VILNIUS TECH
Vilnius Gediminas Technical University

14th International Scientific Conference "Business and Management 2024"
May 16–17, 2024, Vilnius, Lithuania

NEW TRENDS IN CONTEMPORARY ECONOMICS, BUSINESS AND MANAGEMENT

ISSN 2029-4441 / eISSN 2029-929X
eISBN 978-609-476-363-2
Article Number: bm.2024.1317
https://doi.org/10.3846/bm.2024.1317

FROM CYBER SECURITY TO CYBER RESILIENCE: SAFEGUARDING AGAINST EVOLVING RISKS IN THE DIGITAL LANDSCAPE

Alona BAHMANOVA*, Natalja LACE

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

Received 31 January 2024; accepted 26 April 2024

Abstract. This literature review examines the evolving discourse on digitalization's risks, particularly in cyberspace, and advocates for a transition from cyber security to cyber resilience. Initially explored "digital risks", it shifts focus to keywords like "cyber risks", "cybersecurity", and "cyber resilience" to reflect changing dynamics. Through article analysis, it provides insights into researchers' perceptions, challenges, and strategies in addressing cyber risks. Each section offers concise summaries from published articles, fostering interdisciplinary understanding. Emphasising the imperative of embracing cyber resilience, the review highlights the need to adapt to the continually evolving digital threat landscape.

Keywords: cyber risks, cyber threats, cyber security, cyber resilience, industry 4.0, literature review.

JEL Classification: O33, O34, L86, L96, D83.

1. Introduction

Nowadays, the ubiquitous presence of the Internet and online services has become indispensable, profoundly influencing various facets of our lives. This pervasive reliance on digital technologies has substantially increased convenience, rendering it challenging to envisage life devoid of these innovations. However, this convenience often obscures the inherent risks associated with rapid technological advancements. Despite the profound implications of potential data misuse, awareness of these risks remains disproportionately low among entrepreneurs and individuals alike. This study embarks on a comprehensive literature review, utilizing the Scopus database and sources with "grey literature". The investigation pivots towards an exploration of "cyber risks", "cybersecurity", and "cyber resilience". Moreover, the study traces the evolution of terminology, such as the emergence of concepts like "Industry 4.0" or the "Fourth Industrial Revolution," (Schwab, 2017) "Digital Transformation," (Schwab & Davis, 2018) "Digital Maturity," "Cyber Culture" (Borkovich et al., 2023) underscoring their pivotal role in contemporary discourse. Acknowledging the rapid evolution of the field, exacerbated by the COVID-19 pandemic's transformative impact (Schwab & Malleret, 2020), the study narrows its focus to recent literature to glean contemporary insights.

This study is crucial as it sets the foundation for further research by establishing precise terminology. It serves as a preliminary step towards investigating cyber risks and crafting strategies for mitigating them, with a particular focus on enhancing the resilience of Small and Medium Enterprises (SMEs) against such threats.

Employing a structured methodology for the literature review, the study endeavours to elucidate the distinctions between cyber risks, cyber threats, cybersecurity, and cyber resilience. It posits that while risk mitigation strategies are essential, achieving complete immunity against cyber threats remains unattainable. Hence, the study advocates for a paradigm shift towards a sustainable approach to managing cyber risks, recognizing the inherent vulnerability to cybercrimes in the digital era. Transitioning to cyber resilience becomes paramount in this context. Cyber resilience encompasses not only the ability to prevent and detect cyber threats but also the capacity to adapt and recover swiftly in the face of an incident.

Research questions in this study are as follows:

1. How do researchers across different scientific areas perceive cyber risks and cyber threats, considering the multifaceted nature of the term "risks" and its contextual variations?
2. How does the concept of cyber resilience compare with conventional cyber security measures

* Corresponding author. E-mail: *Alona.Bahmanova@edu.rtu.lv*

in addressing the evolving nature of cyber threats, and what factors contribute to its increasing importance in safeguarding digital infrastructure and information assets?

The research object focuses on understanding cyber risks, cyber threats, cybersecurity, and cyber resilience within the context of rapid technological advancements and the pervasive reliance on digital technologies, with a particular emphasis on their implications for SMEs.

The aim of the research is to establish precise terminology and conduct a comprehensive literature review.

Research tasks are as follows:

- Conduct a literature review utilizing the Scopus database and "grey literature" sources,
- Narrow the focus to recent literature to glean contemporary insights,
- Elucidate the distinctions between cyber risks, cyber threats, cybersecurity, and cyber resilience, and explore the perceptions of researchers across different scientific areas regarding these concepts.

