Journal of Systemics, Cybernetics and Informatics (2025) 23(2), 73-83
https://doi.org/10.54808/JSCI.23.02.73

Conceptual Model of the Company's Cyber Resilience Elements

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

This study is a continuation of the paper from last year's conference "Cyber Risks: Systematic Literature Analysis". The work considered the process and risks of digitalization. As a result, definitions of cyber risks and cyber threats, cyber security and cyber resilience were given, and differences between similar concepts were considered. Also, as a result of the work, gaps in current approaches to small and medium enterprise (SME) cyber resilience were identified. To eliminate these gaps, it is necessary to see the full picture, understand which elements are included in the company's security system from cyber threats and are also able to strengthen its cyber resilience against threats and how it is possible to minimize cyber risks. In this work, an attempt will be made to build a conceptual model of cyber resilience of small and medium enterprises, considering the elements of the model and their interrelations and interdependencies.

Keywords: Cyber Resilience, Small and Medium Enterprises (SMEs), Digitalization, Cyber Risks, Cybersecurity, Digital Maturity, Industry 4.0.

1. INTRODUCTION

The digital transformation of business, which has come everywhere with industrialization 4.0, and is commonly referred to as digitalization, has brought numerous benefits and opportunities for business. The benefits include acceleration, scaling of business, simplification of operational processes, and the ability to carry out work processes with lower costs for personnel, meetings with partners, market research and competitor analysis. On the one hand, it may seem that better times are coming for business with the emergence of new opportunities. However, digitalization processes also have a downside. The transition of business to the online environment has brought with it a huge number of risks that many entrepreneurs were not prepared for. Due to operational routine, many entrepreneurs did not have the opportunity to systematically switch to the online environment. Digitalization of business processes occurs chaotically and only as a response to urgent need, and not as a systematic approach to a soft transfer of all processes at the same time with fewer losses. With the development of the digital world, the shadow and criminal sphere of the economy is developing just as rapidly, if not faster. To commit crimes in the cyber environment, criminals need to know not only the technical and legislative aspects of doing business. They need to know the weak points of their potential victims. And while an entrepreneur plans and develops ways to earn and increase profits, in parallel with this, the criminal prepares and waits for the moment when the entrepreneur receives the profit to take it away.

To strengthen its resilience, it is not enough for an entrepreneur to think only about the company's security. It is impossible to protect yourself from a potential criminal completely. The authors believe that it is necessary to ask the question of what to do if a crime has occurred, what losses are possible, and what to do next in order not to lose your position after the losses [1;2].

The authors believe that this requires a systematic, comprehensive approach, looking at the whole problem from above from a bird's eye view. This paper will attempt to consider all elements of the cyber resilience system in small and medium-sized businesses.

Research Questions (RQs)

RQ1: What are the key elements of a conceptual model of cyber resilience for SMEs?

RQ2: How do the relationships and interconnections between these elements contribute to effective cyber risk management?

Research Tasks (RTs)

RT1: Analyze existing literature on cyber resilience, cybersecurity practices, and challenges for SMEs.

RT2: Develop a conceptual model for enhancing cyber resilience in SMEs, focusing on key elements and their interconnections.

This study's subject of research is the development and application of conceptual model for cyber resilience in the context of SMEs.

The object of this research is the cyber risks, cybersecurity practices, digital maturity and resilience strategies employed by SMEs to mitigate and manage digital threats. As the study focuses on understanding the challenges, behaviors, and resilience strategies of SMEs, then SMEs themselves are the object of research. The study examines how SMEs interact with cyber risks, cybersecurity measures, and resilience frameworks.

The goal of this research is to analyze existing literature on cyber resilience, identify gaps and challenges in current approaches, and propose a conceptual model tailored to enhancing the cyber resilience of SMEs in an evolving digital environment.

This study builds upon the previous paper presented at last year's conference, titled "Cyber Risks: Systematic Literature Analysis." That research explored the definitions and nature of concepts such as cybersecurity, cyber resilience, cyber risks, and cyber threats. This paper takes the next step by delving deeper into understanding the entire system of cyber resilience and the components incorporated into its model [3].

2. METHODOLOGY

The primary data source for this study, as in the previous research, was the Scopus database, renowned as the most comprehensive repository for abstracts and citations of peer-reviewed literature. Additionally, supplementary sources, including select books categorized as "gray literature" from the online libraries "O'Reilly" and "Springer," were utilized to enhance the breadth of information examined.

To provide a comprehensive overview of research in the field, the study focused on a 20-year period (2004–2025) when conducting searches in the Scopus database. Only papers with open access were considered. The search methodology consisted of several sequential steps, with each subsequent step building upon the findings of the previous one, gradually addressing the research questions.

Initial Search Step

The first and foundational step for all subsequent searches was to use the term "cyber resilience" as a search string among article titles, abstracts, keywords. It resulted: 1,491 documents. Additional search phrases were incorporated at later stages to refine the results. The authors assumed that individuals, including entrepreneurs, begin prioritizing security when they possess assets that could be at risk. Based on this assumption, the first keyword used in conjunction with "cyber resilience" was "company security," reflecting the company as the object of the study. Search Result: 48 documents found.

Second Search Step

Building on the initial findings, the authors hypothesized that the next stage in the cyber resilience model involves addressing "cyber risks" and "cyber threats." Consequently, the second search combined the keywords "cyber resilience," "cyber risks," and "cyber threats." Search Result: 211 documents found.

Third Search Step

Analyzing the literature on cyber risks and cyber threats led to the realization that "cybersecurity" was a critical next element in the cyber resilience model. This stage involved searching for "cybersecurity" in combination with "cyber resilience." Search Result: 553 documents found

Fourth Search Step

The review of literature on cybersecurity highlighted the importance of "incident response" as the following element in the model. Thus, "operational resilience" was incorporated into the search string alongside "cyber resilience." Search Result: 177 documents found

Final Search Step

The last element explored in the model was "digital maturity." This term was combined with "cyber resilience" to conclude the search process. Search Result: 5 documents found.

In addition to the works retrieved from Scopus, books and articles from the online libraries O'Reilly and Springer were also consulted. Unlike Scopus, these libraries did not impose filters based on the publication date. During each search, the authors entered the phrase "cyber resilience" along with the relevant second keyword or phrase, as specified in the earlier search steps, simultaneously in the search bar. Determining the exact numerical results of the search proved challenging, as the authors prioritized assessing how well the retrieved works addressed the study's objectives and research questions. Not all of the works found were cited; only those that provided answers to the research questions were included. The full list of sources can be found at the end of this study.

