The High Stakes of Cyber Resilience: What Key Business Assets Can SMEs Afford to Lose?

Alona Bahmanova, Natalja Lace

Faculty of Engineering Economics and Management, Riga Technical University, Riga, LV-1048, Latvia
alona.bahmanova@gmail.com
Received date: Feb 12, 2024, revision date: April 4, 2024, Accepted: May 15, 2024

ABSTRACT

The rapid advancement of technology and digitalization has significantly accelerated product and service creation cycles, reducing time and costs. In manufacturing, robots streamline recruitment and training, while in the service sector, businesses can scale globally without geographic constraints. Management and technical decisions are increasingly guided by artificial intelligence (AI) and the Internet of Things (IoT), integrating digitalization into both household and business tasks. However, this technological progress has also led to carelessness and over-reliance on technology. Despite benefits like increased efficiency, cost reduction, and scalability, the associated risks of digitalization are often overlooked by entrepreneurs. Dependence on continuous digital workflows means that any failure can cripple entire systems, leading to financial losses, halted processes, staff panic, reputational damage, and legal issues. This study aims to identify the key business assets within SMEs most vulnerable to cyber threats and to emphasize the importance of building cyber resilience. Through a literature review and content analysis, we categorized SME assets into seven areas: Digital Infrastructure and Systems, Cybersecurity and Intellectual Property, Business Operations and Continuity, Reputation and Compliance, Financial and Economic Impact, Risk and Resilience Management, Human Resources and Customer Relations. The findings highlight the necessity for Small and Medium-sized Enterprises (SMEs) to develop robust cyber resilience strategies to protect these critical assets.

Keywords: digitalization, cyber resilience, business assets, cyber vulnerabilities, asset management.

1. Introduction

With the advancement of technology and the digitalization of production and business processes, the cycles for creating products and services have accelerated, significantly reducing both time and production costs. In manufacturing, robots are increasingly replacing humans, streamlining recruitment and training processes. In the service sector, businesses can now scale up and offer services without being constrained by geographic location. Management decisions are increasingly informed by processed information, with artificial intelligence and predictions derived from big data analysis. Similarly, technical decisions are guided by artificial intelligence (AI) and the Internet of Things (IoT). Digitalization has swiftly integrated into our lives, simplifying tasks at both household and business levels, while we continue to be fascinated by new inventions and the speed of information processing. However, the conveniences brought by technological progress in the era of Industry 4.0 have also led to a certain level of carelessness and over-reliance on technology.

Despite the numerous benefits of digitalization, such as increased efficiency, cost reduction, and the ability to scale businesses globally, it is crucial to consider the associated risks. The convenience and speed of digital processes often lead entrepreneurs to overlook potential downsides. The heavy reliance on continuous digital workflows means that any failure can temporarily cripple the entire system. Entrepreneurs may face substantial financial losses, halted work processes, staff panic, reputational damage, and legal complications.

This study raises important questions for reflection: what key business assets can small and medium-sized enterprises afford to lose? Amid the daily operational processes, do entrepreneurs consider what they might lose? The focus is often placed on generating revenue, rather than on contemplating potential losses.

The research object of this study is the business assets of small and medium-sized enterprises (SMEs) that are vulnerable to cyber threats.

The aim of this research is to explore which business assets in SMEs are most vulnerable to cyber threats and highlight the importance of cyber resilience in protecting these assets.

Research Tasks are as follows:

- Identify the key business assets at risk in SMEs.
- Examine the importance of cyber resilience.

To achieve the research goal, this study will employ a literature review and content analysis approach. This will involve gathering insights from existing research and analyzing data from various business sectors regarding cyber resilience. The study will synthesize the findings to provide a comprehensive understanding of the cyber risks faced by SMEs.

The central research question (RQ) guiding this study is: "What types of business assets are most vulnerable to cyber threats in SMEs?"

2. Research Methodology

The study employed the Scopus database for literature selection, conducting searches across publication titles, abstracts, and keywords.

1. Initially, the search was filtered using the keyword "cyber AND resilience," yielding 3,969 documents.
2. Subsequently, the search was refined to include only open-access documents, resulting in 1,288 articles.
3. Further narrowing focused on documents written in English, identifying 1,277 relevant articles.
4. Adding the keyword "assets" further narrowed the focus to 63 relevant documents.

There were no restrictions on the publication year. Upon further examination, it was found that not all 63 papers provided the necessary information. As a result, content analysis was conducted based on 29 relevant papers, with additional publications identified through citation tracking within the selected papers.

The content analysis process involved categorizing assets based on the selected articles, which allowed for the identification of asset categories and the assessment of their frequency and specific relevance. To gain a deeper understanding of each category, additional searches were conducted in Scopus. These searches used the keyword "cyber resilience" along with specific categories of interest.

3. Results

Twenty-nine relevant publications were analyzed to identify categories of SME assets exposed to cyber risks and threats. Assets vulnerable to cyber risks typically involve digital or cyber elements that can be targeted or compromised, potentially leading to disruptions, financial losses, reputational damage, or other adverse consequences.

Content analysis was employed to determine these categories. This method, which is both systematic and involves quantitative and qualitative analysis, helps to understand the presence, meanings, and relationships

of specific words, themes, or concepts within the texts. Through this process, the context, patterns, and trends within the literature were discerned.

Due to the publications' content analysis, twenty-four categories were identified:

1. Smart contracts;
2. Micro-payment infrastructure;
3. Distributed energy resources (DERs);
4. Blockchain;
5. Intellectual property;
6. Branding secure products;
7. Simulation-based disruption management systems;
8. Cloud-based manufacturing execution systems (MES);
9. SCADA systems (Supervisory control and data acquisition);
10. Supply chains;
11. Company's staff;
12. Digital Twin (DT), Cyber Range (CR);
13. Company reputation;
14. Customer requirements and interests;
15. Regulatory and legal repercussions;
16. Financial losses;
17. AI/ML systems;
18. Cyber-Physical Production System (CPPS);
19. Internet of Things (IoT), Industrial Internet of Things (IIoT);
20. Third-party risks;
21. Interrupt business / production processes;
22. CPS systems (cyberphysical systems) / Robotic Autonomous Systems (RAS);
23. Sensitive Information;
24. IT infrastructure (applications, network, processes and data).

Additionally, four categories that are not typically considered assets were identified:

1. Environment;
2. Monetary benefits from users;
3. Measuring resilience;
4. Communication disruption.

These categories, although not traditionally classified as assets, involve aspects that are indirectly affected by cyber risks or are less directly related to conventional business assets vulnerable to cyber threats. These four items can be appropriately categorized based on their nature and typical considerations in the context of cyber risks:

- Environment: This can be relevant under *Regulatory and Legal Repercussions* (if environmental regulations are impacted by cyber incidents) or *Supply Chains* (if environmental factors influence supply chain resilience and continuity).
- Monetary benefits from users: This falls under Financial losses because any disruption or compromise of monetary transactions or benefits from users due to cyber incidents can lead to financial losses.
- Measuring resilience: This would typically be considered under *Measuring Resilience Itself*, as it directly pertains to evaluating and improving an organization's ability to withstand and recover from cyber threats.

