European Research Studies Journal
Volume XXVIII, Issue 1, 2025

pp. 44-56

The Impact of Supply Chain Security Management on the Functioning of Modern Organizations

Submitted 22/12/24, 1st revision 17/01/25, 2nd revision 29/01/25, accepted 15/02/25

Sławomir Żurawski[1], Zbigniew Ciekanowski[2], Yury Pauliuchuk[3], Emil Ratter[4]

Abstract:

Purpose: *The purpose of this study is to analyze the impact of supply chain security management on the functioning of modern organizations, with a particular focus on operational continuity, financial stability, and compliance with legal regulations. It aims to assess how effective security management strategies contribute to risk reduction and improve overall supply chain performance.*
Design/methodology/approach: *The research problem that serves as the starting point for the study is formulated as follows: How does supply chain security management affect the operational and strategic functioning of modern organizations? The hypothesis posits that effective supply chain security management significantly enhances an organization's operational stability, reduces financial risks, and promotes regulatory compliance, which translates into increased competitiveness and positive financial outcomes. Appropriate research methods were employed in the study. A comprehensive literature review on supply chain security management, risk management models, and compliance frameworks was conducted. Additionally, a case study was performed, and an analysis of survey reports directed at supply chain managers across various industries was carried out. Data collected from these sources were analyzed to identify patterns, correlations, and insights regarding the implementation of security measures and their impact on organizational performance.*
Findings: *The study reveals that effective supply chain security management significantly improves operational continuity by mitigating risks associated with data breaches, supply disruptions, and non-compliance with legal regulations. Furthermore, organizations that prioritize security within their supply chains experience better financial stability and a stronger competitive position. The research also emphasizes that compliance with regulations, particularly those such as GDPR and ISO 27001, is crucial for protecting both organizational data and reputation.*
Practical Implications: *The findings highlight the need for organizations to invest in robust security measures within their supply chains to ensure long-term operational success. It is*

[1]*State Academy of Applied Sciences in Chełm, Poland, ORCID: 0000-0001-9527-3391, e-mail: slawomir.zurawski@onet.pl;*
[2]*John Paul II University in Biala Podlaska, Poland, ORCID 0000-0002-0549-894X, e-mail: zbigniew@ciekanowski.pl;*
[3]*University of Siedlce, Faculty of Social Sciences, Poland, ORCID 0000-0002-2077-5124, e-mail: y.pauliuchuk@wp.pl;*
[4]*Warsaw Management University, Poland, ORCID: 0000-0001-8872-3286, e-mail: em.ratter@gmail.com;*

recommended that companies conduct regular risk assessments, perform thorough supplier audits, and align their practices with international standards and regulations. Such an approach will help mitigate risks and ensure compliance, thereby strengthening trust among stakeholders and customers.
Originality/Value: *This research contributes to updating existing literature by offering a comprehensive analysis of the relationship between supply chain security management and organizational performance. It presents practical frameworks that companies can adopt to enhance the resilience of their supply chains. The originality of the study lies in its focus on the areas of security, risk management, and legal compliance, providing practical insights for contemporary organizations.*

Keywords: *Risk management, organization, supply chain security.*

JEL code: *O15, R40, L2, F50.*

Paper type: *Research article.*

1. Introduction

Supply chain security management is a topic that is gaining importance in light of the increasing complexity of global supply chains and the rising threats associated with cybersecurity, climate change, political instability, and pandemics. Modern organizations are becoming more dependent on external suppliers and business partners, making supply chain security one of the key elements in ensuring business continuity and minimizing operational risks.

Supply chain security management involves actions aimed at protecting against threats that can disrupt the flow of goods, services, information, and data within an organization. Today's supply chains are increasingly complicated, with many links (from raw materials to production, transport, and distribution), which raises the potential risk of unforeseen incidents such as system failures, cyberattacks, delivery delays, or product quality issues.

