OPEN ACCESS
International Journal of Management & Entrepreneurship Research
P-ISSN: 2664-3588, E-ISSN: 2664-3596
Volume 6, Issue 6, P.No.1954-1981, June 2024
DOI: 10.51594/ijmer.v6i6.1208
Fair East Publishers
Journal Homepage: www.fepbl.com/index.php/ijmer

Addressing Cybersecurity Challenges in Sustainable Supply Chain Management: A Review of Current Practices and Future Directions

Oluwabunmi Layode[1], Henry Nwapali Ndidi Naiho[2], Talabi Temitope Labake[3], Gbenga Sheriff Adeleke[4], Ezekiel Onyekachukwu Udeh[5], & Ebunoluwa Johnson[6]

[1]Independent Researcher, Maryland, USA
[2]Independent Researcher, New York, USA
[3]Independent Researcher, Sheffield, UK
[4]Independent Researcher, Lagos, Nigeria
[5]Independent Researcher, RI, USA
[6]Independent Researcher, Johannesburg, South Africa

Corresponding Author: Oluwabunmi Layode
Corresponding Author Email: bunmi2405@gmail.com

Article Received: 12-02-24 **Accepted**: 15-05-24 **Published:** 13-06-24

ABSTRACT

This study investigates the integration of cybersecurity practices within sustainable supply chain management, addressing the dual challenges of securing supply chains against cyber threats while advancing sustainability objectives. The research employs a systematic literature review methodology, sourcing data from peer-reviewed articles published between 2018 and 2023, across databases such as IEEE Xplore, ScienceDirect, and Wiley Online Library. The selection process involved a rigorous screening of titles, abstracts, and full texts based on predefined inclusion and exclusion criteria, focusing on works that explicitly discuss the intersection of cybersecurity and sustainability within supply chains. Key findings reveal that cybersecurity and sustainability, while traditionally viewed in isolation, are increasingly recognized as complementary facets of supply chain management. The study highlights the critical role of emerging technologies, such as blockchain, artificial intelligence, and the

Internet of Things, in enhancing supply chain resilience and sustainability. Furthermore, stakeholder engagement is identified as crucial in developing effective cybersecurity strategies that align with sustainability goals. The future landscape of cybersecure sustainable supply chains is characterized by both challenges and opportunities, necessitating continuous innovation and collaboration across industries and with governmental bodies. Strategic recommendations for industry leaders and policymakers emphasize the importance of fostering a culture that values cybersecurity and sustainability, investing in technology sharing, and developing comprehensive regulatory frameworks. In conclusion, this study underscores the necessity of integrating cybersecurity practices within sustainable supply chain management, offering insights into navigating the complexities of this integration to achieve resilient, transparent, and responsible supply networks.

Keywords: Cybersecurity, Supply Chains, Supply Chain Management, Sustainability.

INTRODUCTION

The Critical Intersection of Cybersecurity and Sustainable Supply Chain Management

The intersection of cybersecurity and sustainable supply chain management (SCM) represents a critical juncture for modern businesses, where the imperatives of environmental stewardship, social responsibility, and economic viability meet the challenges of securing information and operational technologies against cyber threats. This convergence is increasingly important as companies strive to balance the need for sustainability with the imperative to protect against cyber risks that can undermine the integrity, confidentiality, and availability of critical supply chain information and systems.

Melnyk et al. (2021) highlight the significance of cybersecurity within the supply chain, noting that recent breaches have underscored the economic, political, and social ramifications of cyber incidents. These breaches are not isolated events but are symptomatic of the broader vulnerabilities inherent in the interconnected digital ecosystems that define today's organizational landscapes. The complexity of supply chains, coupled with the evolving nature of cyber threats, creates a landscape where traditional approaches to cybersecurity are no longer sufficient. The authors argue for a structured understanding of supply chain cybersecurity, proposing a research framework aimed at guiding future investigations into this critical area (Melnyk et al., 2021).

Kumar and Mallipeddi (2022) delve into the impact of cybersecurity on operations and supply chain management, emphasizing the challenges posed by the integration of Industry 4.0 and 5.0 technologies. These technologies, while driving the smartification of organizations and facilitating automation and data-driven decision-making, also introduce new vulnerabilities to cyberattacks. The authors identify the need for production and operations management researchers to explore robust strategies that can mitigate the risks and repercussions of cyber incidents. Their work underscores the importance of cybersecurity in ensuring the resilience and sustainability of supply chains in the face of evolving cyber threats (Kumar & Mallipeddi, 2022).

Ozkan-Ozen et al. (2023) focus on the risks associated with data-driven technologies in sustainable supply chain management. They argue that the digitalization and data-centric approaches essential for achieving sustainability also expose supply chains to new kinds of risks, including those related to data privacy, trust, and information sharing. Through a hybrid

multi-criteria decision-making model, the study identifies the economic dimension of sustainable SCM as particularly vulnerable to these risks. The findings highlight the critical need for organizations to address cybersecurity risks as part of their sustainability strategies, emphasizing the interconnectedness of data security, privacy, and the technological infrastructure within sustainable supply chains (Ozkan-Ozen et al., 2023).

In synthesizing these perspectives, it becomes clear that the critical intersection of cybersecurity and sustainable supply chain management is defined by a complex interplay of technological, organizational, and environmental factors. The drive towards sustainability, characterized by the integration of environmental, social, and economic considerations, must be paralleled by a comprehensive approach to cybersecurity. This approach should not only address the technological vulnerabilities introduced by digitalization and data-driven technologies but also consider the broader organizational and systemic challenges that these vulnerabilities present. The future direction of research and practice in this area must therefore focus on developing integrated strategies that can enhance the resilience of sustainable supply chains against the backdrop of an increasingly complex and dynamic cyber threat landscape.

Defining the Scope: Cybersecurity Challenges within Sustainable Supply Chains

In the realm of sustainable supply chain management (SCM), the integration of cybersecurity measures has emerged as a paramount concern, necessitating a comprehensive understanding of the scope and nature of cybersecurity challenges. This understanding is crucial for devising effective strategies to mitigate risks and ensure the integrity, confidentiality, and availability of supply chain data and systems. The scope of cybersecurity challenges within sustainable supply chains encompasses a broad spectrum of issues, ranging from data breaches and financial losses to reputational damage and operational disruptions.

Berry (2023) underscores the vulnerability of supply chain management to cyber threats, emphasizing that the coordination of goods, services, and information from suppliers to customers presents multiple points of attack for cyber adversaries. The research identifies the critical nature of cybersecurity in protecting against data breaches, financial loss, and reputational damage, which can have cascading effects on the operational continuity of supply chains. The study advocates for the adoption of best practices in managing cybersecurity risks, highlighting the importance of a proactive and comprehensive approach to safeguarding supply chain ecosystems (Berry, 2023).

Kumar and Mallipeddi (2022) delve into the challenges posed by the advent of Industry 4.0 and 5.0 technologies, which, while facilitating the smartification of organizations and the automation of decision-making processes, also introduce new cybersecurity risks. The integration of cloud computing, big data, the Internet of Things (IoT), artificial intelligence, and nanotechnology into supply chain operations has accelerated the digital transformation of supply chains but has concurrently increased their susceptibility to cyberattacks (Adewusi et al., 2024; Reis et al., 2024; Ajala and Balogun, 2024). The authors call for future research to focus on developing robust strategies to reduce the frequency and impact of these attacks, thereby enhancing the resilience of supply chains against cybersecurity threats (Kumar & Mallipeddi, 2022).

Ozkan-Ozen et al. (2023) explore the risks associated with data-driven technologies in sustainable SCM, noting that the digitalization and reliance on data for decision-making have made supply chains more competitive but also more vulnerable. The study identifies data

privacy, trust, data availability, information sharing, and traceability as key areas of concern. It highlights the economic dimension of sustainable SCM as particularly susceptible to risks posed by data-driven technologies, including data security, data privacy, and the robustness of information technology systems and infrastructure. The findings suggest that addressing these risks is essential for achieving sustainability in all stages of the supply chain, underscoring the interconnectedness of cybersecurity and sustainable SCM (Ozkan-Ozen et al., 2023).

The synthesis of these perspectives reveals that defining the scope of cybersecurity challenges within sustainable supply chains involves understanding the multifaceted nature of these challenges, which are exacerbated by the integration of advanced technologies and the increasing complexity of supply chain networks. The criticality of cybersecurity in sustainable SCM cannot be overstated, as it directly impacts the ability of organizations to maintain operational efficiency, protect stakeholder interests, and achieve sustainability goals. Future research and practice in this area must therefore prioritize the development of integrated cybersecurity strategies that address the unique vulnerabilities of sustainable supply chains, ensuring their resilience against an evolving cyber threat landscape.

Historical Overview: The Evolution of Cybersecurity in Supply Chain Management

The evolution of cybersecurity in supply chain management (SCM) is a narrative that mirrors the broader technological and organizational advancements of the past few decades. This historical overview seeks to chart the trajectory of these developments, highlighting key milestones and shifts in the landscape of supply chain cybersecurity.

The genesis of SCM can be traced back to a time when supply chains were relatively linear and localized. However, as Frazzon et al. (2019) elucidate, the advent of globalization and the digital revolution transformed SCM into a complex, interconnected web of entities, known as Supply Chain Management 4.0 (SCM 4.0). This new paradigm leverages technologies such as Big Data, cloud computing, and the Internet of Things (IoT) to enhance efficiency, transparency, and adaptability within supply chains. The transition to SCM 4.0 marked a significant shift in how supply chains were managed, moving from traditional methods to more integrated and technology-driven approaches (Frazzon et al., 2019).