- Communication disruption: This directly relates to *Interrupting business/production processes* because disruptions in communication systems can severely impact a business's ability to operate and fulfill its functions.

Furthermore, in the study, these four categories are marked with an asterisk (*).

Table 1: Categorized Assets from the Publications, Numbers of Mentions, and References (created by the authors)

Asset Categories Facing Cyber Threats	Number of Mentions	References
IT infrastructure (applications, network, processes and data)	21	(Ahn et al., 2024; Al-Hawamleh, 2024; Ali et al., 2023; Al-Kadhimi et al., 2023; Alqudhaibi et al., 2023; Alsabbagh & Langendorfer, 2023; Arenas et al., 2023; Aslan et al., 2023; Awouda et al., 2024; Bécue et al., 2020; Blum, 2020; Campean et al., 2021; Gürdür Broo et al., 2022; Hossain et al., 2024; Lee et al., 2020; Mustafa et al., 2023a; Ribeiro et al., 2021; Saeed et al., 2023; Sarker et al., 2024; Tabish & Chaur-Luh, 2024; Wai & Lee, 2023)
Sensitive Information	17	(Ahn et al., 2024; Al-Kadhimi et al., 2023; Alqudhaibi et al., 2023; Alsabbagh & Langendorfer, 2023; Arenas et al., 2023; Aslan et al., 2023; Bécue et al., 2020; Blum, 2020; Campean et al., 2021; Hossain et al., 2024; Lee et al., 2020; Petrenko & Elvira, 2019; Ribeiro et al., 2021; Saeed et al., 2023; Tabish & Chaur-Luh, 2024; Tariq et al., 2023; Youssef & Boudriga, 2022)
CPS systems (cyberphysical systems) / Robotic Autonomous Systems (RAS)	15	(Alsabbagh & Langendorfer, 2023; Aron & Sgarbossa, 2023; Awouda et al., 2024; Bécue et al., 2020; Blum, 2020; Campean et al., 2021; Gürdür Broo et al., 2022; Hossain et al., 2024; Lee et al., 2020; Mitchell et al., 2021; Moraitis et al., 2023; Park et al., 2023; Ribeiro et al., 2021; Tabish & Chaur-Luh, 2024; Tariq et al., 2023)
Interrupt business / production processes	13	(Ahn et al., 2024; AL-Hawamleh, 2024; Al-Kadhimi et al., 2023; Alqudhaibi et al., 2023; Aron & Sgarbossa, 2023; Bécue et al., 2020; Blum, 2020; Lee et al., 2020; Mustafa et al., 2023; Park et al., 2023; Ribeiro et al., 2021; Saeed et al., 2023; Tabish & Chaur-Luh, 2024)
Third-party risks	12	(AL-Hawamleh, 2024; Al-Kadhimi et al., 2023; Alqudhaibi et al., 2023; Alsabbagh & Langendorfer, 2023;

Asset Categories Facing Cyber Threats	Number of Mentions	References
		Arenas et al., 2023; Aslan et al., 2023; Bécue et al., 2020; Blum, 2020; Campean et al., 2021; Hossain et al., 2024; Mustafa et al., 2023a; Youssef & Boudriga, 2022)
Internet of Things (IoT), Industrial Internet of Things (IIoT)	12	(Ahn et al., 2024; Ali et al., 2023; Alqudhaibi et al., 2023; Alsabbagh & Langendorfer, 2023; Awouda et al., 2024; Blum, 2020; Hossain et al., 2024; Moraitis et al., 2023; Petrenko & Elvira, 2019; Ribeiro et al., 2021; Tariq et al., 2023; Wai & Lee, 2023)
Cyber-Physical Production System (CPPS)	11	(Ahn et al., 2024; Alqudhaibi et al., 2023; Alsabbagh & Langendorfer, 2023; Aron & Sgarbossa, 2023; Blum, 2020; Gürdür Broo et al., 2022; Lee et al., 2020; Moraitis et al., 2023; Park et al., 2023; Ribeiro et al., 2021; Wai & Lee, 2023)
AI/ML systems	11	(Ali et al., 2023; Bécue et al., 2020; Blum, 2020; Campean et al., 2021; Gürdür Broo et al., 2022; Lee et al., 2020; Mitchell et al., 2021; Mustafa et al., 2023a; Petrenko & Elvira, 2019; Sarker et al., 2024; Tabish & Chaur-Luh, 2024)
Financial losses	10	(AL-Hawamleh, 2024; Al-Kadhimi et al., 2023; Alqudhaibi et al., 2023; Arenas et al., 2023; Blum, 2020; Mustafa et al., 2023a; Ribeiro et al., 2021; Saeed et al., 2023; Wai & Lee, 2023; Youssef & Boudriga, 2022)
Regulatory and legal repercussions	9	(Al-Kadhimi et al., 2023; Alqudhaibi et al., 2023; Arenas et al., 2023; Blum, 2020; Campean et al., 2021; Hossain et al., 2024; Lee et al., 2020; Mitchell et al., 2021; Mustafa et al., 2023a)
Customer requirements and interests	8	(AL-Hawamleh, 2024; Al-Kadhimi et al., 2023; Alqudhaibi et al., 2023; Arenas et al., 2023; Blum, 2020; Campean et al., 2021; Saeed et al., 2023; Youssef & Boudriga, 2022)
Company reputation	7	(AL-Hawamleh, 2024; Al-Kadhimi et al., 2023; Alqudhaibi et al., 2023; Blum, 2020; Lee et al., 2020; Mustafa et al., 2023a; Saeed et al., 2023)
Digital Twin (DT), Cyber Range (CR)	6	(Awouda et al., 2024; Bécue et al., 2020; Gürdür Broo et al., 2022; Lee et al., 2020; Park et al., 2023; Sarker et al., 2024)
Company's staff	5	(Al-Kadhimi et al., 2023; Alqudhaibi et al., 2023; Arenas et