Supply chain security affects organizations at various levels, operational, financial, and reputational. Inadequate security measures can lead to significant production disruptions, increased costs, loss of customers and trust, as well as legal violations that can result in hefty fines. Conversely, effective security management in this area allows for risk minimization, optimization of operational costs, and an increase in trust from customers and business partners.

Consequently, managing supply chain security in modern organizations is an essential component of risk management strategies that not only protect the organization from threats but also build its competitiveness and long-term stability.

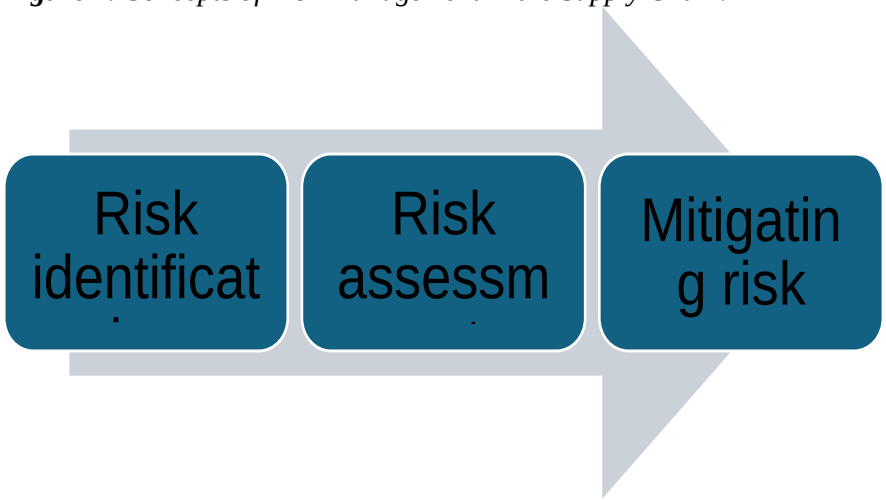
2. Risk Management in Supply Chains

Risk management is currently one of the most important areas of organizational operations as it is closely linked to strategy and achieved goals. (Ciekanowski, Gruchelski, Nowicka, Zdunek, and Żurawski, 2024, p. 145). Additionally, risk management in supply chains is a crucial aspect of modern management aimed at minimizing risks associated with disruptions in the delivery process of goods and services. In light of market globalization, increasing complexity of supply chains, and unpredictable threats (such as climate change, cyberattacks, natural disasters, or political instability), effective risk management has become one of the foundations for maintaining competitiveness and ensuring business continuity.

The supply chain encompasses all stages—from raw material acquisition through production and transport to the distribution of finished products—and is exposed to various threats that can impact its efficiency. Each of these threats carries the risk of disrupting business processes, increasing operational costs, and in some cases even damaging the organization's reputation. Supply chain risk refers to the probability of adopting inappropriate strategies or making poor decisions that could lead to suboptimal logistics system configurations (Kulińska, 2007; Tyagi *et al.*, 2023).

Risk management in supply chains includes a range of activities aimed at identifying, assessing, and monitoring risks as well as implementing strategies that allow for their minimization or transfer. Organizations must not only react to existing threats but also proactively take actions that enhance their supply chain's resilience against future crises. Below are three key concepts for managing risks in supply chains that should be utilized to achieve success and counteract threats.

Figure 1. *Concepts of Risk Management in the Supply Chain.*



Source: *Risk Management in the Supply Chain - A Complete Guide, FourKites https://www.fourkites.com/pl/supply-chain-risk-management/*