D'Aleo (2016) provides a comprehensive review of the SCM evolution, emphasizing the role of competition and the development of competencies as driving forces behind the SCM advancements. The paper discusses how the modern definition of SCM has evolved, incorporating the concept of 'hidden capabilities' which are essential for exploiting competitive advantages in the supply chain. This evolution reflects a broader understanding of SCM, not just as a logistical challenge but as a strategic component of organizational success (D'Aleo, 2016).

The integration of cybersecurity into SCM has become increasingly critical with the digitalization of supply chains. Wen et al. (2023) explore the global research trends in supply chain management, particularly in construction projects, and highlight the growing importance of cybersecurity. The study indicates that the rapid growth in publications related to SCM after 2015 coincides with a heightened focus on sustainability, prefabricated housing, reverse logistics, lean management, and, importantly, cybersecurity. This surge in interest underscores the recognition of cybersecurity as a pivotal element of modern SCM, necessitating robust strategies to protect against cyber threats and ensure the integrity of supply chain operations (Wen et al., 2023).

The historical evolution of cybersecurity in SCM reflects a broader trend towards increased complexity, digitalization, and globalization of supply chains. As supply chains have become more integrated and reliant on digital technologies, the scope and scale of cybersecurity challenges have expanded. The transition to SCM 4.0 has not only brought about efficiencies and innovations but also introduced new vulnerabilities and risks that must be managed. The development of 'hidden capabilities' and the strategic integration of cybersecurity measures are indicative of the evolving landscape of SCM, where managing cyber risks is as critical as managing physical goods and services.

In summary, the historical overview of cybersecurity in SCM reveals a dynamic field that has evolved in response to technological advancements and changing business environments. The integration of cybersecurity into SCM practices is a testament to the recognition of the critical role that information security plays in protecting and enhancing the value of supply chains. As SCM continues to evolve, the focus on cybersecurity is expected to intensify, with ongoing research and innovation aimed at addressing the complex challenges that lie at the intersection of digitalization and supply chain management.

Aims and Objectives of the Review

The primary aim of this study is to bridge the gap between cybersecurity practices and sustainable supply chain management, providing a comprehensive review of current practices and projecting future directions. This study seeks to enhance the understanding of how cybersecurity measures can be integrated within sustainable supply chains to protect against cyber threats while promoting environmental sustainability and social responsibility.

The objectives are;

1. To Review Current Cybersecurity Practices in Sustainable Supply Chains
2. To Identify and Analyze Cybersecurity Challenges
3. To Evaluate the Integration of Cybersecurity and Sustainability

Research Gap

While the importance of cybersecurity in safeguarding supply chain operations has been increasingly recognized, its integration with sustainable supply chain management practices remains underexplored. The existing literature predominantly focuses on either cybersecurity measures to protect supply chains from cyber threats (Kumar & Mallipeddi, 2022) or on strategies to enhance supply chain sustainability (Cheung, Bell, & Bhattacharjya, 2021). However, there is a notable lack of comprehensive research that simultaneously addresses the synergies and conflicts between implementing cybersecurity measures and achieving sustainability objectives within supply chains. Furthermore, the rapid advancement of digital technologies such as the Internet of Things (IoT), blockchain, and artificial intelligence (AI) presents new opportunities and challenges for cybersecure and sustainable supply chain management (Tseng et al., 2020). Yet, the literature seldom provides in-depth analysis on how these technologies can be leveraged to enhance both cybersecurity and sustainability in supply chains, or on the potential trade-offs that may arise between these two objectives. Additionally, the stakeholder perspective on the integration of cybersecurity and sustainability within supply chains is largely missing. While stakeholders play a crucial role in the adoption and success of cybersecurity and sustainability practices (Appiah et al., 2022), there is limited understanding of their perceptions, motivations, and challenges in contributing to cybersecure and sustainable supply chains.

METHODOLOGY

This study employs a systematic literature review methodology to comprehensively understand the integration of cybersecurity within sustainable supply chain management, identify current practices, challenges, and propose future directions.

Data Sources

The literature review sources data from a variety of academic databases and digital libraries, including IEEE Xplore, ScienceDirect, SpringerLink, Wiley Online Library, and Google Scholar. These platforms are chosen for their extensive repositories of peer-reviewed articles, conference proceedings, and book chapters relevant to cybersecurity, supply chain management, and sustainability.

Search Strategy

The search strategy involves the use of specific keywords and phrases related to the study's aim and objectives. Keywords such as "cybersecurity in supply chains," "sustainable supply chain management," "digital security in logistics," and "sustainability and cyber threats" are used in various combinations to ensure a comprehensive search. Boolean operators (AND, OR) are employed to refine the search results, focusing on the intersection of cybersecurity and sustainability within supply chains.

Inclusion and Exclusion Criteria for Relevant Literature

Peer-reviewed articles published between 2018 and 2023 to ensure the relevance and timeliness of the data. Studies that specifically address cybersecurity challenges within the context of sustainable supply chain management. Articles that provide insights into the integration of digital technologies for enhancing supply chain security and sustainability. Non-peer-reviewed sources, such as blogs and non-academic websites. Articles focusing solely on cybersecurity or sustainability without addressing their intersection within supply chains. Studies published before 2018, to maintain the focus on recent advancements and trends.

Selection Process

The selection process involves screening titles and abstracts based on the inclusion and exclusion criteria, followed by a full-text review of shortlisted articles to ensure their relevance to the study's objectives. This two-stage screening process is conducted independently by two reviewers, with discrepancies resolved through discussion or consultation with a third reviewer. The final selection of sources is based on their contribution to understanding the integration of cybersecurity practices within sustainable supply chain management.

Data Analysis

Data analysis employs a thematic synthesis approach to categorize findings into themes related to the study's objectives. This includes identifying common cybersecurity challenges, current practices, technological advancements, and gaps in the literature. The synthesis also explores the implications of these findings for stakeholders in sustainable supply chain management. Quantitative data, such as the frequency of specific themes or the prevalence of certain cybersecurity measures, are analyzed to support the qualitative findings. The analysis aims to provide a comprehensive overview of the current state of research and propose actionable insights for future directions in cybersecure sustainable supply chain management.

LITERATURE REVIEW

Core Concepts: Cybersecurity and Sustainability in Supply Chains

The integration of cybersecurity and sustainability within supply chain management (SCM) has emerged as a pivotal concern for organizations worldwide. This integration is driven by the recognition that cybersecurity is not just a technical issue but a strategic one that underpins the sustainability of supply chains. The core concepts of cybersecurity and sustainability in SCM encompass a broad spectrum of practices, strategies, and technologies designed to protect supply chain data and systems from cyber threats while ensuring the supply chain's operations are environmentally responsible, socially equitable, and economically viable.

Sawik (2022) addresses the critical need for balancing cybersecurity investments across the supply chain to mitigate both direct and indirect cyber risks. The study presents a stochastic programming formulation aimed at optimizing cybersecurity investments and the selection of security controls. This approach underscores the complexity of managing cybersecurity in a multi-tier supply chain, where the goal is to achieve a balanced cybersecurity posture that protects against potential breaches and minimizes supply chain nodes' loss. Sawik's research highlights the importance of a strategic approach to cybersecurity investment, one that considers the interconnected nature of supply chain nodes and the cascading effects of cyber risks (Sawik, 2022).

In the wake of the COVID-19 pandemic, Jabbour et al. (2020) explore the sustainability of supply chains, emphasizing the lessons and trends that have emerged. The pandemic has accentuated the need for supply chains to be both resilient and sustainable, with a heightened focus on building smarter supply chains that can withstand various shocks. The article provides guidelines for supply chain managers on prioritizing resilience and sustainability, highlighting the role of cybersecurity in ensuring the continuity and integrity of supply chain operations. The research suggests that the pandemic has served as a catalyst for reevaluating and strengthening the sustainability and cybersecurity measures within supply chains, pointing towards a future where these aspects are increasingly integrated (Jabbour et al., 2020).

Hryhorak, Trushkina, and Kitrish (2022) delve into the strategic management of supply chain sustainability, offering a comprehensive framework for assessing and enhancing the sustainability of supply chains from an organizational and economic perspective. Their work emphasizes the need for a strategic approach to managing supply chain sustainability, incorporating cybersecurity as a key component of this strategy. The proposed framework includes a set of indicators for sustainable development and strategic guidelines for achieving sustainability under various scenarios. This approach highlights the interconnectedness of cybersecurity and sustainability, suggesting that effective management of one cannot be achieved without considering the other (Hryhorak, Trushkina, & Kitrish, 2022).

The synthesis of these perspectives underscores the critical intersection of cybersecurity and sustainability in SCM. The core concepts of this integration revolve around the recognition that cybersecurity is fundamental to the sustainability of supply chains. As such, strategic investments in cybersecurity, coupled with a commitment to sustainable practices, are essential for building resilient, secure, and sustainable supply chains. The future of SCM lies in the ability of organizations to navigate the complexities of cybersecurity risks while

adhering to principles of sustainability, thereby ensuring the long-term viability and resilience of their supply chains.

The Architecture of Cybersecure Sustainable Supply Chains

The architecture of cybersecure sustainable supply chains is a complex framework that integrates cybersecurity measures with sustainability principles to protect and enhance supply chain operations. This integration is crucial in today's digital age, where supply chains are increasingly reliant on information and communication technologies (ICT) and the Internet of Things (IoT). The design of such an architecture requires a coordinated approach to address the multifaceted challenges of cybersecurity while ensuring the supply chain's sustainability.