3. RESULTS

The reviewed publications focus on critical areas of cybersecurity and resilience, risk assessment, and the integration of emerging technologies. These studies present models designed to enhance cybersecurity and resilience across specific business sectors, including healthcare, energy, transportation, agriculture, and supply chains [4;5] While attention is often given to the unique characteristics of these sectors, the findings from these studies were utilized in this paper to develop a conceptual model of cyber resilience [6].

Significant emphasis is placed on risk assessment and mitigation strategies for critical infrastructures such as power grids, airports, and smart cities. Additionally, the studies explore the potential of emerging technologies, such as the Internet of Things (IoT), artificial intelligence (AI), and digital twin technologies, in combating cyber threats [7;8].

Over the past year, there has been a notable increase in publications focusing on preventive measures and risks that contribute to cyber resilience and the adaptability of small and medium-sized businesses to a high-risk cyber environment. These studies emphasize not only strengthening protection tools and responding to cybercrimes that have already occurred but also fostering proactive resilience.

Furthermore, the involvement of governments in enhancing cyber resilience at the national level is

increasingly highlighted. As cyber risks grow in complexity and scope, their global nature poses significant threats to national security [9].
In this paper, the authors abstract from the specific and unique aspects of the business sectors considered in the reviewed publications and aim to identify common features across all studies. To construct a conceptual model of cyber resilience, no distinction is made between different critical infrastructures (e.g., power grids, airports, healthcare systems) and other cybersecurity issues, such as unauthorized access to company data stored in the cloud.
The authors propose a conceptual model of cyber resilience comprising five key elements: company security, cyber risks and threats, cyber security, incident response and recovery, and digital maturity [10;11].
The following section will examine the key elements that, according to the authors, form a conceptual model of cyber resilience applicable across various domains.

4. FINDINGS

In the previous work, the authors derived definitions of cyber resilience, cybersecurity, cyber risks, and cyber threats based on the publications reviewed. We acknowledge the interconnection between cyber risks and threats, as well as the role of cybersecurity. The definition of cyber resilience was formulated as follows [12]:
Cyber resilience denotes a capacity to endure and recover from cyber threats by integrating anticipation, support, recovery, and adaptation measures within a dynamic cyberspace. While cybersecurity primarily concentrates on defending systems and minimizing data risks, cyber resilience complements these efforts by preparing organizations and individuals to effectively rebound from cyber hazards and ensure system performance despite adversities. This comprehensive approach includes proactive threat response measures before, during, and after incidents, aligning with planning, absorption, recovery, and adaptation stages. Cyber resilience encompasses technological aspects, interdisciplinary research, public debates, and political discourse, thereby safeguarding critical systems and infrastructures from risks inherent in complex socio-technical environments.
Cyber Resilience refers to an organization's ability to prepare for, respond to, and recover from cyber threats, ensuring continuity of critical operations and minimizing the impact of cyber incidents on its systems and operations. It integrates the principles of cybersecurity, operational resilience, and digital maturity to enable organizations to maintain their mission-critical functions despite the occurrence of disruptive cyber events [12;13].
From the definition, it is clear that the concept of cyber resilience encompasses the interacting elements of cyber risks and threats, cybersecurity, responses to incidents, and recovery from cyberattacks. The authors assume that the starting point of this model is the security element of the company.
The need for protection arises when an individual, group of individuals, enterprise, or state possesses assets that are vulnerable to loss. Before the advent of digitalization, the focus was predominantly on protecting material assets. This study assumes that company security is a fundamental element of the cyber resilience model.
Cyber resilience denotes a capacity to endure and recover from cyber threats by integrating anticipation, support, recovery, and adaptation measures within a dynamic cyberspace. While cybersecurity primarily concentrates on defending systems and minimizing data risks, cyber resilience complements these efforts by preparing organizations and individuals to effectively rebound from cyber hazards and ensure system performance despite adversities. This comprehensive approach includes proactive threat response measures before, during, and after incidents, aligning with planning, absorption, recovery, and adaptation stages [7;14]. Cyber resilience encompasses technological aspects, interdisciplinary research, public debates, and political discourse, thereby safeguarding critical systems and infrastructures from risks inherent in complex socio-technical environments [15].

4.1.1. Company security

Company security refers to the implementation of measures designed to protect an organization’s assets, including information, personnel, and physical infrastructure, from threats such as unauthorized access, disruption, or destruction [16]. These measures encompass strategies like deterrence, avoidance, prevention, detection, recovery, and correction, forming a critical part of a comprehensive risk management framework [6;17;18]. Key components include confidentiality, integrity, and availability, with additional attributes such as authenticity, accountability, non-repudiation, usability, and reliability also playing significant roles. In the context of Industry 4.0 and the digitalization of business processes, traditional security risks are now coupled with evolving cyber risks, requiring organizations to adopt robust and adaptive security strategies to ensure operational resilience and the achievement of their critical objectives [1;19;20].

4.1.2. Cyber risks

Building on the concept of company security, cyber risks and threats are critical dimensions in today's digitalized business environment. Cyber risks refer to the potential adverse impacts on organizational operations, assets, individuals, or even the nation due to the loss of confidentiality, integrity, or availability of information systems. These risks encompass financial losses, operational disruptions, and damage resulting from failures in digital technologies used for informational or operational functions [15;22].
In contrast, cyber threats represent the evolving dangers posed by malicious activities in cyberspace, such as cybercrime, cyberterrorism, and espionage. These threats target individuals, organizations, and infrastructure, exploiting vulnerabilities through unauthorized access, destruction, disclosure, or denial of service [22;23].

Unlike cyber risks, which focus on the likelihood and consequences of adverse events, cyber threats emphasize malicious activities and their potential to disrupt digital assets and infrastructure.

Cyber risks and threats, such as data breaches, malware, and insider vulnerabilities, highlight organizational weaknesses and serve as a call to action [24]. These risks necessitate proactive measures to prevent significant damages like financial loss or operational disruption and catalyze the development of a dynamic cybersecurity strategy.

Cybersecurity emerges as the shield, consisting of technologies, policies, and practices that address these vulnerabilities and protect critical assets [6;25].