The research employs a structured methodology for the literature review, utilizing the Scopus database and "grey literature" sources. It also involves analyzing perceptions of researchers across different scientific areas regarding cyber risks and cyber threats.

2. Methodology

The main data source used in this study was Scopus database. Sources with books classified as "grey literature" were utilized to enhance the breadth of information considered. Initially, a 20-year timeframe was selected to ensure a thorough examination of research trends within the field.

1. The database was filtered with keywords as follows:

1.1. "cyber risk*", "cyberrisk*", "cyber-risk*" (cyber AND risk* OR cyberrisk* OR cyber-risk*) resulted 13,805 results.

1.2. "cyber security", "cybersecurity", "cyber-security" (cyber AND risk* OR cyberrisk* OR cyber-risk*) resulted in 10,377 hits.

1.3. "cyber resilience", "cyberresilience", "cyber-resilience" (cyber AND resilience OR cyberresilience OR cyber-resilience) produced 690 matches.

2. 2. Subsequently, the selection process focused on articles falling within specific subject areas:

2.1. Computer Science: 402 articles,

2.2. Social Sciences: 133 articles,

2.3. Decision Sciences: 93 articles,

2.4. Business, Management, and Accounting: 65 articles,

2.5. Economics, Econometrics, and Finance: 34 articles.

Following this, 514 articles remained under consideration.

3. Further refinement of the selection was carried out through additional criteria:

3.1. Limited to articles only: 189 articles resulted.

3.2. Limited publications were in English with open access: 102 articles resulted.

4. The dataset, which initially comprised 102 articles after filtering, was imported into VOS Viewer, a specialized software tool utilized for constructing bibliometric networks. Co-occurrence analysis was selected, with all keywords serving as units for analysis. The list of recurring or misspelled keywords underwent refinement using Google Sheets. Consequently, from the initial 1025 keywords, the list was streamlined to 992 keywords. Employing a default repetition threshold of 5, only 7 keywords met the specified criterion. Subsequently, to gain further insights into bibliometric networks and the relationships among clusters of keywords, the default repetition threshold was adjusted to 3, resulting in the identification of 40 keywords and their interconnections within 7 clusters. The keywords "cyber security" and "cyber resilience" emerged as the most prominent, with strong connections and repetitions. The keywords were categorized in 7 clusters as follows:

1. attack graph, Bayesian network, decision support system, denial-of-service attack, electric power system control, risk assessment, smart grid, smart power grids;
2. 5g mobile communication systems, anomaly detection, artificial intelligence, block chain, machine learning, organisational, security and privacy;
3. cyberattacks, cyber physical system, cyber-physical attacks, decision theory, optimization, power, power system, sociotechnical systems;
4. critical infrastructure, cyber-physical security, risk, safety, supervisory control and data acquisition;
5. computer crime, covid-19, governance, ransomware, security of data;
6. cyber resilience, cyber risk, cyber security, internet;
7. threats analysis;

Association strength method was applied in the network mapping visualisation.

3. Results

Annual publication output reveals a significant increase from 2018 (2004–2017 it was just 1 article published per year) and then in 2018 – 4 articles, in 2019 – 7 articles, in 2020 – 6 articles, in 2021 – 11 articles, in 2022 – 24 articles, in 2023 – 35 articles, in 2024 – 11 articles. This trend, influenced also by the concepts presented in the books authored by Klaus Schwab, prompted a decision to limit the search to articles published within the past four years, coinciding with the surge and transformative impact of the global pandemic. Resulted publication count for reviewing: 77 articles in four research areas. The timespan of reviewed articles is limited to 4 recent years (from 2020 through 2024).

As a result of this refined search criteria, the compiled articles are categorized as follows:

- Computer Science – 60 articles,
- Social Sciences – 30 articles,
- Business, Management, and Accounting – 13 articles,
- Economics, Econometrics, and Finance – 8 articles;

The following journals published articles on the topic of interest: IEEE Access, Computers and Security, Electronics (Switzerland), Sustainability (Switzerland), and Applied Sciences (Switzerland).

The list of top-5 countries published the articles are as follows: USA, United Kingdom, Italy, Netherlands, Germany.

Only a subset of selected articles was included in this study, specifically those closely aligned with the research questions posed. Selection criteria involved assessing the relevance of articles based on their abstracts, keywords, and a cursory review of their content.