Masip-Bruin et al. (2021) present a pioneering architecture designed to orchestrate existing and beyond state-of-the-art security appliances in composed ICT scenarios, including large and complex IoT systems. The proposed architecture, named FISHY, aims to guarantee trusted supply chains of ICT systems built upon distributed, dynamic, potentially insecure, and heterogeneous ICT infrastructures. FISHY addresses security and privacy functionalities related to risks and vulnerabilities management, accountability, mitigation strategies, security metrics, and evidence-based security assurance. This architecture leverages the capabilities of programmable networks and IT infrastructure through seamless orchestration and instantiation of novel security services, both in real-time and proactively. The business analysis included in the study goes beyond technical benefits, highlighting the potential of FISHY adoption in real-world use cases to enhance cybersecurity across the supply chain (Masip-Bruin et al., 2021).

Radmanesh, Haji, and Valilai (2023) introduce a blockchain-based architecture for enhancing sustainability in supply chains through cloud architecture. This innovative approach leverages blockchain technology's advantages, such as smart contracts and distributed decision-making processes, to implement Industry 4.0 more efficiently. The architecture aims to increase productivity in supply chains by enhancing transparency, reducing operational costs, and improving monitoring and supervision throughout the product lifecycle. The study investigates the impact of the proposed blockchain-based platform on supply chain sustainability, revealing significant improvements in decentralized states compared to centralized states. These improvements directly enhance economic and environmental sustainability, showcasing the potential of blockchain technology in creating more sustainable and secure supply chains (Radmanesh, Haji, & Valilai, 2023).

Sayogo et al. (2015) discuss the development of an interoperable data architecture to integrate data regarding sustainability practices from disparate sources in sustainable supply chains. The study identifies the main issues and requirements for such development, emphasizing the challenges of collecting accurate and credible data, limited technological capabilities, complex data ownership, and disclosure policies. The proposed architecture aims to improve market transparency by enabling the integration of sustainability data, addressing challenges such as data quality, integrity, security, and the design of information policies that balance commercial interests and openness. This approach underscores the importance of developing appropriate governance mechanisms to ensure the fair and proper use of the system, thereby supporting the integration of sustainable supply chains (Sayogo et al., 2015).

In summary, the architecture of cybersecure sustainable supply chains encompasses a multifaceted framework that integrates advanced technologies such as blockchain and IoT

with cybersecurity measures and sustainability principles. This integrated approach is essential for protecting supply chain operations from cyber threats while ensuring their sustainability. The frameworks and architectures proposed by Masip-Bruin et al. (2021), Radmanesh, Haji, and Valilai (2023), and Sayogo et al. (2015) offer valuable insights and solutions for designing and implementing cybersecure sustainable supply chains in various industries.

Modalities of Cyber Threats in Supply Chain Management

The modalities of cyber threats in supply chain management (SCM) encompass a wide array of vulnerabilities and attack vectors that can compromise the integrity, confidentiality, and availability of supply chain data and operations. Understanding these modalities is crucial for developing effective cybersecurity strategies to protect supply chains from potential disruptions and breaches.

Prathyusha et al. (2023) emphasize the complexity of the Cyber Supply Chain (CSC) system, characterized by its multifaceted structure comprising several subsystems, each with distinct responsibilities. The inherent vulnerabilities and threats across the CSC pose significant challenges to securing the supply chain, as any component within the system is susceptible to cyber-attacks. The study advocates for a risk-based approach to threat assessment and mitigation, leveraging Cyber Threat Intelligence (CTI) and Machine Learning (ML) techniques to predict and counteract potential cyber threats. By analyzing CTI attributes and employing various ML algorithms, the research aims to identify inherent CSC vulnerabilities and implement appropriate controls to enhance supply chain security (Prathyusha et al., 2023).

Abd Latif et al. (2021) provide a systematic review of cybersecurity in SCM, highlighting the high risk of cyber terrorism, malware, and data theft. The review underscores common cybersecurity activities within supply chains, such as purchasing exclusively from trusted vendors and isolating critical machines from external networks. The study's findings, based on a decade of research articles, reveal a growing trend in cybersecurity research within SCM, particularly in the wake of increased digitalization and interconnectivity of supply chain operations. The analysis identifies key areas of focus, including network security, information security, web application security, and the Internet of Things (IoT), as critical elements in safeguarding supply chains against cyber threats (Abd Latif et al., 2021).

Lamba et al. (2017) investigate the use of information systems in SCM for companies with multicomponent production, aiming to identify effective strategies for information support of supply chain processes. The research highlights the importance of addressing sources of uncertainties, risks, and cybersecurity to integrate business processes between suppliers and customers effectively. The study proposes a new approach to identifying and predicting supply risk within uncertain conditions and suggests a comprehensive solution for securing data in information systems for SCM. This approach underscores the need for a holistic strategy to manage cyber security threats and ensure the resilience of supply chain operations (Lamba et al., 2017.).

In summary, the modalities of cyber threats in SCM are diverse and evolving, necessitating a proactive and informed approach to cybersecurity. The integration of CTI and ML techniques, along with a systematic review of cybersecurity practices and the development of new strategies for risk identification and data security, are essential for protecting supply chains

from cyber threats. As SCM becomes increasingly digital and interconnected, the importance of understanding and mitigating cyber threats to ensure the continuity and integrity of supply chain operations cannot be overstated.

Key Technological Milestones in Securing Supply Chains

The landscape of supply chain management (SCM) has been significantly reshaped by technological advancements, particularly in the realm of cybersecurity. The integration of these technologies has not only enhanced the efficiency and effectiveness of supply chains but also introduced new challenges and milestones in securing them against cyber threats.

Cheung, Bell, and Bhattacharjya (2021) provide a comprehensive overview of cybersecurity measures in logistics and SCM, highlighting the increased attack surface due to the adoption of internet-based technologies. The paper underscores the critical role of cybersecurity in maintaining the performance and reliability of logistics and overall supply chain operations. It identifies several research directions, including the scarcity of studies using real cybersecurity data and the limited focus on logistics despite its crucial role in supply chains. The review also points out the nascent stage of blockchain technologies in transport and logistics and the challenges posed by quantum computing to current encryption schemes. These insights underscore the evolving nature of cybersecurity challenges and the need for innovative solutions to protect supply chains (Cheung, Bell, & Bhattacharjya, 2021).

Hasan and Habib (2022) discuss the transformative impact of technological advancements on SCM, emphasizing the role of new technologies in making supply chains more efficient, productive, and cost-effective. The authors highlight several technologies that have been instrumental in this transformation, including blockchain, the Internet of Things (IoT), artificial intelligence (AI), and big data analytics. These technologies have not only streamlined supply chain operations but also introduced new avenues for securing supply chains against cyber threats. For instance, blockchain technology offers enhanced transparency and security through decentralized ledgers (Ajayi-Nifise et al., 2024), while AI and big data analytics provide sophisticated tools for threat detection and response (Hasan & Habib, 2022).

Kumar and Mallipeddi (2022) explore the impact of cybersecurity on operations and SCM in the context of Industry 4.0 and Industry 5.0. The paper identifies cybersecurity risks as a significant challenge arising from the integration of advanced technologies into supply chain operations. The authors suggest that future research should focus on developing robust strategies to mitigate these risks, thereby enhancing the resilience of supply chains. The study highlights the importance of cybersecurity in the era of smart supply chains, where the integration and automation of decision-making processes necessitate strong protective measures against cyber threats (Kumar & Mallipeddi, 2022).

In conclusion, the key technological milestones in securing supply chains have been driven by the adoption of advanced technologies such as blockchain, IoT, AI, and big data analytics. These technologies have revolutionized SCM, offering new opportunities for efficiency and innovation while also posing challenges for cybersecurity. The ongoing evolution of cybersecurity measures in response to these challenges underscores the need for continuous research and development to safeguard the integrity, confidentiality, and availability of supply chain operations in the digital age.

Review of State-of-the-Art Cybersecurity Practices in Supply Chains

In the realm of sustainable supply chain management, the integration of cybersecurity practices has emerged as a pivotal area of focus. The convergence of cybersecurity and sustainability within supply chains is not merely a trend but a necessity, given the increasing reliance on digital technologies and the internet for supply chain operations.

Boyens et al. (2021) provide a comprehensive overview of cybersecurity supply chain risk management practices for systems and organizations, emphasizing the critical need for robust cybersecurity measures in safeguarding supply chain integrity. Their work underscores the multifaceted nature of cybersecurity threats and the necessity for a holistic approach to risk management that encompasses both technological and organizational dimensions (Okoye et al., 2024). The integration of cybersecurity practices within supply chains is not merely about implementing technological solutions but also about fostering a culture of security awareness and resilience across all supply chain actors (Boyens et al., 2021).

Kottala (2021) expands on the concept of sustainable supply chain management practices by highlighting the importance of considering cybersecurity as an integral component of sustainability. The author argues that cybersecurity practices contribute to the economic, environmental, and social dimensions of sustainability by ensuring the protection of data and resources, thereby minimizing the risk of disruptions and enhancing the overall resilience of the supply chain. Kottala's (2021) analysis suggests that a sustainable supply chain cannot be achieved without addressing the cybersecurity challenges inherent in today's digital and interconnected world.

Furthermore, Duque-Uribe et al. (2019) present an integrative framework for sustainable supply chain management practices, with a specific focus on the healthcare sector. Their systematic review identifies cybersecurity as a critical area for ensuring sustainable performance in hospitals, where the protection of sensitive patient data and the reliability of medical supply chains are paramount. The authors highlight the need for strategic management and leadership in embedding cybersecurity practices within the operational and strategic frameworks of supply chain management, thereby ensuring both sustainability and security (Duque-Uribe et al., 2019).