4.1.3. Cybersecurity

Cybersecurity refers to the measures and strategies designed to protect digital assets, systems, and infrastructure from a wide range of threats, including cybercrime, cyberterrorism, and espionage [26;27]. It involves both technical and non-technical approaches to address risks arising from evolving technologies, human actions, and societal factors [9;27].

At its core, cybersecurity aims to safeguard the confidentiality, integrity, and availability of information and systems by preventing, detecting, and responding to cyber threats effectively. This includes protecting against unauthorized access, use, disclosure, disruption, or destruction of information.

Cybersecurity serves as the foundational shield against cyber threats, focusing on proactive defenses such as encryption, firewalls, access controls, and employee training [28]. However, when preventive measures fail, Incident Response and Recovery become critical [8;29].

4.1.4. Incident response and recovery as operational resilience

Incident response involves detecting, analyzing, and mitigating active cyber threats through containment and remediation, while recovery focuses on restoring normal operations, such as system restorations and data recovery, to minimize downtime and impact. Together, these processes ensure a swift return to business continuity [30]. Beyond incident-specific actions, operational resilience emphasizes the broader capability of organizations to adapt and sustain critical functions despite disruptions, whether caused by cyberattacks, natural disasters, or economic shocks [31]. Unlike reactive approaches like incident response, operational resilience takes a proactive, holistic view, integrating cybersecurity with robust business continuity planning, supply chain management, and workforce flexibility. This shift ensures long-term sustainability, enabling SMEs to thrive even amidst uncertainties [32]. Operational resilience transforms recovery into a strategic advantage, ensuring businesses can adapt, recover, and continue delivering essential services under any circumstance.

Incident response and recovery involve a structured process to identify, manage, and mitigate cybersecurity incidents to restore normal operations efficiently. Operational resilience, as defined by NIST, is the capacity of systems to resist, absorb, recover from, or adapt to adverse events, ensuring that mission-critical functions continue despite disruptions.

Operational resilience transforms recovery into a strategic advantage, helping businesses maintain essential services under any circumstance [5;33].

While operational resilience ensures that an organization can withstand and recover from disruptions, digital maturity focuses on optimizing advanced technologies such as AI, cloud computing, and data analytics to drive long-term performance, competitiveness, and adaptability.

Digital maturity is the next step after operational resilience because it empowers organizations to use technology not just to survive disruptions but to actively drive innovation and growth. By adopting technologies like AI, automation, and data analytics, organizations can enhance decision-making, improve customer experiences, and adapt to changing market dynamics [33;34].

4.1.5. Digital Maturity

Digital maturity refers to an organization's ability to effectively leverage digital technologies to drive value, enhance operations, and foster business transformation. It involves the integration of digital processes, culture, and technologies to support innovation and optimize business performance. It focuses on processes, monitoring and control, technology adoption, and organizational readiness to mitigate cyber risks and threats. Assessing digital maturity enables organizations to identify areas for improvement, align digital initiatives with business objectives, and enhance overall performance [16;35]. In the conceptual model of Cyber Resilience for SMEs, digital maturity plays a key role in fostering sustainable growth by ensuring organizations are not only resilient to current challenges but are also adaptable to emerging risks.

Digital Maturity refers to an organization’s ability to fully integrate advanced technologies to enhance operations, decision-making, and innovation [36]. However, with the adoption of new digital tools and platforms comes an increased exposure to cyber risks, threats, and vulnerabilities. As a result, the concept of a continuous feedback loop between Digital Maturity and Company Security becomes critical.

Each time new technologies are integrated, security policies, cyber defenses, and risk management strategies must be updated to protect digital assets and ensure operational integrity. This process includes strengthening cybersecurity measures, conducting security audits, and adapting to the changing digital landscape.

The feedback loop allows organizations to refine their security strategies and tools to mitigate these risks [4;37]. Additionally, digital maturity requires aligning technology use with security governance structures and organizational goals, ensuring that security practices adapt alongside the company's digital evolution. This loop fosters agility, enabling SMEs to respond quickly to emerging security challenges and maintain long-term sustainability by protecting innovations while reaping the benefits of digital transformation [37;38].

As SMEs progress through digital maturity, they continuously assess their security posture, strengthening defenses and ensuring that their cybersecurity measures keep pace with digital advancements. This ongoing cycle ensures that the organization remains resilient and competitive, safeguarding both current operations and future growth, that the business remains agile, that it maintains robust security standards, and that it can respond to evolving digital threats effectively.