4. Findings

4.1. Cyber risks

The concept of risk has undergone a historical evolution, originating from gambling mathematics in the seventeenth century, where it denoted the amalgamation of probability and potential outcomes. Initially neutral in the eighteenth century, risk encompassed both positive and negative consequences, notably in marine insurance. However, by the nineteenth century, it took on a negative connotation in economics, associating it with hazards from modern technological advancements. Risk, defined as the combination of the probability of occurrence of a hazard and its consequences, is integral to business operations. All risks can be calculated as:

RISK = Likelihood x Consequences (Keyun, 2019)

Risk is present in all spheres of society: political, economic, environmental, psychological, legal, medical spheres. In the last twenty years, with the advent of computers, the Internet, and now artificial intelligence, new types of risks have emerged. In this study, our focus lies specifically on the cyber aspect of risks.

In today's data-driven world, identifying and mitigating risks pose significant challenges, prompting the demand for robust risk management practices in contracts and insurance agreements (Moyo, 2022). Risks are typically classified based on the level of knowledge about the occurrence and impact of risk events, leading to categories such as known-knowns, unknown-knowns, known-unknowns, and unknown-unknowns (Galinec & Luić, 2020).

A cyber risk caused by a cyber threat and it can be both malicious (adversary intended) and non-malicious (unintended or accidental). The risk, and thus the incident, does not relate to faults in cyber systems where cyber risk is not a contributing factor, such as fault in a cyber system (i.e. computers and network) caused by flooding or fire.

Cyber risk extends beyond IT concerns, necessitating comprehensive enterprise-wide accountability from top management, emphasizing the integration of cyber risk management capabilities into broader enterprise risk management systems to address risks affecting availability, security, performance, compliance, and culture, crucial for safeguarding business value and mitigating impacts on system access, data security, productivity, regulatory compliance, and employee behaviour.

The following risks to economic security are most likely to require thorough assessment:

- risks to the resilience of supply chains, including energy security;
- risks to the physical and digital security of critical infrastructure;
- risks that are related to the security of technology and technology leakage;
- the risk of the weaponization of economic dependencies and economic coercion.

Common cyber threats such as malware, ransomware, social engineering impersonation, and data breaches pose significant challenges for small businesses transitioning to digital operations, necessitating proactive cybersecurity measures despite time constraints. Ransomware is a prominent threat exacerbated by entrepreneurs' general lack of self-protective behaviour online, emphasizing the importance of enhancing cybersecurity awareness and preparedness (Luuk et al., 2023; Tam et al., 2021). The Industry 4.0 era's rapid integration of information and operational technologies fuels transformative improvements in production processes across diverse industrial sectors, underlining the critical need for comprehensive cyber risk assessment and mitigation strategies to safeguard organizations' assets and meet regulatory requirements in an increasingly vulnerable digital landscape (Antonucci, 2017; Gombár et al., 2024; Moyo, 2022).

Cyber risk management encompasses a range of strategies, including threat and vulnerability models, maturity frameworks, cyber insurance, regulatory compliance, and formal standards like ISO/IEC 27000 series, collectively aimed at mitigating cyber threats and strengthening organizational cybersecurity posture (Keyun, 2019). Different perspectives on cyber risk are observed across various subject areas, from technical aspects in computer science to social and psychological dimensions in social sciences, financial implications in business and management, and systemic risks in economics and finance (Galinec & Luić, 2020). Despite the dynamic nature of cyber threats, organizations are urged to advance along the cyber risk maturity curve to effectively mitigate evolving risks associated with modern technologies like Industry 4.0 (Gombár et al., 2024).

From an exploration of literature from diverse perspectives, the formulation of "cyber risk" is as follows:

Risk is a multifaceted phenomenon that has evolved over centuries, encompassing the probability of adverse events and their consequences, influenced by uncertainties and organizational objectives. In the digital environment, *cyber risk emerges from cyber threats, whether intentional or unintentional, posing significant challenges for individuals, institutions, and societies. This extends beyond technical vulnerabilities to encompass broader societal, economic, and psychological dimensions. Effective risk management requires comprehensive approaches that involve identifying, mitigating, and enhancing resilience against these threats.*

4.2. Cyber threats

Cyber threats, unlike risks, operate independently of human actions and have grown in scale and sophistication due to advancing technologies and changing work practices. This surge in cyber-related crimes since February 2020 has drawn increased attention from the media and insurance industry, highlighting the severe consequences these attacks can inflict on organizations' operations and overall business continuity (Antonucci, 2017; Alqudhaibi et al., 2023). The interaction between humans, the Internet, and computers creates a common ground where cyber threats, ranging from human errors to malicious attacks, can disrupt critical business operations or expose sensitive information, emphasizing the importance of robust information security measures and organizational capabilities in addressing these threats (Michalec et al., 2022; Moyo, 2022; Nam, 2019; Ulsch, 2014).