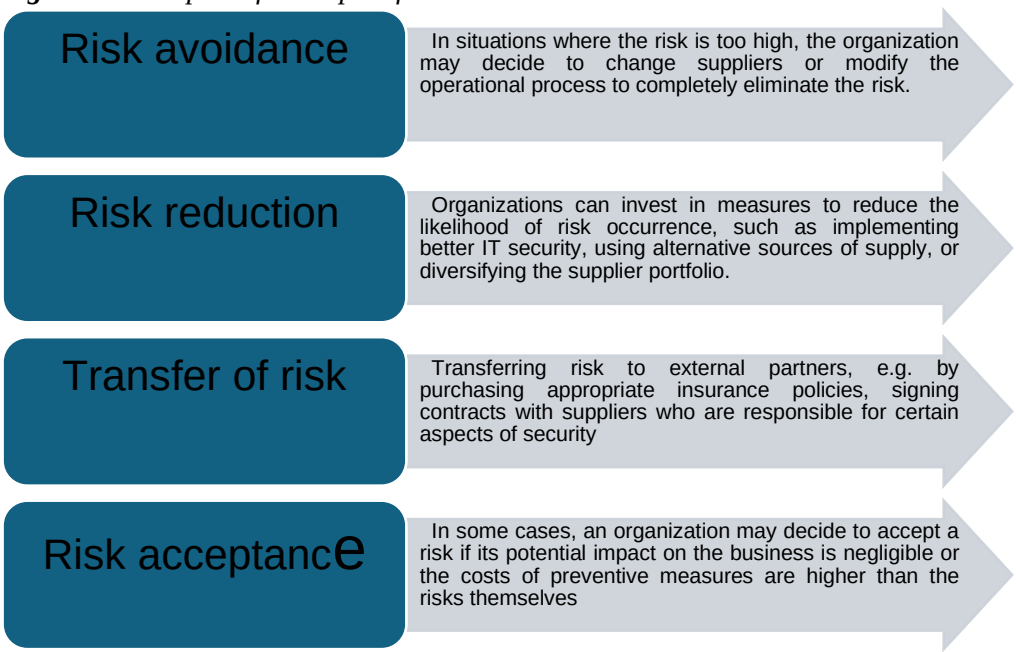
The first step in risk management in the supply chain is identifying risks. These can arise from various sources, such as:

- Supplier-related risks: Financial problems of the supplier, changes in their operational activities, and technological failures can significantly impact the availability of goods or services.
- Operational risks: Delays in transportation, infrastructure failures, issues with storage, or the quality of raw materials can lead to disruptions in production or deliveries.
- External environmental risks: Factors such as political changes, natural disasters, pandemics, economic instability, and cyberattacks can affect the functioning of the supply chain.

Once risks have been identified, the next step is to assess their impact and likelihood of occurrence. To do this, organizations often use various techniques such as SWOT analysis, cause-and-effect analysis, or risk mapping. The goal is to determine which risks have the greatest potential to disrupt operations and should be prioritized.

For example, the risk associated with a cyberattack can have a significant impact on an organization, especially if the company relies on IT systems to manage the entire supply process. When a risk is identified and assessed, the next step is to develop a risk management strategy. There are several approaches to responding to risks, examples of which are presented and described in the diagram below.

Figure 2. *Examples of concepts of reactions to risk.*



Source: *Own elaboration.*

The next key aspect of risk management in the supply chain is monitoring and controlling risks. This process involves continuous assessment of the effectiveness of implemented remedial measures and ongoing adjustments to actions in response to changing market conditions and environments (Auzina *et al.,* 2023).

Technologies such as artificial intelligence, real-time data analysis, and monitoring systems can assist in detecting potential threats and taking swift corrective actions (Kłoczko, 2024, p. 65). Achieving this goal is not always possible due to various barriers to risk management in the supply chain, which are presented in the table below.