Asset Categories Facing Cyber Threats	Number of Mentions	References
		al., 2023; Hossain et al., 2024; Mitchell et al., 2021)
Communication disruption (*)	4	(Al-Kadhimi et al., 2023; Alsabbagh & Langendorfer, 2023; Hossain et al., 2024; Ribeiro et al., 2021)
Measuring resilience (*)	4	(AL-Hawamleh, 2024; Alqudhaibi et al., 2023; Blum, 2020; Campean et al., 2021)
Monetary benefits from users (*)	4	(Al-Kadhimi et al., 2023; Arenas et al., 2023; Blum, 2020; Saeed et al., 2023)
Environment (*)	4	(Alqudhaibi et al., 2023; Blum, 2020; Campean et al., 2021; Mitchell et al., 2021)
Supply chains	4	(AL-Hawamleh, 2024; Alqudhaibi et al., 2023; Aron & Sgarbossa, 2023; Blum, 2020)
SCADA systems (Supervisory control and data acquisition)	4	(Blum, 2020; Erdodi et al., 2022; Moraitis et al., 2023; Wai & Lee, 2023)
Cloud-based manufacturing execution systems (MES)	4	(Aron & Sgarbossa, 2023; Aslan et al., 2023; Park et al., 2023; Ribeiro et al., 2021)
Simulation-based disruption management systems	3	(Awouda et al., 2024; Bécue et al., 2020; Park et al., 2023)
Branding secure products	3	(Alqudhaibi et al., 2023; Blum, 2020; Saeed et al., 2023)
Intellectual property	3	(Al-Kadhimi et al., 2023; Blum, 2020; Saeed et al., 2023)
Blockchain	3	(Lee et al., 2020; Mustafa et al., 2023a; Petrenko & Elvira, 2019)
Distributed energy resources (DERs)	2	(Ahn et al., 2024; Erdodi et al., 2022)
Micro-payment infrastructure	1	(Youssef & Boudriga, 2022)
Smart contracts	1	(Mustafa et al., 2023a)

To improve clarity and utility, we consolidated smaller categories into broader ones, refining their names or codes where necessary. This approach grouped related items under common themes, making the data easier to analyze and interpret. By merging smaller categories, we minimized redundancy and overlap, ensuring that each broader category represented a cohesive set of elements. This process not only streamlined the presentation of findings but also provided a clearer framework for understanding the relationships between different assets within SMEs. Below are the refined, broader categories along with their respective elements.

Digital Infrastructure and Systems. This category encompasses all technological elements critical to the digital operations of SMEs, with a focus on the integration of both physical and cyber components in production and service delivery. It includes hardware, software, networks, and data systems that enable businesses to function effectively in the digital space.

- Smart contracts;
- Micro-payment infrastructure;
- Distributed energy resources (DERs);
- Blockchain;
- Cloud-based manufacturing execution systems (MES);
- SCADA systems (Supervisory control and data acquisition);
- Internet of Things (IoT), Industrial Internet of Things (IIoT);
- Cyber-Physical Production System (CPPS);
- CPS systems (cyberphysical systems) / Robotic Autonomous Systems (RAS);
- IT infrastructure (applications, network, processes, and data);
- AI/ML systems;
- Digital Twin (DT), Cyber Range (CR).

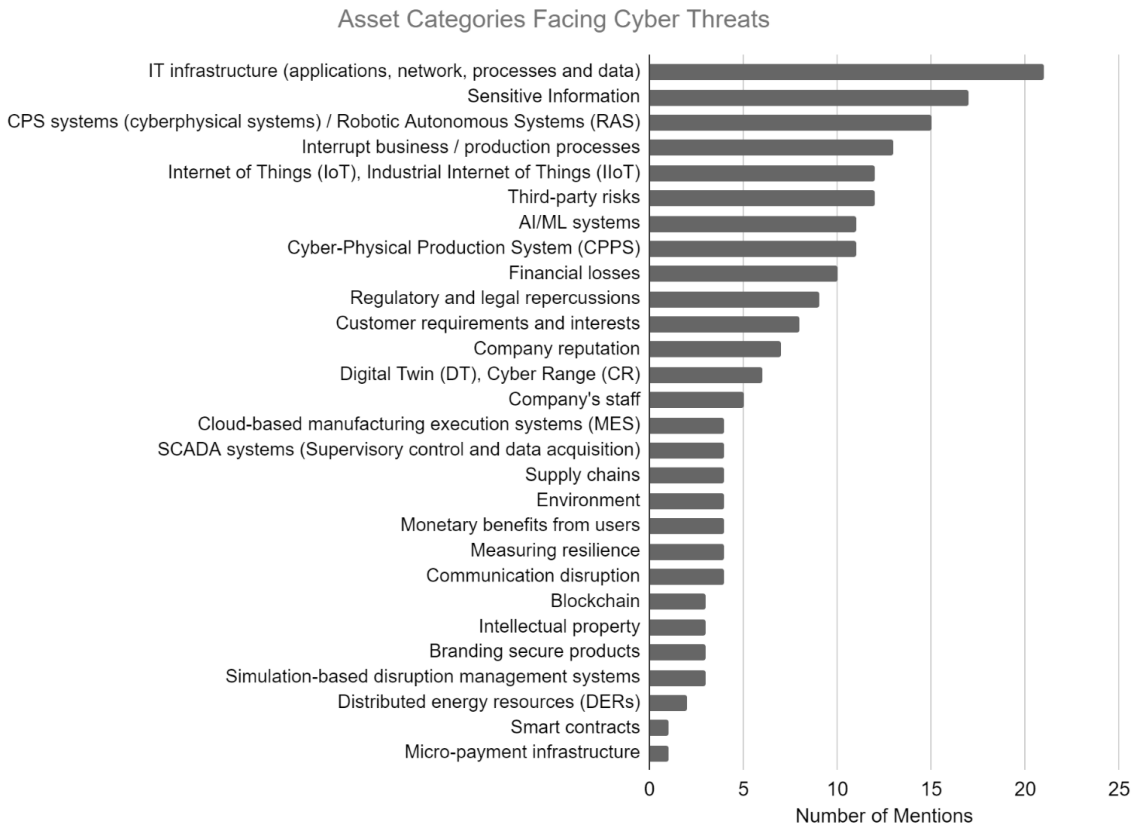

Figure 1: Defined SME Asset Categories sorted by the number of mentions in the publications (created by the authors)

Cybersecurity and Intellectual Property. This category combines the protection of intellectual property with sensitive information, emphasizing the critical need to safeguard digital assets and proprietary knowledge

from cyber threats. It underscores the importance of securing intellectual property rights, trade secrets, and confidential data, ensuring that SMEs' valuable innovations and creations remain protected from unauthorized access or theft.

- Intellectual property;
- Sensitive Information.

Business Operations and Continuity. This category focuses on maintaining operational integrity, encompassing supply chains and systems to manage disruptions, and ensuring seamless business processes.

- Supply chains;
- Simulation-based disruption management systems;
- Interrupt business/production processes;
- Communication disruption (*);
- Environment (*).

Reputation and Compliance. Combining reputation, regulatory issues, and product branding emphasizes the external perception and legal adherence essential for maintaining market trust and compliance.

- Company reputation;
- Regulatory and legal repercussions;
- Branding secure products;
- Environment (*).