Gombár et al. (2024) categorized the cyber threats into five sections, which the author calls pillars as follows:

- Cyber spying
- Disrupting or reducing IT infrastructure resilience
- Enemy campaigns
- Disrupting or reducing eGovernment security
- Cyberterrorism

The most relevant potential sources of threats deriving from digitization, in this case, are the following: (Perozzo et al., 2022)

- Web portal, website, and social media
- New Data Management Solution
- New technologies and techniques

Awareness and perception of cyber threats are essential for developing effective cybersecurity strategies, especially considering the evolving nature of hybrid threats, with individuals' attitudes in cyberspace shaped by their understanding and perception of risks. However, challenges persist in operationalizing and measuring cyber resilience, particularly in integrating social factors into resilience frameworks and addressing the growing societal impact of cyber insecurities (Gombár et al., 2024; Nam, 2019). As organizations navigate through the uncertainties posed by cyber threats, the efficacy of risk management strategies and crisis response becomes paramount, with cyber threat intelligence playing a crucial role in enhancing cybersecurity readiness by providing specific information to proactively defend against potential cyberattacks (Broeders & Sukumar, 2024; Dunn Cavelty et al., 2023; Jesus et al., 2023; Skierka, 2023).

From an exploration of literature from diverse perspectives, the formulation of "cyber threat" is as follows:

A cyber threat signifies the changing risks brought about by harmful actions in cyberspace, aiming at individuals and organizations across different fields. These dangers involve various issues such as cybercrime, cyberterrorism, and espionage, propelled by advancing technologies and criminal methods. Unlike cyber risk, which deals with the likelihood and potential outcomes of unwanted events influenced by uncertainty and organizational goals, cyber threats concentrate specifically on the malicious actions and the potential damage they can inflict on digital assets and infrastructure.

In summary, we will examine the following terms, frequently used interchangeably, elucidating their commonalities and distinctions:

Table 1. Cyber risks vs. threats: similarities and differences

	Similarities	Differences
Cyber Risk	Essential for comprehending and controlling risks in cyberspace, Both notions involve malevolent actions aimed at digital systems, networks, or data.	Cyber risks focus on the possibility of harm or loss stemming from weaknesses, regardless of whether there's malicious intent.
Cyber Threat		Cyber threats refer to harmful actions or entities aiming to take advantage of vulnerabilities for malicious ends.

4.3. Cyber security

Developing accurate models for predicting cyber risk is crucial despite the challenges posed by the evolving IT landscape, akin to the pursuit of constants in nature. However, the pervasive uncertainty in cyber security underscores the need for standardized definitions and nomenclature to mitigate ambiguity and facilitate a clearer understanding of cyber security and cyber defense across national policies and perspectives (Dunn Cavelty et al., 2023; Galinec & Luić, 2020).

While safety and security may appear similar, they diverge significantly in technical, political, and cultural contexts. In infrastructure research, safety primarily focuses on averting, shielding against, and recovering from unintended accidents, whereas security deals with intentional and malicious incidents. Researchers have identified four main paradigms in cybersecurity:

- fixing and breaking technical objects;
- erroneous use of computers;
- malicious political actions by the means of digital tools;
- social construction of expertise around what is deemed worth protecting;

Effective cybersecurity depends not only on technological advancements but also on the complexity of risk perception influenced by human factors. Confidence in cybersecurity risk measurements enables rapid event response and decision-making, essential for identifying intolerable risks and implementing prioritized action plans for control improvements, as well as understanding the implications of threat intelligence and data analytics outputs for faster, targeted responses (Galinec & Luić, 2020; Gombár et al., 2024).

Developing risk-based justifications for investment in cybersecurity solutions and services is essential, yet challenging due to the inherent unknowability of some risks and their dependency on factors such as time, progress, and response (Baezner, 2020; Galinec & Luić, 2020). While cybersecurity policies primarily focus on securing civilian infrastructures, cyber defense activities, often classified, receive less public attention but are crucial for protecting sensitive information and assets against evolving cyber threats.

Directors must recognize cyber risks as integral to enterprise risk management and ensure regular access to cybersecurity expertise to prioritize cyber risk discussions on meeting agendas (Antonucci, 2017). Maintaining cybersecurity visibility involves measuring current risk levels, establishing tolerances, and formulating prioritized mitigation strategies, allowing organizations to construct a holistic assessment of their cybersecurity posture. Additionally, the evolution of artificial intelligence in cybersecurity has become increasingly necessary to address growing cyber threats in modern ICT-dependent environments (Jada & Mayayise, 2024).