Table 1. *Barriers and Principles of Risk Management in the Supply Chain*

Barriers to supply chain risk management	**Principles of supply chain risk management**
● Globalization of supply chains (the share of global markets in most enterprises in the areas of supply, production, and distribution, ● actions focused strictly on cost reduction rather than efficiency, ● poorly managed outsourcing processes, ● the focus of manufacturing enterprises on producing a single product (narrow specialization), ● centralization of distribution, ● increased dependence of the producer on the efficiency of suppliers through an expanded supplier base, ● seasonal, incidental changes in market demand (fluctuation), ● shortening product life cycles, ● lack of access to information, ● errors in information management systems, ● lack of control and evaluation procedures.	● Awareness of risk occurrence, ● Motivating employees to identify their roles in logistics processes and in minimizing supply chain risks, ● Continuous monitoring of the relationships between changes in company strategies and risk profiles, ● Ongoing analysis of the supply chain environment, ● The selection of the best risk management options should be made from the perspective of the entire supply chain and collaboratively by its participants, ● Creation of a contingency plan system, ● Diversification of production or service assortment (diversification), ● Establishment of an evaluation system, ● The length of the production cycle should be minimized, ● Material flows throughout the supply chain should be synchronized, ● Processes should be designed with respect to customer requirements, ● Decisions in the supply chain should be made in a coordinated manner, taking into account their impact on individual participants.

Source: *J. Myszak, M. Sowa, Zarządzanie ryzykiem w łańcuchu dostaw, "PTiL," no. 4/2016 (36), 2016, p. 190.*

Collaboration with suppliers and partners is also an essential element of risk management in the supply chain. Good relationships with suppliers, partners, and other participants in the supply chain can significantly enhance an organization's ability to respond quickly to risks. Regular audits, sharing information about threats, and establishing common safety standards help create more resilient and flexible supply chains.

Properly categorizing types of risks into different categories yields tangible benefits for the entire supply chain. This enables the identification of processes that should be prioritized when developing strategies and indicates those that require greater financial investment to secure against potential threats. Additionally, it allows for the creation of coherent and transparent criteria for assessing various types of risks (developing a risk level hierarchy) and facilitates their comparison, which in turn allows for effective risk management in specific areas of operation (Gaschi-Uciecha, 2014, p. 127).

In the context of safety, managing risk in the supply chain becomes a complex process that requires collaboration with suppliers, logistics partners, and other participants in the process, as well as implementing modern technologies that support monitoring, assessing, and controlling risks. As part of an organization's business continuity strategy, effective risk management not only minimizes losses but also builds trust among customers and stakeholders.

3. Compliance with Regulations and Safety Standards

Managing supply chain security requires compliance with national and international regulations. Organizations must implement appropriate procedures to meet requirements such as:

- ISO 27001 (PN-EN ISO/IEC 27001:2023-08).
- GDPR (Regulation (EU) 2016/679 of the European Parliament and Council dated April 27, 2016).
- HIPAA (Health Insurance Portability and Accountability Act).

These regulations affect how security is managed and require verification of suppliers' ability to meet legal requirements. To ensure compliance with these regulations, organizations must conduct thorough verification of their suppliers and partners. This includes security audits, assessment of data management policies and procedures, and control over protective measures used.

Organizations should require their suppliers to regularly provide documentation regarding compliance with relevant standards and ensure access to audit results and certifications (Urbaniak, 2011, p. 15). Through such actions, organizations can ensure that their supply chain operates in accordance with applicable legal regulations and minimize risks associated with non-compliance.

ISO 27001 is an international standard that specifies requirements for an information security management system (ISMS). Organizations implementing this standard must adopt appropriate procedures and protective measures to ensure data security while preventing loss, theft, or unauthorized access. Compliance with ISO 27001 is crucial in managing supply chain security because organizations must ensure that their suppliers and business partners also meet these requirements. Verifying suppliers for compliance with ISO 27001 allows organizations to minimize risks associated with unauthorized access to sensitive data stored or processed by partners.

The General Data Protection Regulation (GDPR) imposes obligations on organizations regarding the protection of personal data of EU citizens. Organizations must ensure appropriate privacy and data protection procedures, including secure storage and processing of personal information as well as responding to data breaches.

In the context of the supply chain, GDPR requires that suppliers and partners processing personal data on behalf of organizations adhere to the same data protection standards. Consequently, organizations must conduct thorough audits and verification of suppliers regarding their ability to meet GDPR requirements, which helps minimize risks related to data privacy breaches.