Financial and Economic Impact. This category addresses the financial aspects of cyber risks, focusing on both potential losses and economic benefits, providing a comprehensive view of the economic implications of cyber threats.

- Financial losses;
- Monetary benefits from users (*).

Risk and Resilience Management. This category includes elements related to identifying, measuring, and managing risks, focusing on resilience against disruptions and third-party vulnerabilities.

- Measuring resilience (*);
- Third-party risks.

Human Resources and Customer Relations. This category combines internal staff and customer aspects, focusing on the human elements essential for business operations and customer satisfaction.

- Company's staff;
- Customer requirements and interests.

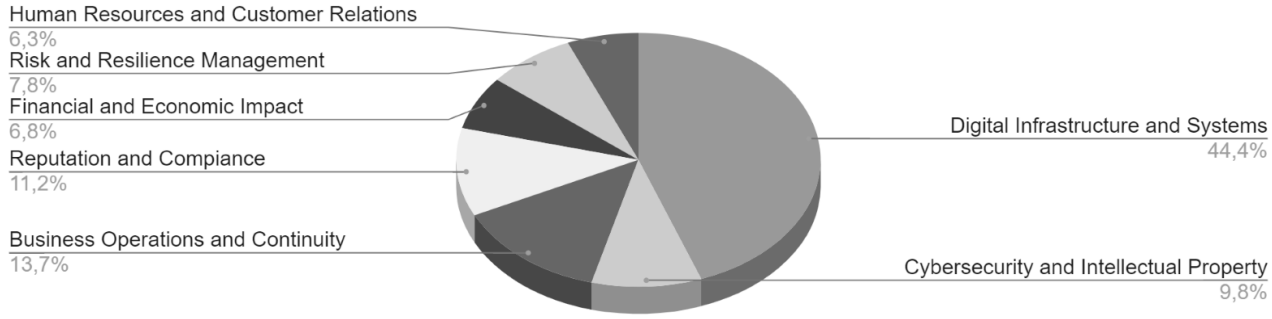

Figure 2: Merged Categories of SME Assets Facing Cyber Threats (created by the authors)

4. Discussion

This section delves into the concept of assets as identified in the existing literature. While some assets received limited focus in our content analysis, their importance should not be underestimated. Given the fast-paced evolution of technology, certain assets are still in the developmental phase, with relatively little research dedicated to them. This study serves as an initial investigation into this area, highlighting the need for further exploration and understanding as these assets continue to grow in relevance.

Throughout the research process, the list of references is likely to expand, which may lead to the emergence of new asset categories while reducing the relevance of those that are currently frequently cited. Additionally, categories may be merged, or new distinctions may arise within existing categories. As a result, the conclusions drawn in this study should be seen as dynamic and subject to revision as future research advances.

It is also important to acknowledge that the asset categories outlined below are not isolated; they are intricately interconnected and mutually influential within a broader system. In practice, many studies address multiple asset types concurrently within a single investigation. This interconnectedness highlights the complexity of effectively managing digital assets. Understanding these interdependencies is essential for developing comprehensive strategies that enhance cyber resilience and mitigate risks across all facets of SME operations.

Smart contracts (SCs), a key component of blockchain technology, automate digital workflows and reduce transaction costs for SMEs. However, they are susceptible to vulnerabilities such as arithmetic bugs and reentrancy, which require careful selection of secure programming languages. The integration of SCs with consensus algorithms in blockchain enhances both security and efficiency. This is particularly valuable in applications like smart grids, which manage Distributed Energy Resources (DERs), as they face significant cybersecurity challenges.

Blockchain's transformative impact goes beyond enhancing transactional efficiency, providing greater security and resilience across various sectors, including healthcare and wireless sensor networks (WSNs) (Faheem, Kuusniemi et al., 2024; Mustafa et al., 2023; Saari et al., 2023; Toub & Hajami, 2024). For SMEs, blockchain-enabled micro-payment infrastructure ensures secure and efficient small transactions, fostering operational stability and enabling micro-shopping (Youssef & Boudriga, 2022).

DERs play a pivotal role in enhancing energy resilience and cost-effectiveness for SMEs by integrating them into smart grids to manage energy variability. Blockchain technology enables decentralized power trading among microgrids, ensuring transparent and secure transactions that support sustainable energy distribution (Ahn et al., 2024; Alasali et al., 2024; Anjimoon et al., 2024; Faheem, Al-Khasawneh, et al.,

2024; Hseiki et al., 2024; Zubin J.B. et al., 2024). This integrated approach highlights blockchain's potential to revolutionize SME operations by enhancing reliability and transparency in energy management.

Blockchain technology strengthens SME cybersecurity and operational efficiency by offering a decentralized ledger for secure data storage and transactions. It promotes transparency, mitigates cyber threats, and supports sustainable growth in competitive markets (Aidynov et al., 2024; Almasabi et al., 2024; Anjimoon et al., 2024).

Cloud-based MES enhances SME manufacturing operations by providing real-time data and analytics, which improves production efficiency and decision-making. Integration with cyber-physical systems optimizes resource allocation and supply chain agility, thereby boosting operational resilience (Abdullayeva, 2023; Aron & Sgarbossa, 2023b; Moura & Hutchison, 2022; Saeed et al., 2023; Tharot et al., 2023).

SCADA systems are crucial for controlling industrial processes in SMEs, which are particularly vulnerable to cyber threats due to their connectivity. To support secure Industry 4.0 transformations, robust cybersecurity frameworks, including access controls and encryption, are essential for safeguarding SCADA environments (Wai & Lee, 2023; Radvanovsky et al., 2013; Alqudhaibi et al., 2023; Kolosok et al., 2022; Stanculescu et al., 2021; Birnbaum et al., 2020).

IIoT enhances SME operational efficiency and security by enabling real-time data exchange and automation in manufacturing processes. Advanced security measures safeguard industrial data from cyber threats, ensuring productivity and resilience in competitive environments (Radanliev et al., 2021; Sukiasyan et al., 2022; Ali et al., 2023; Alasmary, 2023; Adouglid et al., 2024).

CPS and RAS enhance SME manufacturing efficiency and automation in Industry 4.0, integrating IoT for real-time data management. Resilient frameworks mitigate cyber risks, ensuring secure and productive operations amid digital transformations (Espinoza-Zelaya et al., 2023; Cassottana et al., 2023; Adamos et al., 2024; Segovia-Ferreira et al., 2024; Gallab et al., 2024; Bagozi et al., 2021).

AI/ML technologies empower SMEs with intelligent cybersecurity frameworks, detecting and mitigating evolving cyber threats in real time. Neural networks and explainable AI (XAI) enhance security operations, ensuring SME resilience in digital environments (Dari et al., 2023; Schmitt, 2023; Sarker et al., 2024).