The synthesis of information from these sources reveals several key insights into the state-of-the-art cybersecurity practices in supply chains. Firstly, there is a consensus on the necessity of integrating cybersecurity measures as a foundational element of sustainable supply chain management. This integration is vital not only for protecting against cyber threats but also for ensuring the continuity and reliability of supply chain operations in a sustainable manner. Secondly, the literature points to the importance of a holistic approach that encompasses both technological solutions and organizational strategies, including the development of a security-aware culture and the implementation of comprehensive risk management frameworks.

Therefore, the review of state-of-the-art cybersecurity practices in supply chains underscores the critical intersection of cybersecurity and sustainability. As supply chains continue to evolve in the digital age, the integration of robust cybersecurity measures will remain a cornerstone of sustainable supply chain management. The insights from Boyens et al. (2021), Kottala (2021), and Duque-Uribe et al. (2019) provide a valuable foundation for future research and practice, highlighting the need for continuous innovation and collaboration

among supply chain stakeholders to address the complex cybersecurity challenges of the 21st century.

Emerging Trends and Innovations

The landscape of sustainable supply chain management is rapidly evolving, with cybersecurity emerging as a critical pillar in this transformation. The integration of digital intelligence and innovative technologies has become indispensable in enhancing the resilience and sustainability of supply chains against cyber threats.

Wang et al. (2023) delve into the challenges and innovations in implementing sustainable supply chain smart manufacturing, particularly in the metal recycling industry. Their research underscores the pivotal role of digital intelligence empowerment in modernizing supply chains, thereby enhancing their sustainability and resilience against cyber threats. The study reveals that the adoption of smart manufacturing practices, powered by digital technologies, not only mitigates cybersecurity risks but also promotes environmental sustainability through efficient resource utilization (Wang et al., 2023).

Singh and Maheswaran (2023) examine the social barriers to sustainable innovation and digitization in supply chains, identifying key challenges in the adoption of digital technologies. Their analysis highlights the importance of addressing work-related circumstances and employment disruptions to facilitate the seamless integration of cybersecurity and digital innovations within supply chains. The study suggests that overcoming these social barriers is crucial for harnessing the full potential of digital technologies in achieving sustainable supply chain management (Singh & Maheswaran, 2023).

Dai (2022) explores the relationship between supply chain relationship quality and corporate technological innovations, providing valuable insights into how collaborative partnerships within supply chains can foster technological advancements, including cybersecurity innovations. The study emphasizes the dual mediating role of knowledge sharing and integration in enhancing technological innovations, thereby contributing to the sustainability and security of supply chains. Dai's research highlights the significance of mutual commitment among supply chain members in driving high-tech innovations, including those aimed at securing supply chains against cyber threats (Dai, 2022).

The synthesis of these studies sheds light on several key trends and innovations in cybersecure sustainable supply chains. Firstly, the integration of digital intelligence and smart manufacturing practices emerges as a crucial strategy for enhancing the cybersecurity and sustainability of supply chains. This approach not only addresses the immediate cybersecurity challenges but also contributes to the long-term sustainability goals by optimizing resource use and reducing environmental impact. Secondly, the research underscores the importance of overcoming social barriers to innovation and digitization, suggesting that addressing employment disruptions and fostering skill development are essential for the successful integration of cybersecurity measures within supply chains. Lastly, the role of supply chain relationship quality in facilitating technological innovations highlights the importance of collaborative partnerships and knowledge exchange in advancing cybersecurity solutions.

In summary, the emerging trends and innovations in cybersecure supply chains represent a convergence of digital intelligence, sustainability, and cybersecurity. The insights from Wang et al. (2023), Singh and Maheswaran (2023), and Dai (2022) underscore the multifaceted

approach required to enhance the resilience and sustainability of supply chains in the face of evolving cyber threats. As supply chains continue to navigate the digital landscape, the integration of innovative cybersecurity measures will remain a critical factor in achieving sustainable supply chain management.

Advances in Cybersecurity Protocols for Supply Chains

The advent of Industry 4.0 and Industry 5.0 has ushered in a new era of digital transformation, significantly impacting operations and supply chain management. This transformation is characterized by the integration of advanced technologies such as the Internet of Things (IoT), artificial intelligence (AI), and big data analytics, which collectively enhance the efficiency and responsiveness of supply chains. However, this digitalization also introduces complex cybersecurity challenges that necessitate the development and implementation of advanced cybersecurity protocols to safeguard supply chain integrity.

Kumar and Mallipeddi (2022) emphasize the critical impact of cybersecurity on operations and supply chain management, noting that the digitalization of supply chains has exposed organizations to heightened cybersecurity risks. The authors argue that the proliferation of cyberattacks necessitates a strategic approach to cybersecurity, encompassing not only technological solutions but also organizational and operational adjustments. They advocate for future research in production and operations management (POM) to focus on developing robust strategies that can mitigate the impacts of cyberattacks on supply chains. This includes exploring the role of global operations strategy, healthcare operations management, public policy, management of technology, supply chain management, and disruptive technologies in enhancing cybersecurity (Kumar & Mallipeddi, 2022).

Berry (2023) highlights the importance of cybersecurity in supply chain management, identifying the coordination of goods, services, and information from suppliers to customers as a critical vulnerability point for cyber threats. The research underscores the need for comprehensive cybersecurity practices that address the unique challenges of supply chain management, including data breaches, financial loss, reputational damage, and operational disruptions. Berry (2023) proposes a set of best practices for managing cybersecurity risks in supply chains, emphasizing the significance of continuous risk assessment, the implementation of secure communication protocols, and the importance of fostering a culture of cybersecurity awareness among all supply chain stakeholders (Berry, 2023).

Cinar (2023) delves into the specific risks, challenges, and strategies associated with supply chain cybersecurity in a globalized world. The paper outlines the complexities of monitoring supply chain risks and the costly nature of managing these risks effectively. Cinar (2023) presents a comprehensive approach to supply chain risk management, advocating for the adoption of five key actions towards achieving worry-free supply chain risk management. These actions include the implementation of advanced cybersecurity protocols, regular cybersecurity training for employees, the establishment of strong partnerships with suppliers and customers to ensure cybersecurity compliance (Oguejiofor et al., 2023), and the utilization of cybersecurity insurance as a risk management tool (Cinar, 2023).

The synthesis of these studies reveals a consensus on the necessity of advancing cybersecurity protocols within supply chains to address the evolving landscape of cyber threats. The integration of digital technologies in supply chains, while beneficial for operational efficiency and responsiveness, introduces significant cybersecurity challenges that must be addressed

through innovative strategies and protocols. The insights from Kumar and Mallipeddi (2022), Berry (2023), and Cinar (2023) underscore the importance of a holistic approach to cybersecurity, which encompasses technological, organizational, and operational dimensions. This approach is crucial for safeguarding supply chains against cyber threats and ensuring their resilience and sustainability in the digital age.

In summary, the advancements in cybersecurity protocols for supply chains represent a critical area of focus in the context of digital transformation. The research highlighted in this section provides valuable insights into the strategies and innovations that are being deployed to enhance the cybersecurity of supply chains. As the digitalization of supply chains continues to evolve, the development and implementation of robust cybersecurity protocols will remain paramount in mitigating cyber risks and ensuring the integrity and sustainability of supply chains.

Integration and Miniaturization in Cybersecure Supply Chain Solutions

The integration and miniaturization of technologies within cybersecure supply chain solutions represent a pivotal advancement in the realm of supply chain management. This evolution is not only enhancing the efficiency and agility of supply chains but also significantly bolstering their cybersecurity posture. By leveraging compact, integrated technologies, supply chains can achieve greater resilience against cyber threats, while also optimizing their operations for sustainability and efficiency.

Berroir et al. (2023) explore the integration of digital technologies in construction supply chains, emphasizing the role of Building Information Modelling (BIM) and digital twins in facilitating lean and green logistics. The study highlights how digitalization, through the creation of semantic digital twins and the use of Product Information Management systems, can significantly enhance the integration of product data across the supply chain. This integration not only streamlines material flows and reduces costs but also mitigates environmental impacts, showcasing the dual benefits of digital integration in achieving both operational efficiency and sustainability (Berroir et al., 2023).

Damtew, Borena, and Yilma (2021) investigate the impact of cloud-based supply chain integration on firm performance and competitiveness, particularly in the context of developing regions. Their study reveals that cloud computing plays a crucial role in optimizing supply chain integration processes, offering infrastructure, platform, and software solutions that enhance resource utilization, information flow, and system flexibility. The adoption of cloud-based services leads to significant improvements in performance and competitiveness, demonstrating the value of integrating cloud technologies in supply chains for enhanced cybersecurity and operational efficiency (Damtew, Borena, & Yilma, 2021).

Fulconis and Philipp (2019) address the challenges of e-commerce delivery within supply chains, focusing on the integration and flexibility of packaging solutions. Their research underscores the importance of packaging that fulfills both logistic and marketing functions, particularly in satisfying the demands of online consumers. The study suggests that the integration of innovative packaging solutions, which are both flexible and efficient, can significantly enhance the e-commerce supply chain's resilience against operational and cybersecurity challenges. This integration not only improves the delivery process but also contributes to the overall security and sustainability of the supply chain (Fulconis & Philipp, 2019).