HIPAA (Health Insurance Portability and Accountability Act) is a U.S. law concerning the privacy protection of medical data. Organizations processing or storing medical data must adhere to stringent rules for securing this information, including controlling access, securely storing data, and monitoring potential breaches.

In the supply chain—especially within the medical sector—organizations must ensure that their suppliers, logistics partners, and service providers comply with HIPAA rules to ensure full regulatory compliance. Verifying suppliers for adherence to HIPAA standards is crucial to prevent potential financial penalties as well as reputational damage associated with patient privacy breaches.

In summary, adherence to regulations such as ISO 27001, GDPR, or HIPAA in the context of managing supply chain security is essential for ensuring integrity, data security, and protection against legal risks. Organizations must thoroughly verify their suppliers for compliance with these requirements to maintain high standards of security and compliance throughout the supply chain.

4. Challenges and Recommendations in Supply Chain Security Management

Supply chain security management is one of the key elements of operational strategies for modern organizations. In the face of increasing globalization, rapidly changing market conditions, and emerging threats, organizations must confront

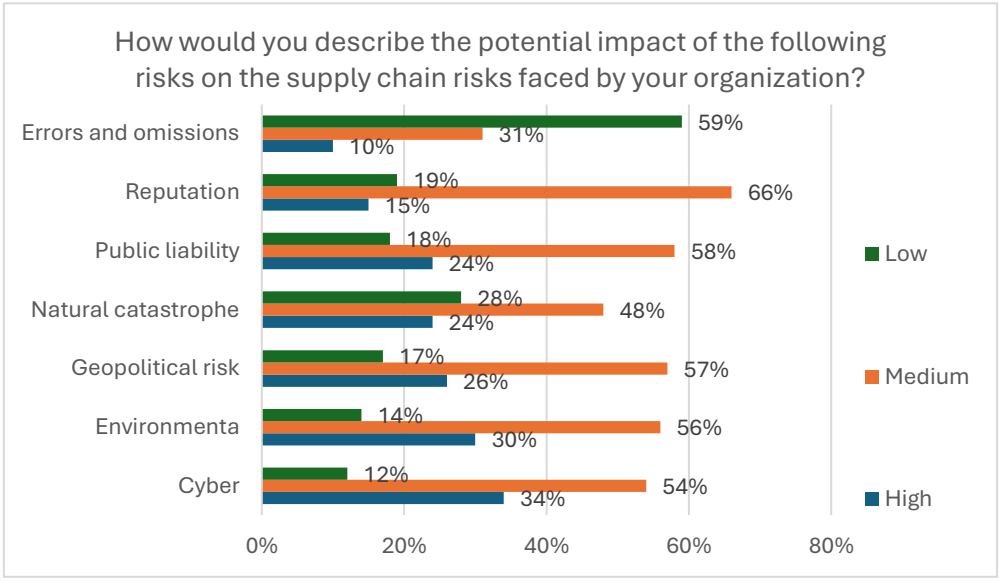
numerous challenges that can impact the stability and continuity of their supply chains. Below are the main challenges associated with security management in this area, along with recommendations that aid in effective risk management.

Modern supply chains are becoming increasingly complex, spanning multiple countries, regions, and industries. This structure heightens risks related to delays, operational errors, and varying safety standards that apply in different parts of the world. Additionally, global disruptions such as pandemics or economic crises can affect operational fluidity throughout the supply chain.

The digitalization of supply chains leads to a growing dependence on IT systems, which is associated with an increased risk of cyberattacks. Hackers may attempt to access sensitive data such as order information, inventory levels, or sales strategies.

Attacks can also disrupt business processes and, in extreme cases, result in data loss, severely impacting the security of the entire supply chain. The potential percentage impact of various risks on the supply chain is illustrated in a chart published in the Global Supply Chain Risk Report 2023.