Digital Twin (DT) technology enhances SME efficiency by virtualizing physical systems but poses cybersecurity challenges. Robust security measures, such as encryption and threat detection, are crucial for protecting DTs and ensuring SMEs capitalize on digital transformation securely (Siddique et al., 2023; O'Connell et al., 2023; Allison et al., 2023; de Donato et al., 2023; Sarker et al., 2024).

Integrating smart contracts (SCs) with blockchain technology offers significant benefits for SMEs by streamlining digital workflows and reducing transaction costs, despite vulnerabilities like arithmetic bugs and reentrancy. This integration enhances security and efficiency in managing Distributed Energy Resources (DERs) within smart grids, effectively addressing cybersecurity challenges. Blockchain's broader application across sectors such as healthcare and wireless sensor networks (WSNs) highlights its role in improving SME cybersecurity, operational transparency, and sustainability. As SMEs adopt blockchain-enabled micro-payment infrastructures and leverage cloud-based Manufacturing Execution Systems (MES) and Industrial Internet of Things (IIoT), they strengthen operational resilience against cyber threats, ensuring secure and efficient digital operations. The integration of AI/ML technologies and the implementation of robust cybersecurity frameworks for SCADA systems, Digital Twins (DTs), and Cyber-Physical Systems (CPS) further reinforce SMEs' capacity to thrive amidst Industry 4.0 transformations, safeguarding against evolving cyber risks and fostering resilient growth in competitive markets.

The critical role of intellectual property (IP) as a valuable asset for SMEs, especially in the context of digital twins (DTs) and cybersecurity, is well-documented in studies. DTs improve operations and resilience by virtualizing physical systems, but they also introduce security risks by making IP more accessible and

synchronized with physical counterparts. The rapid evolution of cyber threats calls for advanced cybersecurity solutions, including explainable AI models that help understand system functions and effectively mitigate risks. Protecting intellectual property against cyber threats is paramount for SMEs utilizing digital technologies such as DTs and AI/ML. Enhanced monitoring and strategic cybersecurity measures are necessary to mitigate risks and ensure resilience in the face of evolving digital landscapes (Moore et al., 2011; Sarker et al., 2024).

In discussing the significance of sensitive information, safeguarding this valuable asset becomes crucial for SMEs, particularly in the face of growing cyber threats. The integration of advanced machine learning algorithms plays a key role in continuous monitoring and real-time prediction of emerging cyber-attacks. Conventional security measures often fall short against sophisticated tactics that exploit human vulnerabilities, underscoring the need for resilient cybersecurity solutions. Furthermore, fostering trust in cyber threat intelligence sharing and adopting intelligent technologies are vital strategies to mitigate risks and protect sensitive data critical to daily business operations (Mugan, 2013; Shabut et al., 2016; Wagner et al., 2018; Keenan, 2019).

A supply chain, which is vital for SMEs, encompasses an interconnected network of organizations, resources, activities, and technologies, spanning from raw material sourcing to final customer delivery, thus supporting efficient market competitiveness. The advent of the metaverse introduces transformative digital landscapes that are reshaping supply chain and operations management (SCOM). This shift requires adaptation to cyber-physical systems, digital supply chain twins, and Industry 4.0/5.0 concepts, which integrate physical and digital chains to enhance operational coordination and resilience. Future research will focus on improving visibility, computational capabilities for data analytics, and fostering digital collaboration across these hybrid environments to drive innovation in processes and performance metrics (Dolgui et al., 2023; Wallis et al., 2023; Marinagi et al., 2023; Aron & Sgarbossa, 2023; Alshurideh et al., 2023).

A simulation-based disruption management system for SMEs is designed to enhance resilience against disruptions such as natural disasters, economic crises, supply chain failures, and cyber-attacks. Specifically, in the food manufacturing sector, advanced simulation models predict and simulate the potential impacts of such disruptions. This enables proactive planning and collaborative decision-making among stakeholders, including dairy farmers and wholesalers, to strengthen supply chain resilience (Tsiamas et al., 2021).

Company reputation is crucial for SMEs, as it directly influences public trust and perceptions. Effective cyber-resilience measures not only protect sensitive information but also help mitigate negative consequences and enhance positive perceptions following cyber incidents, thereby safeguarding this essential asset. The alarming rate of data breaches, exemplified by the theft of 22 billion records in 2021 alone, highlights the severity of the issue. When a data breach occurs, businesses often face public scrutiny and blame, despite being victims themselves. This emphasizes the importance of proactive cyber defenses, not only in protecting sensitive information but also in preserving the trust and reputation that are vital assets for SMEs in today's digital landscape (Leroy et al., 2023; Toma et al., 2023).

Regulatory and legal repercussions are crucial for SMEs facing cyber threats, ensuring compliance with cybersecurity standards and mitigating risks such as cyberfraud. These frameworks safeguard organizational stability, reputation, and customer trust, guiding SMEs in implementing effective cybersecurity measures to minimize financial losses and reputational damage (Saeed et al., 2023; Akinbowale et al., 2024).

The limited attention given to assets such as branding secure products, measuring resilience, third-party risks, company staff, and customer requirements and interests in this study can be attributed to several factors. Firstly, technical digital assets like cybersecurity tools and digital infrastructure often dominate research priorities due to their direct impact on operational efficiency and security. These assets are

perceived as critical in mitigating immediate threats, such as cyber-attacks, which are becoming increasingly prevalent in today's digital landscape.

Secondly, the complexity and breadth of topics such as branding secure products, resilience measurement, and third-party risks require nuanced methodologies and comprehensive data collection, which may not have been fully addressed in this study. These areas often involve interdisciplinary approaches and qualitative research methods to capture diverse perspectives and contextual nuances.

However, in future studies, these assets are likely to receive more attention due to their strategic importance in enhancing SME competitiveness and sustainability. Branding secure products, for instance, directly impacts consumer trust and market positioning in an era where cybersecurity and product integrity are paramount. Measuring resilience and understanding third-party risks are critical for preemptively addressing vulnerabilities and ensuring robust supply chain management. Additionally, focusing on company staff and customer requirements aligns with the broader goal of enhancing organizational resilience and customer satisfaction, which are central to SME success in dynamic market environments.

Therefore, future research endeavors are expected to delve deeper into these areas, employing more tailored methodologies to uncover insights that can inform strategic decision-making and operational practices in SMEs. This will contribute to a more comprehensive understanding of how non-technical assets can strengthen SME resilience, competitiveness, and long-term sustainability.

5. Conclusion

In this study, we conducted a literature content analysis of cyber risks and threats faced by SMEs, focusing on the diverse categories of digital assets susceptible to vulnerabilities. Through content analysis of twenty-nine relevant publications, we identified and categorized twenty-four asset types that are critical to SME operations and at risk of cyber threats. These assets encompass a wide spectrum of technological innovations and operational components, ranging from digital infrastructure and systems to intellectual property and business operations. Our findings underscore the intricate interplay between these assets within SME environments, revealing their susceptibility to cyber risks such as disruptions, financial losses, and reputational damage.