The synthesis of these studies reveals a clear trend towards the integration and miniaturization of technologies in supply chains, highlighting the significant benefits of such advancements in enhancing cybersecurity, operational efficiency, and sustainability. The integration of digital twins, cloud computing, and innovative packaging solutions exemplifies the potential of compact and integrated technologies in transforming supply chains. These innovations not only address the immediate challenges of cybersecurity and efficiency but also contribute to the long-term sustainability and resilience of supply chains.

In summary, the advancements in the integration and miniaturization of cybersecure supply chain solutions represent a crucial development in the field of supply chain management. The insights from Berroir et al. (2023), Damtew, Borena, and Yilma (2021), and Fulconis and Philipp (2019) provide a valuable perspective on the impact of these innovations, underscoring the importance of adopting integrated and compact technologies for the future of secure, efficient, and sustainable supply chains.

DETAILED DISCUSSION AND ANALYSIS

Impact Analysis of Cybersecurity Measures in Supply Chains

The integration of cybersecurity measures within supply chains has become a paramount concern for organizations worldwide. As supply chains become increasingly digital and interconnected, the potential impact of cybersecurity threats on operational efficiency, financial stability, and brand reputation has escalated. Deane, Baker, and Rees (2023) provide a quantitative analysis of cybersecurity risks in supply chains, identifying four primary attack vectors and the key risk factors associated with each. Their study, based on forensic analyses of approximately 2000 companies that experienced cyberattacks, underscores the critical need for robust cybersecurity measures to mitigate these risks. The research highlights the importance of information sharing and information technology (IT) implementation in reducing supply chain risk, yet points out the lack of accepted principles or best practices for quantifying such risks. This gap underscores the necessity for developing standardized risk assessment methodologies that can guide organizations in implementing effective cybersecurity measures (Deane, Baker, & Rees, 2023).

Paulsen et al. (2020) describe the development and use of the Cyber Supply Chain Risk Management (C-SCRM) Interdependency Tool, designed to help federal agencies assess the potential impact of cybersecurity events in their supply chains. This tool represents a significant advancement in the field, offering a practical solution for organizations seeking to understand and mitigate the interdependent risks associated with cyber supply chain threats. The C-SCRM tool's ability to model complex operational environments and supply chain interdependencies provides a valuable resource for organizations aiming to enhance their cybersecurity posture. However, the research also indicates a need for broader adoption and customization of such tools across different sectors to fully address the diverse challenges posed by cyber supply chain risks (Paulsen et al., 2020).

Santos et al. (2021) focus on the implementation of information security assessment and certification within supply chains, proposing a metrics framework suitable for evaluating cybersecurity measures. Their work emphasizes the importance of continuous safety assessment and the adoption of standards such as the IEC 62443 for industrial cybersecurity. The proposed framework aims to facilitate trust between supply chain nodes and streamline the certification process, highlighting the dual benefits of enhancing cybersecurity and

operational efficiency. Despite these advancements, the research points to the ongoing challenge of achieving widespread adoption and integration of such frameworks across all supply chain participants (Santos et al., 2021).

The synthesis of these studies reveals several key insights into the impact of cybersecurity measures in supply chains. Firstly, the technological impact is evident in the enhanced ability of organizations to identify, assess, and mitigate cybersecurity risks through advanced tools and frameworks. Economically, effective cybersecurity measures can significantly reduce the potential for financial loss and reputational damage associated with cyberattacks. Environmentally, the adoption of green IT practices within cybersecurity efforts can contribute to sustainability goals. However, gaps remain in the form of a lack of standardized risk assessment methodologies, the need for broader tool adoption, and challenges in achieving comprehensive integration of security frameworks.

The impact analysis of cybersecurity measures in supply chains highlights the critical importance of these measures in safeguarding organizational assets and maintaining operational continuity. The insights from Deane, Baker, and Rees (2023), Paulsen et al. (2020), and Santos et al. (2021) underscore the need for ongoing research and development in this area, aiming to close existing gaps and enhance the resilience of supply chains against cyber threats.

Technological, Economic, and Environmental Impacts

The integration of cybersecurity measures within supply chains has become increasingly crucial in today's digital age, not only to safeguard sensitive information but also to ensure the seamless operation of supply chain activities. This integration, however, brings with it a myriad of technological, economic, and environmental impacts that necessitate a comprehensive analysis.

Huang (2022) explores the concept of green supply chain management and its implications for economic-environmental performance, particularly in the context of Asian countries. The study underscores the importance of integrating environmental considerations into supply chain management to mitigate the adverse effects of economic production activities on the environment. By adopting green supply chain practices, organizations can not only enhance their economic growth but also contribute to environmental sustainability. This research highlights the critical role of cybersecurity measures in protecting the digital infrastructure that supports green supply chain initiatives, thereby ensuring their effectiveness and longevity (Huang, 2022).

Zhao, Luo, and Liu (2022) examine the impact of technological innovation on environmental firm performance, with a focus on the mediating role of financial development in China. Their findings suggest that supply chain management, particularly when it incorporates green practices and technologies, significantly influences a firm's environmental performance. Technological innovation, including cybersecurity measures, plays a pivotal role in enabling green supply chain management by ensuring the secure exchange of information and facilitating the adoption of green technologies. This study illustrates the economic benefits of integrating cybersecurity measures into supply chains, which not only enhance a firm's performance but also support social welfare through improved environmental outcomes (Zhao, Luo, & Liu, 2022).

Munir et al. (2022) discuss the potential of blockchain technology in achieving sustainable supply chain management from economic, environmental, and social perspectives. The adoption of blockchain can revolutionize supply chains by enhancing transparency, traceability, and efficiency, thereby contributing to economic sustainability. Furthermore, blockchain technology, underpinned by robust cybersecurity protocols, can facilitate environmental and social sustainability by ensuring the responsible use of resources and promoting accountability across the supply chain. This research underscores the technological impact of cybersecurity measures in enabling the adoption of blockchain and other digital technologies for sustainable supply chain management (Munir et al., 2022).

The synthesis of these studies reveals that the integration of cybersecurity measures into supply chains has significant technological, economic, and environmental impacts. Technologically, cybersecurity measures enable the adoption of innovative digital solutions, such as blockchain, that enhance supply chain transparency and efficiency. Economically, these measures support the growth and competitiveness of firms by safeguarding critical supply chain information and facilitating green practices that appeal to environmentally conscious consumers. Environmentally, cybersecurity measures are integral to the implementation of green supply chain management practices, contributing to the reduction of ecological footprints and the promotion of sustainable development.

From the foregoing, the technological, economic, and environmental impacts of cybersecurity measures in supply chains are profound and multifaceted. The insights from Huang (2022), Zhao, Luo, and Liu (2022), and Munir et al. (2022) highlight the necessity of integrating robust cybersecurity protocols within supply chains to support sustainable practices and ensure the resilience of supply chain operations against cyber threats. As digital technologies continue to evolve, the role of cybersecurity in enabling sustainable supply chain management will undoubtedly become even more critical.

Identifying Gaps in Current Cybersecurity Practices and Proposing Solutions

In the contemporary digital landscape, cybersecurity within supply chains has emerged as a pivotal concern, underscored by the increasing sophistication of cyber threats and the interconnected nature of global supply networks.

Melnyk et al. (2022) highlight the criticality of cybersecurity as a supply chain issue, driven by the digital interconnectedness that defines organizational ecosystems. Their research underscores the lack of clarity and existing gaps in the knowledge base regarding cybersecurity across supply chains, attributed to the relative novelty and complexity of both domains. Through an exploratory research methodology that includes literature reviews, interviews with subject matter experts, and external validation, the authors develop a research framework aimed at guiding future investigations into supply chain cybersecurity. This framework serves as a foundational step towards structuring a common understanding of cybersecurity challenges and research opportunities within supply chains, emphasizing the need for a unified approach to address these gaps (Melnyk et al., 2022).

Vollmer (2021) addresses the cybersecurity gaps within the North Atlantic Treaty Organization's (NATO) Space Asset Supply Chain (SASC), highlighting the critical nature of data obtained from space assets for NATO missions and national security. The study identifies vulnerabilities such as legacy systems and the use of Commercial-Off-the-Shelf (COTS) technology as primary cybersecurity gaps. Vollmer suggests that NATO's largely unregulated

cyber SASC exacerbates these vulnerabilities, proposing two major collaboration initiatives: raising awareness throughout the NATO system and advancing the creation of a standardized security framework for SASC cybersecurity. These initiatives aim to enhance transparency, responsibility, and liability, thereby safeguarding mission-critical information (Vollmer, 2021).

Schleper et al. (2021) explore the pandemic-induced knowledge gaps in operations and supply chain management, particularly in the retail industry. The COVID-19 pandemic has amplified the importance of cybersecurity within supply chains, as the shift towards online retailing and remote work has exposed new vulnerabilities. The authors propose a practice-infused research agenda to address these gaps, emphasizing the need for relevant research on business responses to external shocks. This agenda calls for a deeper understanding of how cybersecurity measures can be effectively integrated into supply chain practices to mitigate the impacts of the pandemic and other crises (Schleper et al., 2021).

The synthesis of these studies reveals several key gaps in current cybersecurity practices within supply chains, including a lack of standardized frameworks, vulnerabilities associated with legacy systems and COTS technology, and the need for greater awareness and collaboration among stakeholders. To address these gaps, the research suggests the development of comprehensive cybersecurity frameworks, the modernization of supply chain infrastructure, and the fostering of collaborative initiatives to enhance cybersecurity awareness and practices.

