor, Z. Pourmirza, "Using Self-Organizing Architectures to Mitigate the Impacts of Denial-of-Service Attacks on Voltage Control Schemes," **IEEE Transactions on Smart Grid**, vol. 10, no. 3.0, pp. 3010.0-3019.0, 2019, doi: 10.1109/TSG.2018.2817046.
[21] T. Jungebloud, N.H. Nguyen, D.D. Kim, A. Zimmermann, "Model-based structural and behavioral cybersecurity risk assessment in system designs," **Computers and Security**, vol. 157, , 2025, doi: 10.1016/j.cose.2025.104543.
[22] M. Rubakha, L. Tkachyk, I. Pryimak, N. Demchyshak, R. Yurkiv, "Factor Analysis of Financial Performance and Formation of Strategic Resilience in Ukrainian IT Companies under the Challenges of War," **Financial and Credit Activity: Problems of Theory and Practice**, vol. 1, no. 54.0, pp. 260.0-281.0, 2024, doi: 10.55643/fcaptp.1.54.2024.4229.
[23] G. Moraitis, G.-K. Sakki, G. Karavokiros, D. Nikolopoulos, I. Tsoukalas, P. Kossieris, C. Makropoulos, "Exploring the Cyber-Physical Threat Landscape of Water Systems: A Socio-Technical Modelling Approach," **Water (Switzerland)**, vol. 15, no. 9.0, 2023, doi: 10.3390/w15091687.
[24] R. Fisher, C. Porod, "Enhancing resilience of our Nation's critical infrastructure," **Risk-informed Methods and Applications in Nuclear and Energy Engineering: Modeling, Experimentation, and Validation**, vol. , pp. 241.0-247.0, 2023, doi: 10.1016/B978-0-323-91152-8.00002-8.
[25] E.J. Oughton., D. Ralph, R. Pant, E. Leverett, J. Copic, S. Thacker, R. Dada, S. Ruffle, M. Tuveson, J.W. Hall, "Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks," **Risk Analysis**, vol. 39, no. 9.0, pp. 2012.0-2031.0, 2019, doi: 10.1111/risa.13291.
[26] B. Nikolov, "Approach to Developing a Maritime Cybersecurity Virtual Training Environment," **Vide. Tehnologija. Resursi - Environment, Technology, Resources**, vol. 2, pp. 220.0-225.0, 2024, doi: 10.17770/etr2024vol2.8039.
[27] A. Alshawish, H. de Meer, "Risk mitigation in electric power systems: Where to start?," **Energy Informatics**, vol. 2, no. 1.0, 2019, doi: 10.1186/s42162-019-0099-6.
[28] A.H. Muhammad, A. Nasiri, A. Harimurti, "Machine learning methods for classification and prediction information security risk assessment," **IAES International Journal of Artificial Intelligence**, vol. 14, no. 1.0, pp. 457.0-465.0, 2025, doi: 10.11591/ijai.v14.i1.pp457-465.
[29] M. Rea-Guaman, J.A. Calvo-Manzano, T.S. Feliu, "A prototype to manage cybersecurity in small companies; [Prototipo para Gestionar la Ciberseguridad en Pequeñas Empresas]," **Iberian Conference on Information Systems and Technologies, CISTI**, vol. 2018-June, pp. 1.0-6.0, 2018, doi: 10.23919/CISTI.2018.8399252.
[30] D. Tsuji, J. Fujita, N. Matsumoto, Y. Tamura, J. Doenhoff, T. Shigemoto, "3-layer modelling method to improve the cyber resilience in Industrial Control Systems," **SICE Journal of Control, Measurement, and System Integration**, vol. 16, no. 1.0, pp. 63.0-74.0, 2023, doi:10.1080/18824889.2023.2177074.
[31] D. Ribeiro, A. Almeida, A. Azevedo, F. Ferreira, "Resilience in industry 4.0 digital infrastructures and platforms," **Advances in Transdisciplinary Engineering,** vol. 15, pp. 390.0-395.0, 2021, doi: 10.3233/ATDE210067.
[32] A. AL-Hawamleh, "Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security," **International Journal of Computing and Digital Systems**, vol. 15, no. 1.0, pp. 1315.0-1331.0, 2024, doi: 10.12785/ijcds/150193.
[33] B. Duraj, I. Tola, P. Poshnjari, R. Perri, "Probability of Bank Distress: Investigating a Risk Landscape of an Emerging Economy," **Risk Governance and Control: Financial Markets and Institutions**, vol. 15, no. 1.0, pp. 119.0-129.0, 2025, doi: 10.22495/rgcv15i1p12.
[34] I. Mustafa, A. McGibney, S. Rea, "Smart contract life-cycle management: an engineering framework for the generation of robust and verifiable smart contracts," **Frontiers in Blockchain**, vol. 6, 2023, doi: 10.3389/fbloc.2023.1276233.
[35] M.T. Masud, M. Keshk, N. Moustafa, B. Turnbull, W. Susilo, "Vulnerability defence using hybrid moving target defence in Internet of Things systems," **Computers and Security**, vol. 153, , 2025, doi: 10.1016/j.cose.2025.104380.
[36] J. Pavão, R. Bastardo, N.P. Rocha, "Cyber Resilience and Healthcare Information Systems, a Systematic Review," **Procedia Computer Science**, vol. 239, pp. 149.0-157.0, 2024, doi: 10.1016/j.procs.2024.06.157.