While certain asset categories received extensive attention in our analysis, others, such as branding secure products, measuring resilience, third-party risks, company staff, and customer requirements and interests, were comparatively underexplored. This gap in research attention can be attributed to the complex nature of these assets and the evolving dynamics of cyber threats, which require nuanced approaches and interdisciplinary perspectives for a more comprehensive understanding.

Looking ahead, we anticipate a shift towards greater emphasis on these overlooked asset categories in future research endeavors. The strategic importance of branding secure products, for instance, in enhancing consumer trust and market positioning, highlights its relevance amidst increasing cybersecurity concerns. Similarly, the need to measure resilience and manage third-party risks reflects growing awareness of supply chain vulnerabilities and operational dependencies in SME ecosystems. The focus on company staff and customer requirements aligns with broader efforts to strengthen organizational resilience and stakeholder engagement, both crucial for maintaining competitiveness and adaptability in turbulent market conditions.

This study provides an initial framework for assessing and prioritizing cyber risks across various SME assets. As we continue to refine our knowledge and methodologies, the goal is to equip SMEs with robust defenses and strategic foresight, enabling them to navigate and thrive securely in the digital economy.

References

Abdullayeva, F. (2023). Cyber resilience and cyber security issues of intelligent cloud computing systems. *Results in Control and Optimization*, 12. https://doi.org/10.1016/j.rico.2023.100268

Adamos, K., Stergiopoulos, G., Karamousadakis, M., & Gritzalis, D. (2024). Enhancing attack resilience of cyber-physical systems through state dependency graph models. *International Journal of Information Security*, 23(1), 187–198. https://doi.org/10.1007/s10207-023-00731-w

Ahn, B., Kim, T., Ahmad, S., Mazumder, S. K., Johnson, J., Mantooth, H. A., & Farnell, C. (2024). An Overview of Cyber-Resilient Smart Inverters Based on Practical Attack Models. *IEEE Transactions on Power Electronics*, 39(4), 4657–4673. https://doi.org/10.1109/TPEL.2023.3342842

Aidynov, T., Goranin, N., Satybaldina, D., & Nurusheva, A. (2024). A systematic literature review of current trends in electronic voting system protection using modern cryptography. *Applied Sciences*, 14(7). https://doi.org/10.3390/app14072742

Akinbowale, O. E., Klingelhöfer, H. E., Zerihun, M. F., & Mashigo, P. (2024). Development of a policy and regulatory framework for mitigating cyberfraud in the South African banking industry. *Heliyon*, 10(1). https://doi.org/10.1016/j.heliyon.2023.e23491

Alasali, F., Hayajneh, A. M., Ghalyon, S. A., El-Naily, N., AlMajali, A., Itradat, A., Holderbaume, W., & Zaroure, E. (2024). Enhancing resilience of advanced power protection systems in smart grids against cyber–physical threats. *IET Renewable Power Generation*, 18(5), 837–862. https://doi.org/10.1049/rpg2.12957

Alasmary, H. (2023). RDAF-IIoT: Reliable device-access framework for the industrial Internet of things. *Mathematics*, 11(12). https://doi.org/10.3390/math11122710

Al-Hawamleh, A. (2024). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. *International Journal of Computing and Digital Systems*, 15(1), 1315–1331. https://doi.org/10.12785/ijcds/150193

Ali, H., Khan, M. S., Driss, M., Ahmad, J., Buchanan, W. J., & Pitropakis, N. (2023). CellSecure: Securing image data in industrial Internet-of-things via cellular automata and chaos-based encryption. *IEEE Vehicular Technology Conference*. https://doi.org/10.1109/VTC2023-Fall60731.2023.10333478

Ali, Y., Khan, H. U., & Khalid, M. (2023). Engineering the advances of the artificial neural networks (ANNs) for the security requirements of Internet of Things: a systematic review. *Journal of Big Data*, 10(1). https://doi.org/10.1186/s40537-023-00805-5

Al-Kadhimi, A. A., Singh, M. M., & Khalid, M. N. A. (2023). A Systematic literature review and a conceptual framework proposition for advanced persistent threats (APT) detection for mobile devices using Artificial Intelligence techniques. *Applied Sciences*, 13(14). https://doi.org/10.3390/app13148056

Allison, D., Smith, P., & McLaughlin, K. (2023). Digital twin-enhanced incident response for cyber-physical systems. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3600160.3600195

Almasabi, S., Shaf, A., Ali, T., Zafar, M., Irfan, M., & Alsuwian, T. (2024). Securing smart grid data with blockchain and wireless sensor networks: A collaborative approach. *IEEE Access*, 12, 19181–19198. https://doi.org/10.1109/ACCESS.2024.3361752

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). https://doi.org/10.3390/s23094539

Alqudhaibi, A., Deshpande, S., Jagtap, S., & Salonitis, K. (2023). Towards a sustainable future: developing a cybersecurity framework for manufacturing. *Technological Sustainability*, 2(4), 372–387. https://doi.org/10.1108/TECHS-05-2023-0022

Alsabbagh, W., & Langendorfer, P. (2023). Security of programmable logic controllers and related systems: Today and tomorrow. *IEEE Open Journal of the Industrial Electronics Society*, 4, 659–693. https://doi.org/10.1109/OJIES.2023.3335976

Alshurideh, M. T., Alquqa, E. K., Alzoubi, H. M., al Kurdi, B., & Alhamad, A. (2023). The impact of cyber resilience and robustness on supply chain performance: Evidence from the UAE chemical industry. *Uncertain Supply Chain Management*, 11(1), 187–194. https://doi.org/10.5267/j.uscm.2022.10.008

Anjimoon, S., Chandrashekar, R., Singh, N., Parmar, A., Sharma, N., & Mohammad, Q. (2024). Secure and sustainable energy distribution through blockchain technology in smart grids. *E3S Web of Conferences*, 505. https://doi.org/10.1051/e3sconf/202450502002

Arenas, L. A., Yactayo-Arias, C., Quispe, S. R., & Sandoval, J. L. (2023). Leveraging security modeling and information systems audits to mitigate network vulnerabilities. *International Journal of Safety and Security Engineering*, 13(4), 763–771. https://doi.org/10.18280/ijsse.130420

Aron, C., & Sgarbossa, F. (2023). The physical Internet as an approach for resilient logistics practices: Literature review and future research avenues. *IFAC-PapersOnLine*, 56(2), 11068–11075. https://doi.org/10.1016/j.ifacol.2023.10.811

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6). https://doi.org/10.3390/electronics12061333