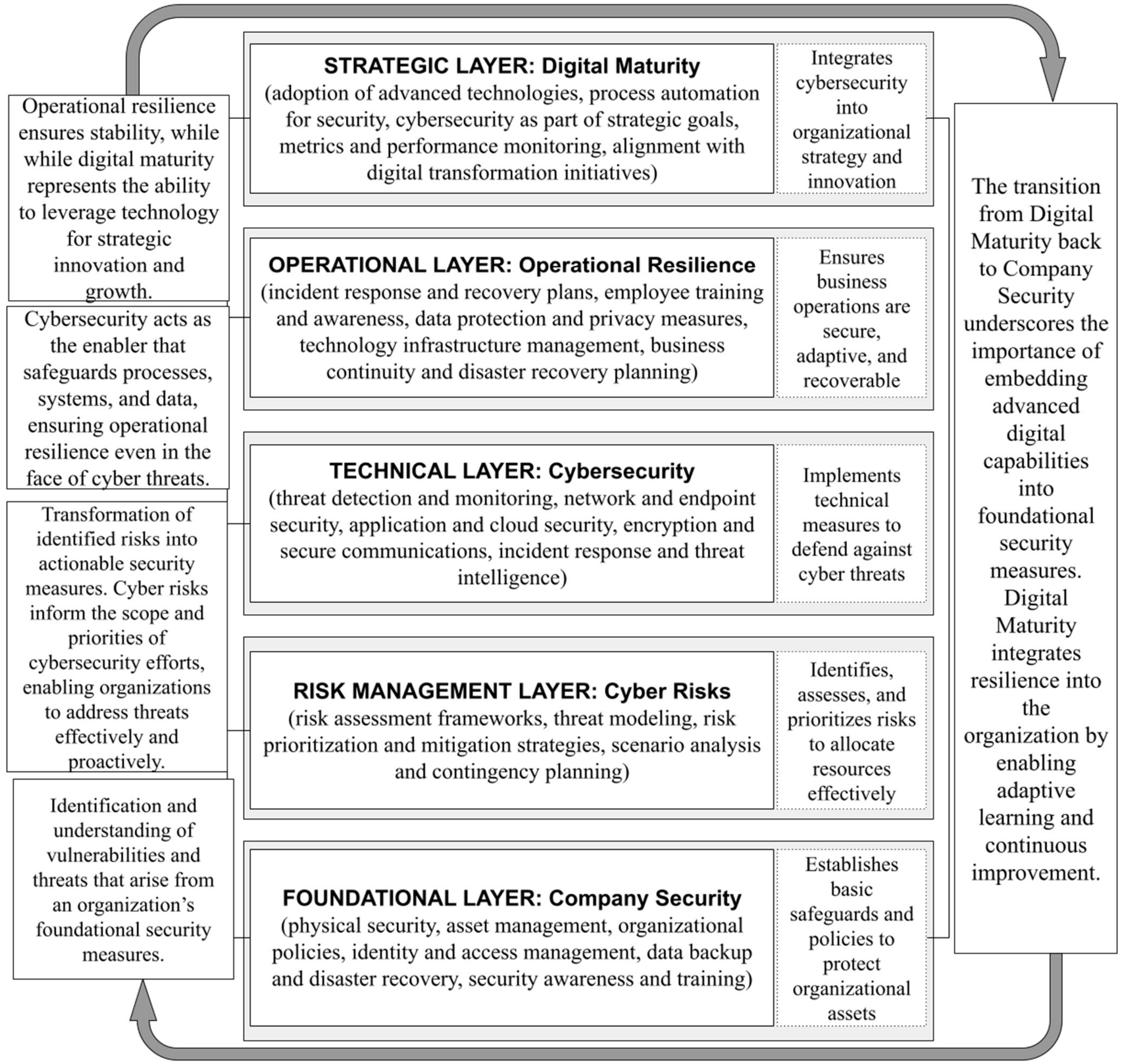

Figure 1: The Continuous Loop of Cyber Resilience in SMEs (Created by Authors)

In this section, the authors have outlined the main elements of the conceptual model of cyber resilience for SMEs, as depicted in Figure 1. The figure illustrates how the five key elements of the model are interconnected, with each element building on the previous one and driving the next. This creates a continuous, iterative process that ensures the ongoing enhancement of the organization's cyber resilience. The model emphasizes that cyber resilience is not a static achievement but a dynamic and evolving framework that requires constant adaptation and improvement to address emerging challenges and risks.

The elements discussed in the above are interconnected not only in the sequential flow that generates each subsequent element but also through more complex relationships [38].

These interconnections create a dynamic, agile model, allowing for stronger linkages between all components. In this section, we will explore these additional, intricate relationships within the conceptual model of SME cyber resilience, emphasizing how they contribute to the overall strength and flexibility of the model.

4.2.1. Company security (Foundation)

Company Security - Cyber Risks

Company security plays a pivotal role in mitigating cyber risks by proactively identifying and addressing internal vulnerabilities. By reducing the attack surface—such as weaknesses in software, hardware, or processes—it helps prevent cyber threats from exploiting these vulnerabilities. The identification of cyber risks triggers necessary updates to security policies, tools, and infrastructure, reinforcing the organization's defenses [39;40]. These risk identification and mitigation strategies form a feedback loop, ensuring the security system continuously adapts to evolving threats.

Company Security - Cybersecurity

Company Security provides the critical foundation for implementing effective cybersecurity measures. A strong internal security framework, which includes well-defined policies such as access control and secure network architecture, enables the organization to deploy essential cybersecurity tools [40]. These tools—firewalls, antivirus software, encryption protocols, and intrusion detection systems—are vital to protect the organization's digital assets. A robust company security framework ensures that these tools are effectively integrated and operational, creating a secure digital environment in which all cybersecurity measures function optimally [3;41;42].

Company Security - Operational Resilience

A well-established company security framework directly supports Operational Resilience by ensuring that effective incident response and recovery processes are in place. By preventing or minimizing the severity of cyber incidents, strong security measures reduce the impact on operations. In the event of a disruption, the recovery process draws from lessons learned during the incident, leading to improvements in the security infrastructure. This cyclical process of continuous improvement not only strengthens the organization's ability to recover but also enhances its overall resilience against future disruptions [43;44].

Company Security - Digital Maturity

Company security is foundational to developing and maintaining cyber maturity within the organization. By establishing basic security controls, such as secure networks and data encryption, the company lays the groundwork for the integration of more advanced digital technologies. As the organization matures digitally, security policies, processes, and training programs evolve to address new challenges [45]. Cyber maturity involves an ongoing effort to upgrade security measures in line with technological advances and emerging risks. This continuous evolution ensures that the organization remains capable of addressing current and future cybersecurity needs as it integrates more sophisticated digital tools.

These interrelationships highlight the importance of company security as the cornerstone of the entire cyber resilience framework. Company security not only acts as the bedrock for addressing cyber risks and deploying cybersecurity defenses, but it also supports the organization's ability to maintain operational continuity and evolve digitally.

4.2.2. Cyber risks (Catalyst)

Cyber Risks - Company Security

The awareness of cyber risks is a crucial catalyst for identifying vulnerabilities and gaps within an organization's foundational security. Recognizing these risks, organizations can craft a strong security framework that mitigates these threats. This awareness forms the foundation for ensuring that security policies are tailored to the specific needs and vulnerabilities exposed by identified risks [45].

Cyber Risks - Cybersecurity

The identification and assessment of cyber risks directly influence the design and implementation of cybersecurity measures. Firewalls, intrusion detection systems, and data encryption, are chosen and deployed based on the nature of the identified risks [46]. These defenses form the first line of protection against vulnerabilities and external threats. Cyber risks, therefore, act as the key input in creating a cybersecurity architecture that is specifically aligned with the organization's most pressing threats and weaknesses [47].

Cyber Risks - Operational Resilience

Awareness of cyber risks plays a critical role in shaping the organization's approach to incident response and recovery. By identifying potential risk scenarios and understanding their possible impact, organizations can develop more effective strategies for responding to and recovering from cyber incidents [3;47;48]. The lessons learned from recovery processes can help refine the organization's risk management framework. The ability to effectively manage and respond to cyber incidents enhances the organization's capacity to bounce back from disruption [49;50;51].