In conclusion, identifying and addressing the gaps in current cybersecurity practices within supply chains is imperative for safeguarding against cyber threats and ensuring the resilience of global supply networks. The insights from Melnyk et al. (2022), Vollmer (2021), and Schleper et al. (2021) underscore the necessity of a unified and proactive approach to cybersecurity, emphasizing the importance of collaboration, standardization, and continuous research to navigate the evolving cyber landscape.

Evolutionary Trends in Cybersecurity Measures and Their Effectiveness

The evolution of cybersecurity measures within supply chains has become a focal point for organizations striving to mitigate the risks associated with the digital transformation of their operations. This evolution is characterized by the adoption of advanced technologies and methodologies aimed at enhancing the effectiveness of cybersecurity defenses.

Dai et al. (2023) delve into the complexities of digital supply chains driven by cybersecurity, employing an evolutionary game model to analyze the development patterns and long-term trends. Their findings suggest that irrational decisions can render the evolutionary path of digital supply chains complex and unpredictable. This study underscores the importance of strategic decision-making in cybersecurity practices within supply chains, highlighting the need for organizations to adopt a more calculated approach to digitalization and cybersecurity. The research provides valuable guidance for enterprises navigating the digital transformation process, emphasizing the critical role of cybersecurity in ensuring the stability and efficiency of digital supply chains (Dai et al., 2023).

Zhao and Wang (2024) examine the impact of digital strategies on supply chain decision-making through an evolutionary game model, focusing on the role of government measures in influencing these decisions. Their analysis reveals that government incentives and penalties play a significant role in shaping the digital decision-making process within supply chains.

The study illustrates how stronger government interventions can prompt abrupt changes in the evolutionary game system, encouraging suppliers and manufacturers to adopt digital strategies. This research highlights the evolving nature of cybersecurity measures in supply chains, where government policies and regulations significantly influence the adoption of digital and cybersecurity practices (Zhao & Wang, 2024).

Wright (2023) addresses the paramount importance of cybersecurity in healthcare supply chain management, emphasizing the risks posed by cybercrime to patient safety, data security, and operational efficiency. The study explores the role of cybersecurity as the primary defense against online threats, focusing on the protection of patient data and medical equipment. Wright's research underscores the evolving challenges in healthcare cybersecurity, advocating for vigilant detection and mitigation efforts to safeguard against cyber threats. The study highlights the critical need for robust cybersecurity measures in healthcare supply chains, reflecting the broader trend of increasing cybersecurity risks across various industries (Wright, 2023).

The synthesis of these studies reveals a clear trend towards the increasing complexity and sophistication of cybersecurity measures in supply chains. The evolution of these measures is driven by the need to address the dynamic nature of cyber threats and the growing digitalization of supply chain operations. The research underscores the importance of strategic decision-making, government intervention, and industry-specific considerations in enhancing the effectiveness of cybersecurity practices.

In summary, the evolutionary trends in cybersecurity measures within supply chains underscore the necessity of adopting advanced technologies and methodologies to mitigate cyber risks effectively. The insights from Dai et al. (2023), Zhao and Wang (2024), and Wright (2023) highlight the multifaceted approach required to navigate the challenges posed by the digital transformation of supply chains. As cyber threats continue to evolve, so too must the cybersecurity measures employed by organizations to protect their supply chains and ensure their operational resilience.

Projecting Future Directions in Cybersecurity Supply Chain Management

The landscape of supply chain management is rapidly evolving, with cybersecurity emerging as a critical component in safeguarding operations and ensuring continuity. This evolution is driven by the advent of Industry 4.0 and 5.0 technologies, which, while offering unprecedented opportunities for efficiency and integration, also introduce new vulnerabilities and challenges.

Kumar and Mallipeddi (2022) discuss the impact of cybersecurity on operations and supply chain management, emphasizing the challenges posed by recent technological advancements. The authors identify several key areas for future research, including global operations strategy, healthcare operations management, public policy, management of technology, and disruptive technologies. Their work underscores the necessity for production and operations management researchers to develop robust strategies for mitigating cyber threats. This includes exploring the integration of cybersecurity measures within the broader context of supply chain management and operations, ensuring that these measures are adaptable to the rapid pace of technological change (Kumar & Mallipeddi, 2022).

Cheung, Bell, and Bhattacharjya (2021) provide an overview of cybersecurity in logistics and supply chain management, highlighting the need for further research in this area. The paper

points out several gaps in current research, such as the scarcity of studies using real cybersecurity data and the limited focus on logistics despite its critical role in supply chains. The authors call for more quantitative research approaches to study cybersecurity in logistics and supply chain management and emphasize the potential of blockchain technologies. They also note the challenges posed by quantum computing techniques to current encryption schemes, suggesting that future research should explore more secure encryption methods and the integration of information security and digital forensic investigation within supply chain management (Cheung et al., 2021).

Khan et al. (2021) conduct a meta-analysis on sustainable supply chain management (SSCM), investigating present and emerging trends while exploring future research directions. Their study highlights the dominance of multiple-criteria decision-making methods in SSCM research and the need for studies at the macro level, such as country and region-level analyses. The authors suggest that future research should focus on employing efficient algorithms, advanced economic modeling, and exploring new linkages in the field of SSCM. This includes the integration of cybersecurity measures to ensure the sustainability of supply chains in the face of evolving cyber threats (Khan et al., 2021).

The synthesis of these studies reveals a consensus on the need for a multifaceted approach to cybersecurity in supply chain management. Future directions include the development of comprehensive frameworks that incorporate cybersecurity measures within the broader objectives of efficiency, sustainability, and resilience. The research underscores the importance of adapting to technological advancements, exploring new methodologies, and fostering collaboration between academia, industry, and government to address the complex challenges of cybersecurity in supply chains.

In conclusion, projecting future directions in cybersecure supply chain management involves a holistic understanding of the interplay between technology, policy, and operations. The insights from Kumar and Mallipeddi (2022), Cheung et al. (2021), and Khan et al. (2021) highlight the critical need for innovative research and strategic planning to navigate the challenges and opportunities presented by the digital transformation of supply chains. As cyber threats continue to evolve, so too must the strategies employed to protect and enhance the resilience of global supply networks.

The Role of Standards and Regulatory Frameworks

In the contemporary digital landscape, the role of standards and regulatory frameworks in enhancing cybersecurity within supply chains has become increasingly pivotal. As organizations navigate the complexities of securing their supply chains against cyber threats, the adoption of comprehensive standards and regulatory frameworks emerges as a critical strategy. This section explores the significance of these frameworks in cybersecure supply chain management, drawing insights from recent research.

Rogers (2020) discusses the growing importance of cybersecurity in supply chain management, emphasizing procurement's role in securing the network. The study highlights the shift in focus towards cybersecurity due to the rising number of malicious actors targeting supply chains' "weak cyber links." Rogers outlines the necessity for supply managers to adapt their sourcing strategies to mitigate these threats, including the adoption of basic cybersecurity standards and cross-functional teamwork. This approach underscores the significance of standards in enhancing supply chain cybersecurity, suggesting that a strategic

alignment between procurement practices and cybersecurity standards can stymie cyberattacks effectively (Rogers, 2020).

Anjum et al. (2023) delve into the vulnerabilities of software supply chains, examining the tactics and techniques employed by cybercriminals and the impact of stakeholders' traits and actions on attack success. The research identifies regulatory tools and protocols governing software supply chains as crucial elements in reducing organizations' susceptibility to cyber threats. By highlighting the importance of regulatory frameworks in mitigating software supply chain vulnerabilities, Anjum et al. (2023) provide valuable insights into the role of governance in enhancing cybersecurity. Their findings suggest that a comprehensive understanding of regulatory frameworks, coupled with proactive stakeholder engagement, is essential for safeguarding software supply chains against cyberattacks (Anjum et al., 2023).

Wallis and Dorey (2023) describe the implementation of a community within the energy sector focused on operational technology environments and their supply chains' cybersecurity. The study explores the challenges and progress of operators and suppliers in delivering cybersecurity, emphasizing the influence of regulatory frameworks on individual organizations. The research advocates for collaborative approaches and systems engineering methodologies to create a reference model for improving supply chain cybersecurity management. Wallis and Dorey's work illustrates the transformative potential of partnerships and regulatory frameworks in fostering cybersecurity resilience across the energy sector's supply chain, highlighting the importance of collective efforts in achieving security and resilience outcomes (Wallis & Dorey, 2023).

The synthesis of these studies reveals the critical role of standards and regulatory frameworks in bolstering cybersecurity within supply chains. From procurement's strategic alignment with cybersecurity standards to the governance of software supply chains and the collaborative efforts in the energy sector, the research underscores the multifaceted approach required to enhance supply chain cybersecurity. The insights from Rogers (2020), Anjum et al. (2023), and Wallis and Dorey (2023) highlight the necessity of adopting comprehensive standards and regulatory frameworks, emphasizing the importance of stakeholder collaboration and strategic planning in navigating the challenges of cybersecurity in supply chains.

In conclusion, the role of standards and regulatory frameworks in cybersecure supply chain management is indispensable. As organizations continue to grapple with the evolving landscape of cyber threats, the integration of robust standards and regulatory frameworks will remain paramount in safeguarding supply chains and ensuring their resilience.

Implications for Stakeholders in Sustainable Supply Chain Management

The integration of sustainability into supply chain management has become a critical concern for stakeholders across various industries. This integration not only addresses environmental, social, and economic performance but also aligns with the growing demand for responsible and sustainable business practices.