Awouda, A., Traini, E., Bruno, G., & Chiabert, P. (2024). IoT-based framework for digital twins in the Industry 5.0 era. *Sensors*, 24(2). https://doi.org/10.3390/s24020594

Bagozi, A., Bianchini, D., & Antonellis, V. D. (2021). Context-based resilience in cyber-physical production system. *Data Science and Engineering*, 6(4), 434–454. https://doi.org/10.1007/s41019-021-00172-2

Bécue, A., Maia, E., Feeken, L., Borchers, P., & Praça, I. (2020). A new concept of digital twin supporting optimization and resilience of factories of the future. *Applied Sciences*, 10(13). https://doi.org/10.3390/app10134482

Birnbaum, Z., Davis, M., Salman, S., Schaffter, J., Watkins, L., Yamajala, S., & Paul, S. (2020). Cyber-resilient scada systems via secure state restoration. *In IFIP Advances in Information and Communication Technology* (Vol. 596). https://doi.org/10.1007/978-3-030-62840-6_9

Blum, D. (2020). Rational cybersecurity for business: The security leaders' guide to business alignment. In *Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment*, 1st edition. https://doi.org/10.1007/978-1-4842-5952-8

Campean, F., Kabir, S., Dao, C., Zhang, Q., & Eckert, C. (2021). Towards a resilience assurance model for robotic autonomous systems. *Proceedings of the Design Society*, 1, 3189–3198. https://doi.org/10.1017/pds.2021.580

Cassottana, B., Roomi, M. M., Mashima, D., & Sansavini, G. (2023). Resilience analysis of cyber-physical systems: A review of models and methods. *Risk Analysis*, 43(11), 2359–2379. https://doi.org/10.1111/risa.14089

Dari, S. S., Thool, K. U., Deshpande, Y. D., Aush, M. G., Patil, V. D., & Bendale, S. P. (2023). Neural networks and cyber resilience: Deep insights into AI architectures for robust security framework. *Journal of Electrical Systems*, 19(3), 78–95. https://doi.org/10.52783/jes.653

de Donato, L., Dirnfeld, R., Somma, A., de Benedictis, A., Flammini, F., Marrone, S., Saman Azari, M., & Vittorini, V. (2023). Towards AI-assisted digital twins for smart railways: preliminary guideline and reference architecture. *Journal of Reliable Intelligent Environments*, 9(3), 303–317. https://doi.org/10.1007/s40860-023-00208-6

Dolgui, A., & Ivanov, D. (2023). Metaverse supply chain and operations management. *International Journal of Production Research*, 61(23), 8179–8191. https://doi.org/10.1080/00207543.2023.2240900

Espinoza-Zelaya, C., & Moon, Y. B. (2023). Framework for enhancing the operational resilience of cyber-manufacturing systems against cyber-attacks. *Manufacturing Letters*, 35, 843–850. https://doi.org/10.1016/j.mfglet.2023.07.004

Faheem, M., Al-Khasawneh, M. A., Khan, A. A., & Madni, S. H. H. (2024). Cyberattack patterns in blockchain-based communication networks for distributed renewable energy systems: A study on big datasets. *Data in Brief*, 53. https://doi.org/10.1016/j.dib.2024.110212

Faheem, M., Kuusniemi, H., Eltahawy, B., Bhutta, M. S., & Raza, B. (2024). A lightweight smart contracts framework for blockchain-based secure communication in smart grid applications. *IET Generation, Transmission and Distribution*, 18(3), 625–638. https://doi.org/10.1049/gtd2.13103

Gallab, M., di Nardo, M., & Naciri, L. (2024). Navigating contemporary challenges and future prospects in digital industry evolution. *Discover Applied Sciences*, 6(5). https://doi.org/10.1007/s42452-024-05913-2

Gürdür Broo, D., Bravo-Haro, M., & Schooling, J. (2022). Design and implementation of a smart infrastructure digital twin. *Automation in Construction*, 136. https://doi.org/10.1016/j.autcon.2022.104171

Hossain, M., Kayas, G., Hasan, R., Skjellum, A., Noor, S., & Islam, S. M. R. (2024). A holistic analysis of Internet of Things (IoT) security: principles, practices, and new perspectives. *Future Internet*, 16(2). https://doi.org/10.3390/fi16020040

Hseiki, H. A., El-Hajj, A. M., Ajra, Y. O., Hija, F. A., & Haidar, A. M. (2024). A secure and resilient smart energy meter. *IEEE Access*, 12, 3114–3125. https://doi.org/10.1109/ACCESS.2023.3349091

Kolosok, I., & Gurina, L. (2022). Cyber resilience models of systems for monitoring and operational dispatch control of electric power systems. *IFAC-PapersOnLine*, 55(9), 485–490. https://doi.org/10.1016/j.ifacol.2022.07.084

Lee, J., Azamfar, M., Singh, J., & Siahpour, S. (2020). Integration of digital twin and deep learning in cyber-physical systems: Towards smart manufacturing. *IET Collaborative Intelligent Manufacturing*, 2(1), 34–36. https://doi.org/10.1049/iet-cim.2020.0009

Leroy, I., & Zolotaryova, I. (2023). Critical infrastructure defense: perspectives from the EU and USA cyber experts | Захист критичної інфраструктури: бачення кібер-експертів ЄС і США. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, 5, 165–170. https://doi.org/10.33271/nvngu/2023-5/165

Marinagi, C., Reklitis, P., Trivellas, P., & Sakas, D. (2023). The Impact of Industry 4.0 Technologies on Key Performance Indicators for a Resilient Supply Chain 4.0. *Sustainability*, 15(6). https://doi.org/10.3390/su15065185

Mitchell, D., Blanche, J., Zaki, O., Roe, J., Kong, L., Harper, S., Robu, V., Lim, T., & Flynn, D. (2021). Symbiotic system of systems design for safe and resilient autonomous robotics in offshore wind farms. *IEEE Access*, 9, 141421–141452. https://doi.org/10.1109/ACCESS.2021.3117727

Moore, A. P., Hanley, M., & Mundie, D. (2011). A pattern for increased monitoring for intellectual property theft by departing insiders. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/2578903.2579157

Moraitis, G., Sakki, G.-K., Karavokiros, G., Nikolopoulos, D., Tsoukalas, I., Kossieris, P., & Makropoulos, C. (2023). Exploring the cyber-physical threat landscape of water systems: A socio-technical modelling approach. *Water*, 15(9). https://doi.org/10.3390/w15091687

Moura, J., & Hutchison, D. (2022). Resilience enhancement at edge cloud systems. *IEEE Access*, 10, 45190–45206. https://doi.org/10.1109/ACCESS.2022.3165744

Mugan, J. (2013). A developmental approach to learning causal models for cyber security. *Proceedings of SPIE - The International Society for Optical Engineering*, 8751. https://doi.org/10.1117/12.2014418