Figure 3. *Potential impact of the following risks on the supply chain.*



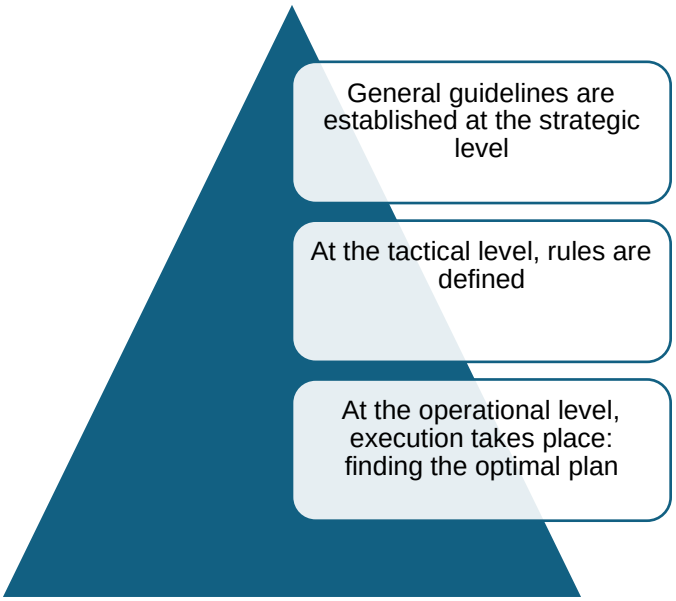
Source: *Global Supply Chain Risk Report, 2023, WTW p. 15.*

The global PwC study conducted in 2020 on the impact of supply chain digitalization on business performance highlighted a very important conclusion: companies that are leaders in supply chain digitalization not only enjoy more automated operations and customer service but also achieve tangible results from their investments in the supply chain, reflected in twice as high revenue growth rates

and cost reductions (PwC, 2020). The use of AI enables numerous improvements, such as increasing the capacity and efficiency of logistics systems (Koszany, Jakubowiec, 2022). In supply chain management, the application of AI is significant in areas involving data utilization and analysis, including forecasting and analytics processes (Kozłowska, 2024, p. 107).

AI provides predictive tools that facilitate demand management and inventory levels in pursuit of optimizing the decision-making process (Huang and Fu, 2019). Below are the levels of supply chain management in the context of digitalization.

Figure 4. *Levels of supply chain management in the context of digitalization*



Source: *Supply chain digitalization, PwC, https://www.pwc.pl/pl/artykuly/cyfryzacja-lancucha-dostaw.html*

Companies are increasingly relying on external suppliers and partners, which carries the risk of insolvency, changes in the quality of services provided, or logistics issues. For this reason, it is essential to regularly monitor the financial stability of suppliers and assess their ability to deliver products according to established standards. Inadequate risk management in this area can lead to serious disruptions in production processes.

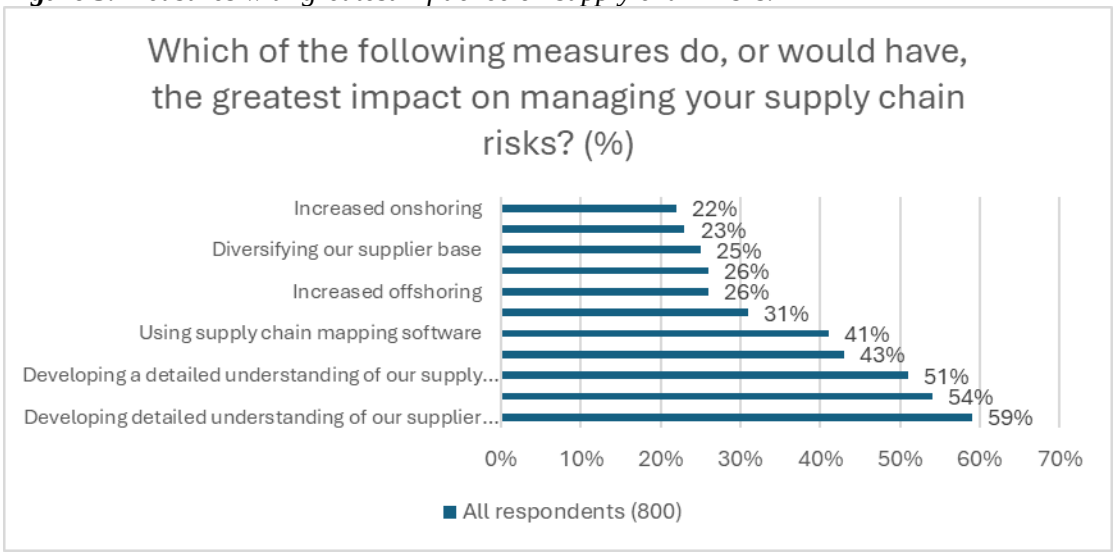
Changing legal regulations, especially those related to personal data protection (e.g., GDPR) or regulations concerning environmental responsibility, poses another challenge for organizations managing supply chains. Implementing appropriate compliance systems and adapting processes to new legal standards is crucial to avoid sanctions and maintain the organization's reputation in the market.