Cyber Risks - Digital Maturity

Cyber risks are a powerful force in driving the organization towards greater digital maturity. By exposing weaknesses in processes, technologies, and behaviors, these risks challenge the organization to continuously evolve. Cyber maturity enables the organization to better understand and manage these risks through systematic threat modeling, risk assessments, and strategic planning [51;52;53]. As the organization matures, it becomes better equipped to identify emerging risks and integrate advanced digital tools and practices to mitigate them. In this way [56].

4.2.3. Cyber security (Shield)

Cybersecurity - Company Security

Company security provides the foundational infrastructure and policies that cybersecurity is built upon. Secure access controls, data encryption protocols, and employee awareness programs form the essential components of the internal security architecture. Cybersecurity then acts as a protective layer, reinforcing these foundational security measures by addressing external threats and vulnerabilities. It ensures that the internal systems, which company security has established, are adequately defended against potential cyberattacks and other digital threats that could compromise the organization's operations.

Cybersecurity - Cyber Risks

Cyber risks directly inform the configuration and focus of cybersecurity defenses. By identifying specific threats and vulnerabilities, cyber risks guide the deployment of targeted cybersecurity measures. Cybersecurity then mitigates these risks by proactively addressing vulnerabilities and preventing breaches before they occur [3;56] In this context, cybersecurity tools and strategies, such as firewalls, intrusion detection systems, and encryption, are deployed specifically to counteract the identified risks, forming an essential shield that defends against potential breaches [56;57].

Cybersecurity - Operational Resilience

Cybersecurity measures are essential in detecting, preventing, and mitigating potential threats, which, in turn, reduces the frequency and severity of cyber incidents. When security breaches or disruptions do occur, the robust defenses put in place by cybersecurity enable organizations to focus on incident response and recovery rather than emergency containment [4]. A strong cybersecurity framework minimizes the impact of incidents by ensuring that systems are protected and resilient, thus supporting an effective recovery process and ensuring business continuity [56;57].

Cybersecurity - Digital Maturity

Digital maturity plays a vital role in enhancing cybersecurity by promoting the adoption of advanced technologies and the improvement of organizational processes. As organizations progress in their digital maturity journey, they integrate better security practices and tools, resulting in a more robust defense mechanism [58]. Cybersecurity, in turn, strengthens digital maturity by providing the necessary systems and tools that support a structured and scalable approach to managing digital threats. This mutual relationship between cybersecurity and digital maturity ensures that the organization's security framework evolves to meet emerging threats and challenges as the organization becomes more digitally advanced.

4.2.4. Incident Response and Recovery (Operational Resilience)

Incident Response and Recovery - Company Security

Cyber risks play a significant role in shaping the priorities of Incident Response, ensuring that the organization is prepared for the most relevant and impactful threats. By identifying and understanding the risks, company security helps define which incidents need to be prioritized during the response phase. Incident Response works to reduce the impact of these cyber risks by containing threats, mitigating the damage, and facilitating a swift recovery [49]. The strength of company security thus directly influences the effectiveness of incident response efforts, ensuring that the organization can recover quickly and effectively from disruptions [48;56].

Incident Response and Recovery - Cyber Risks

Cyber risks drive the focus and priorities of incident response, ensuring that the organization is ready to address the most pressing and likely threats. Incident response reduces the impact of these risks by quickly identifying and containing threats before they can cause significant damage [51;52]. Furthermore, by continuously assessing the evolving risk landscape, incident response can better inform future risk management strategies, ensuring that identified vulnerabilities are addressed and the organization is prepared for future disruptions [53].

Incident Response and Recovery - Cybersecurity

Cybersecurity measures, such as firewalls, intrusion detection systems, and antivirus software, play a crucial role in the early detection and containment of threats, enabling a faster and more effective incident response. These cybersecurity tools form the first line of defense, helping the organization identify potential incidents before they escalate. At the same time, incident response provides valuable feedback to cybersecurity, identifying weaknesses in existing defense mechanisms [54]. This feedback leads to continuous improvements in security tools, systems, and technologies, enhancing the organization's ability to detect and respond to future threats.

Incident Response and Recovery - Digital Maturity

Cyber maturity strengthens incident response by introducing structured processes, advanced tools, and a skilled workforce that is equipped to handle incidents effectively. As organizations advance in their digital maturity, they integrate more sophisticated incident management processes, ensuring that they can respond to and recover from incidents with greater efficiency [18;55]. Incident response and recovery also drive the development of cyber maturity by providing insights after each incident [31;56]. These insights lead to process optimization, system improvements, and organizational learning, reinforcing the organization's ability to respond effectively to future disruptions.

4.2.5. Digital Maturity (Growth)

Digital Maturity - Company Security

Cyber maturity plays a vital role in enhancing the design and optimization of foundational security practices. A mature organization continually revisits and updates its internal security policies and infrastructure to stay aligned with evolving risks, technological advancements, and compliance standards [46;55]. As digital maturity progresses, the organization is better equipped to anticipate new challenges, making it more capable of refining and strengthening its security framework to protect against emerging threats and vulnerabilities. This ongoing improvement helps establish a resilient security infrastructure that evolves alongside the organization's digital transformation.

Digital Maturity - Cyber Risks

Cyber maturity represents an organization's ability to understand, adapt to, and manage cyber risks. As organizations grow in maturity, their ability to identify and analyze risks improves, fostering a proactive approach to cybersecurity [57]. With advanced maturity, the organization's processes for performing threat modeling, conducting periodic risk assessments, and evaluating potential impacts become more sophisticated and comprehensive. This heightened capability enables the organization to detect, evaluate, and mitigate risks more effectively [58]. As the organization matures, its capacity to understand and manage risks also strengthens, allowing for a more strategic and informed approach to cybersecurity.

Digital Maturity - Cybersecurity

At higher levels of Cyber Maturity, organizations are better positioned to implement advanced, integrated cybersecurity tools and strategies. Mature organizations leverage their growth to adopt proactive technologies, such as AI-based threat detection, and refine cybersecurity processes, such as real-time monitoring and automated patch management. This increased sophistication enhances the organization's ability to respond to evolving threats and better protect its digital assets. With greater maturity, the organization can move beyond basic defenses to deploy more intelligent, adaptive security measures that keep pace with emerging challenges in the cyber threat landscape [48;50].