Mustafa, I., McGibney, A., & Rea, S. (2023). Smart contract life-cycle management: an engineering framework for the generation of robust and verifiable smart contracts. *Frontiers in Blockchain*, 6. https://doi.org/10.3389/fbloc.2023.1276233

O'Connell, E., O'Brien, W., Bhattacharya, M., Moore, D., & Penica, M. (2023). Digital twins: Enabling interoperability in smart manufacturing networks. *Telecom*, 4(2), 265–278. https://doi.org/10.3390/telecom4020016

Park, K.-T., Park, Y. H., Park, M.-W., & Noh, S. D. (2023). Architectural framework of digital twin-based cyber-physical production system for resilient rechargeable battery production. *Journal of Computational Design and Engineering*, 10(2), 809–829. https://doi.org/10.1093/jcde/qwad024

Patrick Keenan, K. (2019). Creating spaces of public insecurity in times of terror: The implications of code/space for urban vulnerability analyses. *Environment and Planning C: Politics and Space*, 37(1), 81–101. https://doi.org/10.1177/2399654418776660

Petrenko, S., & Elvira, K. (2019). Method of improving the cyber resilience for Industry 4.0. digital platforms. In *Lecture Notes in Computer Science* (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 11771 LNCS. https://doi.org/10.1007/978-3-030-29852-4_24

Radanliev, P., de Roure, D., van Kleek, M., Santos, O., & Ani, U. (2021). Artificial intelligence in cyber physical systems. *AI and Society*, 36(3), 783–796. https://doi.org/10.1007/s00146-020-01049-0

Radvanovsky, R., & Brodsky, J. (2013). *Handbook of SCADA/Control Systems Security*. https://doi.org/10.1201/b13869

Ribeiro, D., Almeida, A., Azevedo, A., & Ferreira, F. (2021). Resilience in industry 4.0 digital infrastructures and platforms. *Advances in Transdisciplinary Engineering*, 15, 390–395. https://doi.org/10.3233/ATDE210067

Saari, H., Amin, M. M., Saleh Abbas, M., Ismail, A. F., Husna Haris Fadzilah, A., & Nordin, M. (2023). Transforming industrial operations with blockchain: The healthcare application health-chain. *3rd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2023*, 1175–1179. https://doi.org/10.1109/ICACITE57410.2023.10182959

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, 23(15). https://doi.org/10.3390/s23156666

Sarker, I. H., Janicke, H., Mohsin, A., Gill, A., & Maglaras, L. (2024). Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects. *ICT Express*. https://doi.org/10.1016/j.icte.2024.05.007

Sarker, P. S., Sadanandan, S. K., & Srivastava, A. K. (2023). Resiliency metrics for monitoring and analysis of cyber-power distribution system with IoTs. *IEEE Internet of Things Journal*, 10(9), 7469–7479. https://doi.org/10.1109/JIOT.2022.3183180

Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration*, 36. https://doi.org/10.1016/j.jii.2023.100520

Segovia-Ferreira, M., Rubio-Hernan, J., Cavalli, A., & Garcia-Alfaro, J. (2024). A survey on cyber-resilience approaches for cyber-physical systems. *ACM Computing Surveys*, 56(8). https://doi.org/10.1145/3652953

Shabut, A. M., Lwin, K. T., & Hossain, M. A. (2016). Cyber attacks, countermeasures, and protection schemes - A state of the art survey. *SKIMA 2016 - 2016 10th International Conference on Software, Knowledge, Information Management and Applications*, 37–44. https://doi.org/10.1109/SKIMA.2016.7916194

Siddique, S., Haque, M. A., Rifat, R. H., George, R., Shujaee, K., & Gupta, K. D. (2023). Cyber security issues in the industrial applications of digital twins. *2023 IEEE Symposium Series on Computational Intelligence*, SSCI, 873–878. https://doi.org/10.1109/SSCI52147.2023.10371850

Stănculescu, M., Deleanu, S., Andrei, P. C., & Andrei, H. (2021). A case study of an industrial power plant under cyberattack: Simulation and analysis. *Energies*, 14(9). https://doi.org/10.3390/en14092568

Sukiasyan, A., Badikyan, H., Pedrosa, T., & Leitao, P. (2022). Secure data exchange in industrial Internet of Things. *Neurocomputing*, 484, 183–195. https://doi.org/10.1016/j.neucom.2021.07.101

Tabish, N., & Chaur-Luh, T. (2024). Maritime autonomous surface ships: A Review of cybersecurity challenges, countermeasures, and future perspectives. *IEEE Access*, 12, 17114–17136. https://doi.org/10.1109/ACCESS.2024.3357082

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review. *Sensors*, 23(8). https://doi.org/10.3390/s23084117

Tharot, K., Duong, Q. B., Riel, A., & Thiriet, J.-M. (2023). A cybersecurity training concept for cyber-physical manufacturing systems. *Procedia CIRP*, 120, 1375–1380. https://doi.org/10.1016/j.procir.2023.09.179

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

Toub, A., & Hajami, A. (2024). Data Manipulation in Wireless Sensor Networks: Enhancing Security Through Blockchain Integration with Proposal Mitigation Strategy. *International Journal of Advanced Computer Science and Applications*, 15(2), 95–105. https://doi.org/10.14569/IJACSA.2024.0150212

Tsiamas, K., & Rahimifard, S. (2021). A simulation-based decision support system to improve the resilience of the food supply chain. *International Journal of Computer Integrated Manufacturing*, 34(9), 996–1010. https://doi.org/10.1080/0951192X.2021.1946859

Wagner, T. D., Palomar, E., Mahbub, K., & Abdallah, A. E. (2018). A novel trust taxonomy for shared cyber threat intelligence. *Security and Communication Networks*, 2018. https://doi.org/10.1155/2018/9634507

Wai, E., & Lee, C. K. M. (2023). Seamless Industry 4.0 integration: A multilayered cyber-security framework for resilient SCADA deployments in CPPS. *Applied Sciences*, 13(21). https://doi.org/10.3390/app132112008

Wallis, T., & Dorey, P. (2023). Implementing partnerships in energy supply chain cybersecurity resilience. *Energies*, 16(4). https://doi.org/10.3390/en16041868

Youssef, S. B. H., & Boudriga, N. (2022). A resilient micro-payment infrastructure: An approach based on blockchain technology. *Kuwait Journal of Science*, 49(1). https://doi.org/10.48129/KJS.V49I1.10578

Zubin J.B. Sunitha R., Gopakumar Pathirikkat (2024). A novel method for fully distributed sealed bid power trading in a network of islanded microgrids using consortium blockchains and a framework for its implementation. *International Journal of Electrical Power and Energy Systems*, 158. https://doi.org/10.1016/j.ijepes.2024.109963