From an exploration of literature from diverse perspectives, the formulation of "cyber security" is as follows:

Cybersecurity involves the methods and plans put in place to protect digital assets and infrastructure from a range of threats, like cybercrime, cyberterrorism, and espionage. It deals with both technical and non-technical aspects, tackling challenges from advancing technologies, human behaviour, and societal influences. While different countries may have their own views and priorities regarding cybersecurity, the main goal remains the same: to stop, find, and deal with cyber threats efficiently, ensuring the strength and safety of digital systems.

4.4. Cyber resilience

Resilience, discussed across various disciplines, entails successfully overcoming challenges or uncertainties by adapting and responding positively. However, its ambiguous nature presents challenges, with engineering approaches focusing on measurable parameters and ecological approaches emphasizing adaptation to new environmental extremes, both relevant to cybersecurity (Dupont et al., 2023; Mott et al., 2023; Toma et al., 2023).

Cyber resilience, distinct from traditional cyber security, entails not only protecting data and systems from attacks but also swiftly resuming operations post-attack. It involves planning for adverse events, absorbing stress, recovering, and preparing for future challenges, emphasizing a holistic approach across organizational dimensions, including physical, informational, cognitive, and social aspects (Bellini et al., 2021; Vuţă et al., 2022).

Cyber resilience goes beyond standard prevention and recovery tactics, focusing on an organization's capacity to absorb and adapt to cyber incidents (Mott et al., 2023). This involves early detection, robust defense mechanisms, and maintaining agility against evolving threats (Bagheri et al., 2023). Cyber event management involves planning, absorbing disruptions, recovering functionalities, and adapting through learning, while effective cybersecurity readiness strategies require addressing the interdependence between technical tools and social factors within organizations (Perozzo et al., 2022).

The conceptual frameworks of cyber security and resilience thinking are closely intertwined, both focusing on the protection and functionality of critical infrastructures. While the end of the Cold War shifted the emphasis to technical systems as objects of security, the complex socio-technical nature of cyberspace underscores the need for resilience beyond purely technological solutions, acknowledging societal factors and individual experiences of inequality and coping mechanisms (Dunn Cavelty et al., 2023).

The sustainability of cybersecurity and cyber resilience hinges on societal actors' perceptions of risks posed by hybrid threats, underscoring the importance of widespread awareness and proactive measures. Cyber resilience practices involve mobilizing technologies, processes, and human resources to minimize and overcome shocks caused by cybersecurity incidents, emphasizing a comprehensive approach to mitigating risks (Akacha & Awad, 2023; Borkovich et al., 2023; Durst et al., 2024; Toma et al., 2023).

Cyber resilience is essential in cyberspace to bolster cyber security, utilizing technological principles to develop adaptive capabilities for managing unforeseen disruptions. While the internet's current technical architecture serves as a foundation for discussions on cyber resilience, expanding the concept beyond technical aspects and engaging in interdisciplinary research, public debates, and political discourse are vital to safeguard critical systems and infrastructures from risks inherent in complex socio-technical environments (Dunn Cavelty et al., 2023).

From an exploration of literature from diverse perspectives, the formulation of "cyber resilience" is as follows:

Cyber resilience refers to the ability to withstand and bounce back from cyber threats by integrating anticipation, support, recovery, and adaptation measures within a constantly changing cyberspace. While cyber security primarily focuses on defending systems and reducing data risks, cyber resilience complements these efforts by preparing organizations and individuals to effectively recover from cyber hazards and ensure system performance despite challenges. This holistic approach includes proactive measures to respond to threats before, during, and after incidents, aligning with planning, absorption, recovery, and adaptation stages. Cyber resilience encompasses not only *technological elements but also interdisciplinary research, public discussions, and political discourse, thus safeguarding critical systems and infrastructures from risks inherent in complex socio-technical environments.*

In summary, we will compare the definitions of "cyber security" and "cyber resilience":

Table 2. Cyber security vs. resilience: similarities and differences

	Similarities	Differences
Cyber security	Both strive to protect digital assets and guarantee the confidentiality, integrity, and availability of information. Both stress the importance of taking proactive steps to reduce risks and implementing strategies for response and recovery.	Cybersecurity extends beyond addressing threats to encompass broader measures such as prevention, detection, and response.
Cyber resilience		Cyber resilience underscores the capacity to adjust and bounce back from cyber threats, extending beyond mere protection to guarantee the uninterrupted operation of systems.