Tseng et al. (2022) examine the role of stakeholders in the sustainable supply and process management within the healthcare industry in Vietnam. Their study employs the fuzzy Delphi method and exploratory factor analysis to validate and confirm the criteria and aspects of SSCM from a stakeholder perspective. The findings indicate that sustainable supply management and process management are pivotal, with supplier assessment, environmental management systems, and green certification among the top criteria. This research

underscores the significance of stakeholder involvement in enhancing the sustainability of supply chains, particularly in the healthcare sector, where investment recovery and supplier collaboration play crucial roles (Tseng et al., 2022).

Vijayan and Kamarulzaman (2020) provide an introduction to SSCM and its business implications, emphasizing the concept of sustainability as a vital element for global acceptance and competitive differentiation. The chapter discusses the basic elements of sustainability in supply chain management and the global models adopted for its implementation. It highlights the strategic advantage of reverse logistics as a sustainability supply chain process and the role of the United Nations Global Compact program in promoting sustainability across businesses. This analysis illustrates the broad implications of SSCM for stakeholders, including the potential for strategic advantage and the importance of adopting global sustainability models (Vijayan & Kamarulzaman, 2020).

Appiah et al. (2022) focus on the petroleum industry in Ghana, investigating the relationship between SSCM practices and sustainable performance (SP), with a particular emphasis on the role of stakeholders' pressure. Their study reveals that environmental, economic, and social dimensions of SSCM are positively related to SP, and stakeholders' pressure significantly strengthens this relationship. The research highlights the emergent model of SP with enhanced predictability, suggesting that policymakers and advocates can achieve greater sustainability by maximizing stakeholders' pressure. This study provides a clear example of how stakeholder engagement and pressure can drive the adoption of SSCM practices and improve sustainable performance in the petroleum industry (Appiah et al., 2022).

The synthesis of these studies reveals the multifaceted implications of SSCM for stakeholders. From enhancing sustainability in the healthcare industry and leveraging strategic advantages through reverse logistics to the pivotal role of stakeholders' pressure in the petroleum industry, the research underscores the strategic importance of SSCM. The insights from Tseng et al. (2022), Vijayan and Kamarulzaman (2020), and Appiah et al. (2022) highlight the necessity of stakeholder involvement and engagement in driving sustainability initiatives within supply chains.

In summary, the implications of SSCM for stakeholders are profound and wide-ranging. As organizations continue to navigate the complexities of integrating sustainability into their supply chains, the role of stakeholders from suppliers and manufacturers to policymakers and advocates becomes increasingly critical. The research underscores the need for collaborative efforts and strategic planning to achieve sustainable supply chain management, ensuring environmental, social, and economic performance are balanced and optimized.

CONCLUSIONS

The exploration of cybersecurity challenges within the realm of sustainable supply chain management has unveiled intricate dynamics between securing digital infrastructures and advancing sustainability objectives. This study has illuminated the nuanced interplay between cybersecurity practices and sustainable supply chain management, highlighting the essential role of integrating these domains to foster resilient, transparent, and responsible supply networks.

The key findings from this investigation reveal that cybersecurity and sustainability, rather than being at odds, can be synergistically aligned to bolster supply chain resilience. The research underscores the criticality of stakeholder engagement across the spectrum, from

suppliers to policymakers, in crafting and implementing cybersecurity strategies that do not compromise on sustainability goals. Emerging technologies such as blockchain, artificial intelligence, and the Internet of Things have emerged as pivotal tools, offering new pathways to secure supply chains while enhancing their sustainability (Aderibigbe et al., 2023).

Looking into the future landscape, the study acknowledges the dual nature of challenges and opportunities presented by the evolving digital and cyber threat landscape. While the advancement of technology and the sophistication of cyber threats pose continuous challenges, they also open doors to innovation in cybersecurity solutions that can simultaneously drive sustainability. The opportunity for cross-industry collaboration and the development of comprehensive regulatory frameworks stand out as crucial elements in navigating the future of cybersecure sustainable supply chains. In response to these insights, the study offers strategic recommendations aimed at both industry leaders and policymakers. For industry leaders, the emphasis is on fostering a culture that values both cybersecurity and sustainability, through investments in training, partnerships for technology sharing, and comprehensive risk management strategies. Policymakers are encouraged to develop regulatory standards that balance cybersecurity and sustainability, support technological innovation, and promote public-private partnerships.

As the digital landscape continues to evolve, so too will the intersection of cybersecurity and sustainable supply chain management. Future research directions are suggested to include longitudinal studies to assess the impact of cybersecurity measures on sustainability, comparative analyses across industries, and investigations into the human and organizational factors influencing the adoption of these practices.

Finally, the journey toward integrating cybersecurity within sustainable supply chain management is complex and ongoing. It demands continuous innovation, strategic collaboration, and foresight. By addressing the research gaps identified and adhering to the strategic recommendations proposed, stakeholders can significantly contribute to shaping resilient, secure, and sustainable supply chains for the future. This study not only contributes to the academic discourse but also offers practical insights for navigating the challenges and opportunities at the nexus of cybersecurity and sustainability in supply chain management.

Reference

Abd Latif, M. N., Sarawak, S., Abd Aziz, N. A., Hussin, N., & Abdul Aziz, Z. (2021). Cyber security in supply chain management: A systematic review. *LogForum, 17*(1), 49-57 https://doi.org/10.17270/J.LOG.2021555

Aderibigbe, A. O., Efosa, P. O., Nwaobia, N.K., Gidiagba, J.O. & Ani, E. C., (2023). Artificial intelligence in developing countries: bridging the gap between potential and implementation

Adewusi, A. O., Okoli, U. I., Olorunsogo, T., Adaga, E., Daraojimba, D. O., & Obi, O. C. (2024). Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA. *World Journal of Advanced Research and Reviews, 21*(1), 2263-2275. https://doi.org/10.30574/wjarr.2024.21.1.0313

Ajala, O.A. & Balogun, O. (2024). Leveraging AI/ML for anomaly detection, threat prediction, and automated response. *World Journal of Advanced Research and Reviews, 21*(1), 2584-2598. https://doi.org/10.30574/wjarr.2024.21.1.0287

Ajayi-Nifise, A. O., Falaiye, T., Olubusola, O., Daraojimba, A. I., & Mhlongo, N. Z. (2024). Blockchain in US Accounting: A Review: Assessing Its Transformative Potential for Enhancing Transparency and Integrity. *Finance & Accounting Research Journal, 6*(2), pp.159-182.

Anjum, N., Sakib, N., Rodriguez-Cardenas, J., Brookins, C., Norouzinia, A., Shavers, A., & Shahriar, H. (2023). Uncovering software supply chains vulnerability: a review of attack vectors, stakeholders, and regulatory frameworks. In 2023 IEEE 47th Annual Computers, Software, and Applications Conference, (pp. 1816-1821). IEEE. DOI: 10.1109/COMPSAC57700.2023.00281

Appiah, M.K., Boateng, F., Abugri, A., & Barnes, S. (2022). Modeling the implications of sustainable supply chain practices on sustainable performance in Ghana's petroleum industry: the role of stakeholders' pressure. *International Journal of Sustainable Engineering, 15*(1), 312-322. DOI: 10.1080/19397038.2022.2149875

Berroir, F., Pyszkowski, M., Omar, M. & Mack, N. (2023). Construction supply chain product data integration for lean and green site logistics. Proceedings of the 31st Annual Conference of the International Group for Lean Construction (IGLC31), 1662–1673. DOI: 10.24928/2023/0154

Berry, H. S. (2023). The importance of cybersecurity in supply chain. In 2023 11th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE. DOI: 10.1109/ISDFS58141.2023.10131834.

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2021). Cyber supply chain risk management practices for systems and organizations (No. NIST Special Publication (SP) 800-161 Rev. 1 (Draft)). National Institute of Standards and Technology. DOI: 10.6028/nist.sp.800-161r1-draft2

Cheung, K.-F., Bell, M. G. H., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review, 146*, 102217. https://doi.org/10.1016/J.TRE.2020.102217

Cinar, B. (2023). Supply chain cybersecurity: risks, challenges, and strategies for a globalized world. *Journal of Engineering Research and Reports, 25*(9), 196-210. DOI: 10.9734/jerr/2023/v25i9993

Dai, D., Wu, X., Si, F., Feng, Z., & Chu, W. (2023). Complex characteristics analysis of time-delay digital supply chain driven by cybersecurity. *Kybernetes, 52*(9), 3362-3390. DOI: 10.1108/k-08-2021-0738

Dai, X. (2022). Supply chain relationship quality and corporate technological innovations: A multimethod study. *Sustainability, 14*(15), 9203. DOI: 10.3390/su14159203

D'Aleo, V. (2016). Supply chain management: overview, competition and competences, how to exploit the'hidden capabilities'. *International Journal of Management and Network Economics, 3*(4), 336-346 https://doi.org/10.1504/IJMNE.2016.079878

Damtew, A. W., Borena, T., & Yilma, Y. (2021). The roles of cloud-based supply chain integration on firm performances and competitiveness. *International Journal of Industrial and Manufacturing Systems Engineering, 6*(3), 49-58. DOI: 10.11648/J.IJIMSE.20210603.12

de Sousa Jabbour, A. B. L., Jabbour, C. J. C., Hingley, M., Vilalta-Perdomo, E. L., Ramsden, G., & Twigg, D. (2020). Sustainability of supply chains in the wake of the coronavirus (COVID-19/SARS-CoV-2) pandemic: lessons and trends. *Modern Supply Chain Research and Applications, 2*(3), 117-122. https://doi.org/10.1108/mscra-05-2020-0011