Digital Maturity - Incident Response and Recovery

Cyber maturity directly influences the organization's approach to incident response and recovery by providing a structured and strategic framework. The lessons learned from each incident are invaluable for advancing cyber maturity. Post-incident analyses help uncover gaps in defenses, processes, or employee behavior, driving improvements in training, tools, and response plans. As organizations mature, they integrate these lessons into their ongoing operations, optimizing their incident management processes and strengthening their resilience. Each incident serves as an opportunity for growth, enabling the organization to refine its response strategies and enhance overall operational readiness [36;37].

Cyber maturity acts as the growth engine for an organization's cybersecurity capabilities. As cyber maturity progresses, so too does the organization's ability to adapt to new challenges and remain agile in the face of evolving cyber threats [49].

5. DISCUSSION

The conceptual model of cyber resilience for SMEs, as described in the preceding sections, provides a holistic and interconnected framework for understanding the interconnectedness of critical cybersecurity elements and their role in fostering long-term organizational resilience [5]. By emphasizing the continuous feedback loops between company security, cyber risks, cybersecurity, incident response and recovery, and cyber maturity, the model provides SMEs with a dynamic and agile approach to managing digital risks [3;41;59].

One of the key insights from the model is the recognition that cyber resilience is not a static achievement but a dynamic and ongoing process. As SMEs adopt new technologies and integrate more advanced digital systems into their operations, the cyber resilience model underscores the importance of continuous feedback loops [1;48]. These loops connect various elements— company security, cyber risks, cybersecurity, incident response and recovery, and digital maturity—ensuring that as one element progresses, the others evolve accordingly. This interconnectedness provides SMEs with the agility needed to adapt to new threats, risks, and opportunities.

Unlike larger organizations that may have dedicated resources for each aspect of cybersecurity, SMEs often face resource constraints that can make maintaining this continuous loop more challenging. The ability to continually update security policies, implement advanced threat detection tools, and recover from incidents requires an ongoing commitment to both technological upgrades and employee training [34;42]. Despite these challenges, the model emphasizes the importance of integrating these practices into the broader business strategy to ensure that cybersecurity is not an afterthought but an integral part of the organization's long-term goals.

A critical takeaway from the model is the role of cybersecurity in enabling digital transformation. As SMEs evolve digitally, they increasingly rely on cloud services, AI, and data analytics, among other technologies. While these advancements offer significant benefits, they also introduce new vulnerabilities and risks. The integration of cybersecurity into the digital transformation process allows SMEs to not only protect their digital assets but also ensure that their innovation initiatives remain secure and sustainable [35].

For instance, the adoption of AI-based threat detection tools can enhance an SME's ability to proactively monitor its digital environment, identify emerging threats, and respond quickly [8;25]. This proactive approach strengthens the company's competitive advantage and helps avoid potential disruptions that could arise from cyber incidents. In this way, cybersecurity does not just act as a shield but also as a driver of growth and digital maturity. It enables SMEs to confidently embrace new technologies and innovation, knowing that they have a resilient and adaptive security framework in place.

The concept of cyber maturity is particularly significant in the context of SMEs [24;30]. As organizations mature digitally, they inevitably face new challenges that test their ability to respond to increasingly sophisticated threats. Cyber maturity involves not only the adoption of advanced technologies but also the continuous refinement of processes and the development of organizational skills. For SMEs, this means that cybersecurity becomes an ongoing process, where each stage of maturity builds upon the previous one, creating a cycle of improvement that enhances overall resilience [39;51].

However, achieving cyber maturity requires more than just technological upgrades. It necessitates a cultural shift towards prioritizing security at all levels of the organization. Senior management must recognize the value of investing in cybersecurity and fostering a security-conscious culture. Employees, from entry-level staff to executives, must be trained to recognize potential threats and understand the importance of adhering to security protocols. This holistic approach to cyber resilience ensures that all aspects of the organization are aligned in their efforts to build and maintain a secure, adaptive infrastructure.

One of the most valuable aspects of the cyber resilience model is its emphasis on incident response and recovery. In the face of inevitable breaches or disruptions, SMEs must not only contain and recover from incidents but also learn from them. Post-incident analysis allows organizations to identify gaps in their defenses, improve response strategies, and refine their security practices. The lessons learned from incidents contribute directly to the organization's growth, as they provide insights into the weaknesses that need to be addressed in future security measures.

This cyclical process of learning from incidents strengthens the organization's overall resilience. SMEs are not only recovering from threats but also reinforcing their defenses to prevent future occurrences [32].

The offered model underscores the importance of being proactive rather than reactive in addressing cybersecurity challenges. In an increasingly complex digital landscape, SMEs can no longer afford to adopt a “wait-and-see” approach when it comes to security [33;48]. As cyber threats evolve in sophistication and frequency, SMEs must be prepared to anticipate risks, deploy preventive measures, and continuously monitor their digital environments.

A proactive approach involves regular risk assessments, security audits, and vulnerability testing to identify potential weaknesses before they are exploited by malicious actors. Furthermore, SMEs must stay informed about the latest cybersecurity trends, tools, and best practices to ensure that their defenses are up to date. The cyber resilience model highlights that this proactive stance, coupled with the feedback loops discussed earlier, helps SMEs stay ahead of emerging threats and maintain operational continuity [44].

While the benefits of the cyber resilience model are clear, SMEs face several challenges in implementing and maintaining these practices. Limited resources, budget constraints, and a lack of specialized expertise can hinder their ability to fully integrate advanced cybersecurity measures [6;22]. However, the model offers opportunities for SMEs to scale their resilience efforts gradually. By adopting a step-by-step approach, SMEs can begin with foundational security practices, such as implementing basic access controls and employee awareness training, and then build upon these with more advanced technologies and processes as their digital maturity grows. Additionally, collaboration with external cybersecurity experts, partnerships with industry associations, and leveraging affordable cybersecurity solutions can help SMEs overcome resource limitations and bolster their defenses [4;23].

The model serves as a roadmap for SMEs to navigate the complexities of digital transformation while safeguarding their assets and operations.

6. CONCLUSIONS

This study aimed to explore the key elements of a conceptual model for cyber resilience in SMEs and understand the interconnections between these elements that contribute to effective cyber risk management. By examining the relationships between company security, cyber risks, cybersecurity, incident response and recovery, and digital maturity, the research provides insights into how SMEs can enhance their resilience against cyber threats.