5. Discussion

Scholarly articles originating from four distinct scientific areas were compiled to elucidate the concept of cyber risks and advocate for the adoption of a cyber resilience approach to cybersecurity. Each discipline provides a nuanced perspective on the subject matter. Presented below is a summary of the chosen articles.

Computer Sciences

Scholarly articles extensively examine cyber risks, threats, security, and resilience, particularly focusing on issues like geopolitical manipulation of internet infrastructure and supply chain vulnerabilities (Creazza et al., 2022). They highlight the need for improved risk management tools like Cyber-Value-at-Risk (CVaR), and comprehensive threat analysis for sectors such as automotive safety amidst the proliferation of connected smart cars. Additionally, challenges arising from AI adoption and cyber resilience across sectors like healthcare, maritime power systems, agriculture and urban transit are thoroughly discussed, underscoring the complexities within the subject area of computer science. Post-incident communication challenges within organizations , insurance against ransomware and tensions in cyber-resilience implementations are explored (Dart & Ahmed, 2023; Erstad et al., 2021; Sahay et al., 2023).

Social Sciences

The articles offer thorough analysis of cyber risks, threats, security, and resilience, shedding light on vulnerabilities within critical infrastructures, and the socio-economic implications of cybersecurity investments. They emphasize the importance of delving into motivational factors influencing protective measures against ransomware, highlighting the crucial role of cyber resilience in organizational survival and reputation management. These insights underscore the intersection between cybersecurity and social science, emphasizing the need for interdisciplinary approaches to address contemporary challenges effectively.

Business, Management, and Accounting

The articles delve into various aspects of cyber resilience within business, management, and accounting areas, highlighting the vulnerability of SMEs and banking system to cyber threats and the importance of cyber culture, in organizational security. They emphasize the challenge of balancing insurance-based governance with cyber resilience amidst evolving threats and the development of situational awareness models for effective cybersecurity risk assessment (Dudin & Shkodinsky, 2022). Additionally, the correlation between organizational cyber risk climate, cybersecurity performance, and investments is explored, while a gap in open Cyber Threat Intelligence (CTI) sharing underscores the need for further research in this area to establish industry standards.

Economics, Econometrics, and Finance: 8

Scholarly articles in economics, econometrics, and finance explore various facets of cyber resilience, including the role of cyber insurance in incentivizing effective risk management and the preparedness of regulatory frameworks to address cyber risks in the financial sector. They emphasize the development of situational awareness models for assessing cybersecurity risks and highlight the need for interdisciplinary approaches and advanced econometric modelling techniques to develop comprehensive risk management strategies. Furthermore, empirical studies analyzing regulatory interventions' impact on economic and financial system resilience to cyber threats could offer insights into effective governance mechanisms for mitigating risks and ensuring financial stability.

Challenges

The literature underscores the multifaceted nature of cyber risk and the challenges it poses across various science areas, including business, governance, and psychology. Key obstacles include the scarcity of relevant data for identifying risk factors, organizational barriers to effective cyber risk management at the board level, and discrepancies between perceived threats and actual preparedness (Fraga-Lamas & Fernandez-Carames, 2020). Addressing these challenges necessitates a holistic approach that integrates cyber risk into enterprise risk management models, fosters collaboration for open Cyber Threat Intelligence adoption, and promotes international cooperation to bridge cybersecurity gaps. Challenges also arise from the absence of standardized methods for assessing losses caused by cyber risks and threats, along with a reluctance to adopt new approaches to cybersecurity. Additionally, operationalizing cyber resilience requires formalization and the development of practical measurement tools, with existing frameworks adopting functionality-based or capacity-based approaches to assess resilience (Erola et al., 2022; Knight & Nurse, 2020; Renaud & Coles-Kemp, 2022).

The transition from cyber security to cyber resilience is essential for addressing the evolving IT landscape's challenges and uncertainties. While cyber security focuses on preventing and recovering from cyber-attacks, cyber resilience emphasizes the capacity to adapt and respond positively to incidents, involving early detection, robust defense mechanisms, and organizational agility against evolving threats. This shift requires standardized definitions and nomenclature to enhance understanding across national policies and perspectives, prioritizing comprehensive approaches that mobilize technologies, processes, and human resources to minimize and overcome cybersecurity shocks (Safitra et al., 2023).