Climate change and political instability can cause supply disruptions, particularly when supply chains depend on regions prone to natural disasters, wars, or unstable political conditions (Global Supply Chain Risk Report, WTW, 2023, p. 22). Events such as hurricanes, floods, or geopolitical tensions can significantly impact the availability of raw materials or finished products, creating risks for the continuity of business operations.

In organizations involved in supply chain management, a key step is implementing an effective risk management strategy. Regular risk analyses allow for the identification of potential threats in the supply chain, assessment of their impact, and development of contingency plans. Organizations should also ensure that these analyses are up to date, considering dynamic changes in the business environment.

The WTW Global Supply Chain Risk Report 2023 clearly indicates that people want to know more about their suppliers and have as much visibility as possible down to external tiers of the chain. Many believe that filling knowledge gaps is key to managing supply chain risk. Below is a chart showing measures that have the greatest impact on supply chain risk.

Figure 5. *Measures with greatest influence on supply chain risks.*



Source: *Global Supply Chain Risk Report, 2023, WTW p. 18.*

To the question of which measures would have the greatest impact on risk management, 59% of respondents indicated: detailed understanding of the supplier network, 54% improvement of relationships with suppliers and customers, and 51% detailed understanding of our supply chain. The next most popular response also emphasizes the desire for deeper knowledge 43% pointed to improving data and sharing it, with this percentage rising to 52% in the case of complex manufacturing (Global Supply Chain Risk Report, WTW, 2023, p. 18).

To effectively monitor and manage risk, organizations should invest in modern technologies such as supply chain management (SCM) systems that enable tracking of products at every stage of their flow (Kanicki, 2011, p. 92). These technologies allow for quicker detection of potential threats such as delivery delays or quality issues. Additionally, implementing data protection and cybersecurity systems can help safeguard against cyberattacks (Nermend *et al.*, 2021).

Building strong and transparent relationships with suppliers and business partners is crucial in supply chain risk management. Regular communication, joint establishment of safety standards, and sharing information about risks can significantly enhance supply chain security. Organizations should also consider diversifying suppliers to reduce dependence on a single source and increase resilience to disruptions.

To effectively manage security within the supply chain, it is essential that employees are adequately trained in risk and security management. These trainings should cover both technical issues and aspects of relationship management with suppliers as well as threat mitigation. Furthermore, raising awareness of risks among employees enables quicker responses when problems arise in the supply chain.

Regular audits and monitoring of all elements of the supply chain help detect potential issues before they become serious threats. These audits should encompass both operational aspects and IT security to ensure that all processes within the supply chain comply with established standards and procedures. Digital transformation introduces numerous changes that revolutionize how organizations operate and their security. Increased use of digital technologies brings significant benefits but also presents new security challenges (Nowicka, Ciekanowski, Kudins, and Dąbrowski, 2024, p. 469).

Effective supply chain security management requires a risk-based approach, implementation of appropriate technologies, and collaboration with partners and suppliers. Through these actions, organizations can minimize threats, improve operational efficiency, and enhance resilience to disruptions, which ultimately translates into their competitiveness and market stability.