Deane, J., Baker, W., & Rees, L. (2023). Cybersecurity in supply chains: quantifying risk. *Journal of Computer Information Systems, 63*(3), 507-521. DOI: 10.1080/08874417.2022.2081882

Duque-Uribe, V., Sarache, W., & Gutiérrez, E. V. (2019). Sustainable supply chain management practices and sustainable performance in hospitals: a systematic review and integrative framework. *Sustainability, 11(*21), 5949. DOI: 10.3390/su11215949

Frazzon, E. M., Rodriguez, C. M. T., Pereira, M. M., Pires, M. C., & Uhlmann, I. (2019). Towards supply chain management 4.0. *Brazilian Journal of Operations & Production Management, 16*(2), 180-191. https://doi.org/10.14488/BJOPM.2019.V16.N2.A2

Fulconis, F., & Philipp, B. (2019). The supply chain facing the challenges of e-commerce delivery: between integration and flexibility, what packaging solutions? *Logistics & Management, 27*(2), 132-147. DOI: 10.1080/12507970.2018.1546127

Hasan, I., & Habib, M. (2022). The future of supply chain management through technological advancements. *International Supply Chain Technology Journal, 8*(6). https://doi.org/10.20545/isctj.v08.i06.01

Hryhorak, M. Y., Trushkina, N. V., & Kitrish, K. Y. (2022). Organizational and economic mechanism of strategic management of sustainability of supply chains of industrial enterprises. *Electronic Scientific and Practical Publication in Economic Sciences*. https://doi.org/10.46783/smart-scm/2022-11-5

Huang, H. (2022). Green supply chain management and its impact on economic-environmental performance: evidence from Asian countries. *Journal of Environmental and Public Health, 2022.* DOI: 10.1155/2022/7035260

Khan, S. A. R., Yu, Z., Golpira, H., Sharif, A., & Mardani, A. (2021). A state-of-the-art review and meta-analysis on sustainable supply chain management: Future research directions. *Journal of Cleaner Production, 278,* 123357. DOI: 10.1016/j.jclepro.2020.123357

Kottala, S. Y. (2021). Sustainable supply chain management practices: a review. *International Journal of Social Ecology and Sustainable Development (IJSESD), 12*(3), 47-65. http://doi.org/10.4018/IJSESD.2021070104

Kumar, S., & Mallipeddi, R. R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management, 31*(12), 4488-4500. https://doi.org/10.1111/poms.13859

Lamba, A., Singh, S., Balvinder, S., Dutta, N., & Rela, S. (2017). Analyzing and fixing cyber security threats for supply chain management. *International Journal for Technological Research in Engineering, 4*(5). https://doi.org/10.2139/ssrn.3492687

Masip-Bruin, X., Marín-Tordera, E., Ruiz, J., Jukan, A., Trakadas, P., Cernivec, A., Lioy, A., López, D. R., Santos, H., Gonos, A., Silva, A., Soriano, J., & Kalogiannis, G. (2021).

Cybersecurity in ICT supply chains: key challenges and a relevant architecture. *Sensors, 21*(18), 6057. https://doi.org/10.3390/s21186057

Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research, 60*(1), 162-183. https://doi.org/10.1080/00207543.2021.1984606

Munir, M. A., Habib, M. S., Hussain, A., Shahbaz, M. A., Qamar, A., Masood, T., ... & Salman, C. A. (2022). Blockchain adoption for sustainable supply chain management: Economic, environmental, and social perspectives. *Frontiers in Energy Research, 10,* 899632. DOI: 10.3389/fenrg.2022.899632.

Oguejiofor, B. B., Omotosho, A., Abioye, K. M., Alabi, A. M., Oguntoyinbo, F. N., Daraojimba, A. I., & Daraojimba, C. (2023). A review on data-driven regulatory compliance in Nigeria. *International Journal of applied research in social sciences, 5*(8), 231-243.

Okoye, C. C., Ofodile, O. C., Tula, S. T., Ajayi-Nifise, A. O., Falaiye, T., Ejairu, E., & Addy, W. A. (2024). Risk management in international supply chains: a review with USA and African Cases. *Magna Scientia Advanced Research and Reviews, 10*(01), 256-264.

Ozkan-Ozen, Y. D., Sezer, D., Ozbiltekin-Pala, M., & Kazançoğlu, Y. (2023). Risks of data-driven technologies in sustainable supply chain management. *Management of Environmental Quality, 33*(4), 926-942. https://doi.org/10.1108/meq-03-2022-0051

Paulsen, C., Paulsen, C., Boyens, J., Ng, J., Winkler, K., & Gimbi, J. (2020). Impact analysis tool for interdependent cyber supply chain risks. US Department of Commerce, National Institute of Standards and Technology. DOI: 10.6028/nist.ir.8272-draft

Prathyusha, J. P., Jyothi, V. E., Jhansi, V., Chowdary, N. S., Madhuri, A., & Sindhura, S. (2023). Securing the cyber supply chain: a risk-based approach to threat assessment and mitigation. In 2023 4th International Conference on Electronics and Sustainable Communication Systems, pp. 508-513. IEEE. https://doi.org/10.1109/ICESC57686.2023.10193255

Radmanesh, S.-A., Haji, A., & Valilai, O. F. (2023). Blockchain-Based Architecture for a Sustainable Supply Chain in Cloud Architecture. *Sustainability, 15*(11), 9072. https://doi.org/10.3390/su15119072

Reis, O., Eneh, N. E., Ehimuan, B., Anyanwu, A., Olorunsogo, T., & Abrahams, T. O. (2024). Privacy law challenges in the digital age: a global review of legislation and enforcement. *International Journal of Applied Research in Social Sciences, 6*(1), 73-88. https://doi.org/10.51594/ijarss.v6i1.733.

Rogers, Z.S. (2020). Supply Chain cybersecurity: procurement's role in securing the network', in Thomas Y. Choi, and others (eds). The Oxford Handbook of Supply Chain Management (online edn, Oxford Academic, 6. https://doi.org/10.1093/oxfordhb/9780190066727.013.9

Santos, H., Oliveira, A., Soares, L., Satis, A., & Santos, A. (2021). Information Security Assessment and Certification within Supply Chains. In Proceedings of the 16th International Conference on Availability, Reliability and Security (pp. 1-6). DOI: 10.1145/3465481.3470078

Sawik, T. (2022). Balancing cybersecurity in a supply chain under direct and indirect cyber risks. *International Journal of Production Research, 60*(2), 766-782. https://doi.org/10.1080/00207543.2021.1914356

Sayogo, D., Zhang, J., Luna-Reyes, L., Jarman, H., Tayi, G., Andersen, D. L., Pardo, T., & Andersen, D. (2015). Challenges and requirements for developing data architecture supporting integration of sustainable supply chains. *Information Technology and Management, 16*(1), 5-18. https://doi.org/10.1007/S10799-014-0203-3

Schleper, M. C., Gold, S., Trautrims, A., & Baldock, D. (2021). Pandemic-induced knowledge gaps in operations and supply chain management: COVID-19's impacts on retailing. *International Journal of Operations & Production Management, 41*(3), 193-205. DOI: 10.1108/IJOPM-12-2020-0837

Singh, P. K., & Maheswaran, R. (2023). Analysis of social barriers to sustainable innovation and digitisation in supply chain. *Environment, Development and Sustainability*, 1-26.DOI: 10.1007/s10668-023-02931-9

Tseng, M. L., Ha, H. M., Lim, M. K., Wu, K. J., & Iranmanesh, M. (2022). Sustainable supply chain management in stakeholders: supporting from sustainable supply and process management in the healthcare industry in Vietnam. *International Journal of Logistics Research and Applications, 25*(4-5), 364-383. DOI: 10.1080/13675567.2020.1749577

Vijayan, G., & Kamarulzaman, N. H. (2020). An introduction to sustainable supply chain management and business implications. In Sustainable business: Concepts, methodologies, tools, and applications, pp. 158-176. IGI Global. DOI: 10.4018/978-1-5225-0635-5.CH002

Vollmer, B. (2021). NATOs Mission-Critical space capabilities under threat: cybersecurity gaps in the military space asset supply chain. arXiv preprint arXiv:2102.09674. https://arxiv.org/abs/2102.09674.

Wallis, T., & Dorey, P. (2023). Implementing partnerships in energy supply chain cybersecurity resilience. *Energies, 16*(4), 1868. DOI: 10.3390/en16041868

Wang, F., Hou, Z., Huang, H., Juanatas, R., & Niguidula, J. (2023). Challenges and innovations in implementing sustainable supply chain smart manufacturing in the metal recycling industry. *Scientific and Social Research, 5*(11), 27-32. DOI: 10.26689/ssr.v5i11.5525

Wen, S., Tang, H., Ying, F., & Wu, G. (2023). Exploring the global research trends of supply chain management of construction projects based on a bibliometric analysis: current status and future prospects. *Buildings, 13*(2), 373. https://doi.org/10.3390/buildings13020373

Wright, J. (2023). Healthcare cybersecurity and cybercrime supply chain risk management. *Health Economics and Management Review, 4*(4), 17-27. https://doi.org/10.61093/hem.2023.4-02.

Zhao, D., & Wang, X. (2024). Evolutionary game of digital decision-making in supply chains based on system dynamics. *RAIRO-Operations Research, 58*(1), 475-510. DOI: 10.1051/ro/2023190

Zhao, W., Luo, Z., & Liu, Q. (2023). Does supply chain matter for environmental firm performance: mediating role of financial development in China. *Economic Change and Restructuring, 56*(6), 3811-3837. DOI: 10.1007/s10644-022-09410-7