Through an analysis of existing literature and conceptual frameworks, this study identified that cyber resilience in SMEs is not a static, one-time achievement but rather a dynamic, continuous process that requires constant feedback and adaptation. The relationships between the elements of the model highlight the interconnectedness of security practices, risk management strategies, and the role of incident response in strengthening overall resilience. The model provides a foundational framework that SMEs can use to enhance their cybersecurity posture and better prepare for future digital challenges. With this, the research questions have been answered.

The findings presented here will serve as a valuable starting point for deeper investigations into how SMEs can develop robust, adaptive, and sustainable cybersecurity practices.

However, this study is not a comprehensive exploration of the subject and serves as an initial step toward a deeper, more detailed analysis of the factors influencing cyber resilience in SMEs. There are several limitations to the current research. Firstly, the model presented in this study is conceptual and theoretical, meaning it requires further empirical testing and validation in real-world SME settings. Additionally, the scope of the study is limited to secondary data analysis and existing frameworks, which leaves room for future research to expand on the practical application of the model.

Future research could explore the effectiveness of the proposed model in various SME contexts, investigate the role of organizational culture in fostering cyber resilience, and evaluate the impact of specific cybersecurity tools and practices on improving resilience. Furthermore, a longitudinal approach could provide insights into how cyber resilience evolves over time and the long-term benefits of adopting a comprehensive resilience strategy.

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] S. Pettersen and T. O. Grøtan, **Exploring the grounds for cyber resilience in the hyper-connected oil and gas industry**, Saf Sci, vol. 171, 2024.

[2] A. Kokaji and A. Goto, **An analysis of economic losses from cyberattacks: based on input–output model and production function**, J Econ Struct, vol. 11, no. 1, 2022.

[3] A. Bahmanova and N. Lace, **Cyber Risks: Systematic Literature Analysis**, in Proceedings IMCIC - International Multi-Conference on Complexity, Informatics and Cybernetics, 2024.

[4] S. Silvestri, S. Islam, D. Amelin, G. Weiler, S. Papastergiou, and M. Ciampi, **Cyber threat assessment and management for securing healthcare ecosystems using natural language processing**, Int J Inf Secur, vol. 23, no. 1, pp. 31–50, 2024.

[5] S. AlDaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger, and K.-K. Raymond Choo, **The role of national cybersecurity strategies on the improvement of cybersecurity education**, Comput Secur, vol. 119, 2022.

[6] A. Alshawish and H. de Meer, **Risk mitigation in electric power systems: Where to start?**, Energy Informatics, vol. 2, no. 1, 2019.

[7] K. Awiszus, Y. Bell, J. Lüttringhaus, G. Svindland, A. Voß, and S. Weber, **Building resilience in cybersecurity: An artificial lab approach**, Journal of Risk and Insurance, vol. 91, no. 3, pp. 753–800, 2024.

[8] A. Mehmood, G. Epiphaniou, C. Maple, N. Ersotelos, and R. Wiseman, **A Hybrid Methodology to Assess Cyber Resilience of IoT in Energy Management and Connected Sites**, Sensors (Basel), vol. 23, no. 21, 2023.

[9] M. Ramírez, L. R. Ariza, M. E. G. Miranda, and Vartika, **The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index**, Sustainability (Switzerland), vol. 14, no. 3, 2022.

[10] National Institute of Standards and Technology, **Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy**, NIST SP 800-37 Revision 2, 2018.

[11] M. Erbas, S. M. Khalil, and L. Tsiopoulos, **Systematic literature review of threat modeling and risk assessment in ship cybersecurity**, Ocean Engineering, vol. 306, 2024.

[12] R. U. Maheshwari, P. R. Shankar, G. Chandrasekaran, and K. Mahendrakhan, **Assessment of Cybersecurity Risks in Digital Twin Deployments in Smart Cities**, International Journal of Computational and Experimental Science and Engineering, vol. 10, no. 4, pp. 695–700, 2024.

[13] M. Alsharif, S. Mishra, and M. AlShehri, **Impact of Human Vulnerabilities on Cybersecurity**, Computer Systems Science and Engineering, vol. 40, no. 3, pp. 1153–1166, 2021.

[14] D. Blum, **Rational Cybersecurity for Business,** The Security Leaders' Guide to Business Alignment. 2020.

[15] National Institute of Standards and Technology, **Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Security Requirements for Nonfederal Systems**, NIST SP 800-171 Revision 3, 2023.

[16] National Institute of Standards and Technology, **Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems**, NIST SP 800-160 Volume 2 Revision 1, 2021.

[17] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, **Smart airport cybersecurity: Threat mitigation and cyber resilience controls**, Sensors (Switzerland), vol. 19, no. 1, 2019.

[18] N. Marshall, D. Sturman, and J. C. Auton, **Exploring the evidence for email phishing training: A scoping review**, Comput Secur, vol. 139, 2024.

[19] B. A. Kazancı, **The Strategic Importance of Cyber Security in Electric Energy Policies**, International Journal of Energy Economics and Policy, vol. 14, no. 4, pp. 599–605, 2024.

[20] A. Veeramany et al., **Framework for modeling high-impact, low-frequency power grid events to support risk-informed decisions**, International Journal of Disaster Risk Reduction, vol. 18, pp. 125–137, 2016.

[21] A. Creazza, C. Colicchia, S. Spiezia, and F. Dallari, **Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era**, Supply Chain Management, vol. 27, no. 1, pp. 30–53, 2022.

[22] D. P. Sharma, A. Habibi Lashkari, and M. Parizadeh, **Understanding Cybersecurity Management in Healthcare**, Cham: Springer Nature Switzerland, 2024.

[23] B. Luuk, V. H.-D. G. (Maria) Susanne, M.-T. H. Ellen, V. H. Ynze, S. Remco, and L. Eric Rutger, **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**, Comput Secur, vol. 127, 2023.

[24] R. Faleiro, L. Pan, S. R. Pokhrel, and R. Doss, **Digital Twin for Cybersecurity: Towards Enhancing Cyber Resilience**, 2022, pp. 57–76.

[25] N. Uraipan, P. Praneetpolgrang, and T. Manisri, **Application of a fuzzy analytic hierarchy process to select the level of a cyber resilient capability maturity model in digital supply chain systems**, ECTI Transactions on Computer and Information Technology, vol. 15, no. 2, pp. 198–207, 2021.