6. Conclusions

This study examined scholarly articles and grey literature focusing on cyber risks, threats, security, and resilience, highlighting the necessity to reconsider cybersecurity strategies in the dynamic and evolving cyberspace. It emphasizes that cyber resilience surpasses addressing immediate cyber risk concerns by emphasizing the significance of readiness to mitigate damages arising from technological interactions and potential harm, whether deliberate or accidental. Numerous challenges and research gaps require a proactive approach and preparedness to anticipate and address forthcoming changes. Cyber resilience necessitates proactive thinking rather than reactive responses, promoting foresight and proactive decision-making.

Future research should prioritize the development of standardized methods for assessing losses caused by cyber risks and threats, as well as exploring strategies to overcome reluctance in adopting novel approaches to cybersecurity. Moreover, with the continuous evolution of cyberspace, a proactive approach and enhanced preparedness will be essential to effectively anticipate and navigate forthcoming changes, thereby reinforcing the importance of embracing cyber resilience as a cornerstone of contemporary cybersecurity paradigms.

References

Akacha, S. A.-L., & Awad, A. I. (2023). Enhancing security and sustainability of e-learning software systems: A comprehensive vulnerability analysis and recommendations for stakeholders. *Sustainability*, *15*(19), Article 14132. https://doi.org/10.3390/su151914132

Alqudhaibi, A., Albarrak, M., Aloseel, A., Jagtap, S., & Salonitis, K. (2023). Predicting cybersecurity threats in critical infrastructure for industry 4.0: A proactive approach based on attacker motivations. *Sensors*, *23*(9), Article 4539. https://doi.org/10.3390/s23094539

Antonucci, D. (2017). *The cyber risk handbook: Creating and measuring effective cybersecurity capabilities.* (1st ed.). Wiley. https://doi.org/10.1002/9781119309741.ch1

Baezner, M. (2020). Cybersecurity in Switzerland: Challenges and the way forward for the Swiss armed forces. *Connections*, *19*(1), 63–72. https://doi.org/10.11610/Connections.19.1.06

Bagheri, S., Ridley, G., & Williams, B. (2023). Organisational cyber resilience: Management perspectives. *Australasian Journal of Information Systems*, *27*. https://doi.org/10.3127/ajis.v27i0.4183

Bellini, E., Marrone, S., & Marulli, F. (2021). Cyber resilience meta-modelling: The railway communication case study. *Electronics*, *10*(5), Article 583. https://doi.org/10.3390/electronics10050583

Borkovich, D. J., Skovira, R. J., & Kohun, F. (2023). Foundation of cybersecurity infoscapes: It's all about the culture. *Issues in Information Systems*, *24*(3), 1–14. https://doi.org/10.48009/3_iis_2023_101

Broeders, D., & Sukumar, A. (2024). Core concerns: The need for a governance framework to protect global Internet infrastructure. *Policy and Internet*, *16*(2), 411–427. https://doi.org/10.1002/poi3.382

Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2022). Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management*, *27*(1), 30–53. https://doi.org/10.1108/SCM-02-2020-0073

Dart, M., & Ahmed, M. (2023). CYBER-AIDD: A novel approach to implementing improved cyber security resilience for large Australian healthcare providers using a unified modelling language ontology. *Digital Health*, *9*.

Dudin, M. N., & Shkodinsky, S. V. (2022). Challenges and threats of the digital economy to the sustainability of the national banking system. *Finance: Theory and Practice*, *26*(6), 52–71. https://doi.org/10.26794/2587-5671-2022-26-6-52-71

Dunn Cavelty, M., Eriksen, C., & Scharte, B. (2023). Making cyber security more resilient: Adding social considerations to technological fixes. *Journal of Risk Research*, *26*(7), 801–814. https://doi.org/10.1080/13669877.2023.2208146

Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers and Security*, *132*, Article 103372. https://doi.org/10.1016/j.cose.2023.103372

Durst, S., Hinteregger, C., & Zieba, M. (2024). The effect of environmental turbulence on cyber security risk management and organizational resilience. *Computers and Security*, *137*, Article 103591. https://doi.org/10.1016/j.cose.2023.103591

Erola, A., Agrafiotis, I., Nurse, J. R. C., Axon, L., Goldsmith, M., & Creese, S. (2022). A system to calculate cyber-value-at-risk. *Computers and Security*, *113*, Article 102545. https://doi.org/10.1016/j.cose.2021.102545

Erstad, E., Ostnes, R., & Lund, M. S. (2021). An operational approach to maritime cyber resilience. *International Journal on Marine Navigation and Safety of Sea Transportation*, *15*(1), 27–34. https://doi.org/10.12716/1001.15.01.01