[26] I. H. Sarker, H. Janicke, A. Mohsin, A. Gill, and L. Maglaras, **Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects**, ICT Express, vol. 10, no. 4, pp. 935–958, 2024.

[27] H. T. Bui et al., **Agriculture 4.0 and beyond: Evaluating cyber threat intelligence sources and techniques in smart farming ecosystems**, Comput Secur, vol. 140, 2024.

[28] 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, pp. 1315–1331, 2024.
[29] National Institute of Standards and Technology, **Developing Cyber-Resilient Systems: A Systems Security Engineering Approach**, NIST Special Publication 800-160, Vol. 2, Rev. 1, Nov. 2021.
[30] M. Dacorogna, N. Debbabi, and M. Kratz, **Building up cyber resilience by better grasping cyber risk via a new algorithm for modelling heavy-tailed data**, Eur J Oper Res, vol. 311, no. 2, pp. 708–729, 2023.
[31] H. Mouratidis, J. Zdravkovic, and J. Stirna, **Cyber Security Resilience in Business Informatics: An Exploratory Paper**, 2020, pp. 53–66.
[32] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, **A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience**, Sensors, vol. 23, no. 16, 2023.
[33] M. Ahmed, O. Kazar, and S. Harous, **Cyber-physical system model based on multi-agent system**, IET Cyber-Physical Systems: Theory and Applications, vol. 9, no. 4, pp. 424–434, 2024.
[34] S. Durst, C. Hinteregger, and M. Zieba, **The effect of environmental turbulence on cyber security risk management and organizational resilience**, Comput Secur, vol. 137, 2024.
[35] K. Awiszus, Y. Bell, J. Lüttringhaus, G. Svindland, A. Voß, and S. Weber, **Building resilience in cybersecurity: An artificial lab approach**, Journal of Risk and Insurance, vol. 91, no. 3, pp. 753–800, 2024.
[36] M. Baezner, **Cybersecurity in switzerland: Challenges and the way forward for the swiss armed forces**, Connections, vol. 19, no. 1, pp. 63–72, 2020.
[37] C. Joyce, F. L. Roman, B. Miller, J. Jeffries, and R. C. Miller, **Emerging Cybersecurity Threats in Radiation Oncology**, Adv Radiat Oncol, vol. 6, no. 6, 2021.
[38] S. Mishra, K. Anderson, B. Miller, K. Boyer, and A. Warren, **Microgrid resilience: A holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies**, Appl Energy, vol. 264, 2020.
[39] A. Erola, I. Agrafiotis, J. R. C. Nurse, L. Axon, M. Goldsmith, and S. Creese, **A system to calculate cyber-value-at-risk**, Comput Secur, vol. 113, 2022.
[40] K. Adamos, G. Stergiopoulos, M. Karamousadakis, and D. Gritzalis, **Enhancing attack resilience of cyber-physical systems through state dependency graph models**, Int J Inf Secur, vol. 23, no. 1, pp. 187–198, 2024.
[41] S. Park and H. Park, **PIER: cyber-resilient risk assessment model for connected and autonomous vehicles**, Wireless Networks, vol. 30, no. 5, pp. 4591–4605, 2024.
[42] F. Cremer, B. Sheehan, M. Mullins, M. Fortmann, B. J. Ryan, and S. Materne, **On the insurability of cyber warfare: An investigation into the German cyber insurance market**, Comput Secur, vol. 142, 2024.
[43] E. Karyani, T. Faturohman, A. Noveria, and R. A. Rahadi, **Financial resilience in ASEAN-4 banking sector: Impact of cyber risk disclosure**, Kasetsart Journal of Social Sciences, vol. 45, no. 3, pp. 901–914, 2024.
[44] I. H. Sarker, H. Janicke, A. Mohsin, A. Gill, and L. Maglaras, **Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects**, ICT Express, vol. 10, no. 4, pp. 935–958, 2024.
[45] G. Vardakis, G. Hatzivasilis, E. Koutsaki, and N. Papadakis, **Review of Smart-Home Security Using the Internet of Things**, Electronics (Switzerland), vol. 13, no. 16, 2024.
[46] M. Gombár, A. Vagaská, A. Korauš, and P. Račková, **Application of Structural Equation Modelling to Cybersecurity Risk Analysis in the Era of Industry 4.0**, Mathematics, vol. 12, no. 2, 2024.
[47] M. Rubakha, L. Tkachyk, I. Pryimak, N. Demchyshak, and 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, pp. 260–281, 2024.
[48] H. Taherdoost, **A Critical Review on Cybersecurity Awareness Frameworks and Training Models**, in Procedia Computer Science, 2024.
[49] M. Belesioti, J. Carapinha, R. Makri, and I. P. Chochliouros, **The Challenge of Security Breaches in the Era of 5G Networking**, 2021.
[50] I. Buzhin, M. Bessonov, Y. Mironov, and M. P. Farkhadov, **Integrity, Resilience and Security of 5G Transport Networks Based on SDN/NFV Technologies**, 2022.
[51] P. M. Datta, **Global Technology Management 4.0**, Cham: Springer International Publishing, 2022.
[52] R. T. Kreutzer, **Toolbox Digital Business**. Wiesbaden: Springer Fachmedien Wiesbaden, 2022.
[53] M. D. Tugrul U Daim, **Cybersecurity. A Technology Landscape Analysis**. Cham: Springer International Publishing, 2023.
[54] Praz, **Link Technology to Your Long-Term Business Goals**. Apress Berkeley, CA, 2022.
[55] Thomas Schneider, **Digitalization and Artificial Intelligence**. Springer Gabler Wiesbaden, 2023. Accessed: Dec. 25, 2024.
[56] T. Schneider, **Data Security**, in Digitalization and Artificial Intelligence : Use by and in Controlling, T. Schneider, Ed., Wiesbaden: Springer Fachmedien Wiesbaden, 2023.
[57] M. Alsharif, S. Mishra, and M. AlShehri, **Impact of Human Vulnerabilities on Cybersecurity**, Computer Systems Science and Engineering, vol. 40, no. 3, pp. 1153–1166, 2021.
[58] E. Skare and S. Haugdal Jore, **Hybrid threats in the Norwegian petroleum sector. A new category of risk problems for safety science?**, Saf Sci, vol. 176, 2024.