Fraga-Lamas, P., & Fernandez-Carames, T. M. (2020). Fake news, disinformation, and deepfakes: Leveraging distributed ledger technologies and blockchain to combat digital deception and counterfeit reality. *IT Professional*, *22*(2), 53–59. https://doi.org/10.1109/MITP.2020.2977589

Galinec, D., & Luić, L. (2020). Design of conceptual model for raising awareness of digital threats. *WSEAS Transactions on Environment and Development*, *16*, 493–504. https://doi.org/10.37394/232015.2020.16.50

Gombár, M., Vagaská, A., Korauš, A., & Račková, P. (2024). Application of structural equation modelling to cybersecurity risk analysis in the era of industry 4.0. *Mathematics*, *12*(2), Article 343. https://doi.org/10.3390/math12020343

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, *8*(2), Article 100063. https://doi.org/10.1016/j.dim.2023.100063

Jesus, V., Bains, B., & Chang, V. (2023). Sharing is caring: Hurdles and prospects of open, crowd-sourced cyber threat intelligence. *IEEE Transactions on Engineering Management*, *71*, 6854–6873. https://doi.org/10.1109/TEM.2023.3279274

Keyun, R. (2019). *Digital asset valuation and cyber risk measurement: Principles of cybernomics*. Academic Press.

Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers and Security*, *99*, Article 102036. https://doi.org/10.1016/j.cose.2020.102036

Luuk, B., (Maria) Susanne, V. H.-D. G., Missana-ter Huurne, E. F. J., Ynze, V. H., Remco, S., & Eric Rutger, L. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers and Security*, *127*, Article 103099. https://doi.org/10.1016/j.cose.2023.103099

Michalec, O., Milyaeva, S., & Rashid, A. (2022). When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures? *Big Data and Society*, *9*(1). https://doi.org/10.1177/20539517221108369

Mott, G., Nurse, J. R. C., & Baker-Beall, C. (2023). Preparing for future cyber crises: Lessons from governance of the coronavirus pandemic. *Policy Design and Practice*, *6*(2), 160–181. https://doi.org/10.1080/25741292.2023.2205764

Moyo, S. (2022). *Executive's guide to cyber risk: Securing the future today*. Wiley.

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society*, *58*, Article 101122. https://doi.org/10.1016/j.techsoc.2019.03.005

Perozzo, H., Zaghloul, F., & Ravarini, A. (2022). CyberSecurity readiness: A model for SMEs based on the socio-technical perspective. *Complex Systems Informatics and Modeling Quarterly*, (33), 53–66. https://doi.org/10.7250/csimq.2022-33.04

Renaud, K., & Coles-Kemp, L. (2022). Accessible and inclusive cyber security: A nuanced and complex challenge. *SN Computer Science*, *3*(5). https://doi.org/10.1007/s42979-022-01239-1

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), Article 13369. https://doi.org/10.3390/su151813369

Sahay, R., Estay, D. A. S., Meng, W., Jensen, C. D., & Barfod, M. B. (2023). A comparative risk analysis on CyberShip system with STPA-Sec, STRIDE and CORAS. *Computers and Security*, *128*, Article 103179. https://doi.org/10.1016/j.cose.2023.103179

Schwab, K. (2017). *The Fourth Industrial Revolution*. Crown Currency.

Schwab, K., & Davis, N. (2018). *Shaping the Fourth Industrial Revolution.* World Economic Forum.

Schwab, K., & Malleret T. (2020). *COVID-19: The great reset.* World Economic Forum.

Skierka, I. (2023). When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis. *Government Information Quarterly*, *40*(1), Article 101781. https://doi.org/10.1016/j.giq.2022.101781

Tam, T., Rao, A., & Hall, J. (2021). The invisible COVID-19 small business risks: Dealing with the cyber-security aftermath. *Digital Government: Research and Practice*, *2*(2). https://doi.org/10.1145/3436807

Toma, T., Décary-Hétu, D., & Dupont, B. (2023). The benefits of a cyber-resilience posture on negative public reaction following data theft. *Journal of Criminology*, *56*(*4*), 470–493. https://doi.org/10.1177/26338076231161898

Ulsch, M. (2014). *Cyber threat! How to manage the growing risk of cyber attacks* (1st ed.). Wiley. https://doi.org/10.1002/9781118915028

Vuță, D. R., Nichifor, E., Țierean, O. M., Zamfirache, A., Chițu, I. B., Foris, T., & Brătucu, G. (2022). Extending the frontiers of electronic commerce knowledge through cybersecurity. *Electronics*, *11*(14), Article 2223. https://doi.org/10.3390/electronics11142223