5. Conclusions

Supply chain security management is crucial for the functioning of modern organizations. In light of market globalization, increasing dependence on new technologies, and constant changes in the external environment, organizations face numerous challenges that can affect the stability of their operations. Effective management of supply chain security is essential for ensuring operational continuity, minimizing risks, and protecting company resources.

Modern organizations must identify, assess, and respond to security threats across various areas of their supply chains, such as cyberattack risks, changing legal regulations, supplier instability, or geopolitical factors.

Supply chain security management impacts organizations at multiple levels—from operational to strategic. Organizations that effectively manage these risks can expect greater stability, better financial performance, and increased competitiveness in the market. Conversely, neglecting supply chain security issues can lead to serious consequences both materially and reputationally. Risk management becomes a key element of organizational strategy that helps minimize the impact of threats on business operations while ensuring long-term growth.

Collaboration with suppliers and business partners, investment in modern technologies, and adaptation to changing legal regulations form the foundation for effective supply chain security management. Conducting audits, monitoring risks, verifying compliance with applicable standards such as ISO 27001, GDPR or HIPAA, and maintaining transparency in operations allow organizations to maintain high levels of security. Adapting processes to legal requirements not only protects organizations from sanctions but also builds trust among customers, suppliers, and other business partners.

Despite significant progress in supply chain security management, there remains a need for further analysis, especially in light of the rapidly changing environment. As new technologies evolve and new threats emerge, organizations will need to adjust their risk management approaches. Future research will be essential for identifying innovations such as artificial intelligence, blockchain or automation that may influence supply chain security.
Additionally, analyzing the impact of changes in legal regulations, particularly those related to data protection or sustainable development—will be crucial. Changing market demands and regulatory requirements create new challenges that necessitate a flexible and integrated approach to managing supply chain security.

Supply chain security management will increasingly become a complex process requiring rapid adaptation to new realities. Ongoing analysis in this area will enable the development of modern management strategies that effectively address growing challenges related to supply chain security while allowing organizations to maintain stability, competitiveness, and growth in a dynamically changing business environment.

References:

Auzina, I., Volkova, T., Norena-Chavez, D., Kadłubek, M., Thalassinos, E. 2023. Cyber Incident Response Managerial Approaches for Enhancing Small–Medium-Size Enterprise's Cyber Maturity. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (pp. 175-190). Emerald Publishing Limited.

Ciekanowski, M., Żurawski, S., Pauliuchuk, Y., Ciekanowski, Z., Marciniak, S. 2024. Strategies for Effective Cybersecurity Management in Organizations. European Research Studies Journal, Volume XXVII, Issue 1, pp. 365-379.

Ciekanowski, Z., Gruchelski, M., Nowicka, J., Zdunek, M., Żurawski, S. 2024. Risk Management and Organizational Resistance to Threats. European Research Studies Journal, Volume XXVII, Issue 1, pp. 142-153.

Cyfryzacja łańcucha dostaw, PwC. https://www.pwc.pl/pl/artykuly/cyfryzacja-lancucha-dostaw.html.

Gaschi-Uciecha, A. 2014. Istota ryzyka w procesach logistycznych. Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, nr. 70, pp. 119-129.

Global Supply Chain Risk Report, WTW. 2023.

Health Insurance Portability and Accountability Act. 1996.

Huang, Y., Li, J., Fu, J. 2019. Review on application of artificial intelligence in civil engineering. Computer Modelling in Engineering & Sciences, 121(3), 845-875.

Kanicki, T. 2011. Systemy informatyczne w logistyce. Ekonomia i Zarządzanie, vol. 3, no. 4, pp. 87-97.

Kłoczko, A. 2024. Wykorzystanie sztucznej inteligencji w zarządzaniu organizacją jako potencjał obniżenia kosztów. Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie, Nr. 55, pp. 61-77.

Koszany, D., Jakubowiec, M. 2020. Transformacja cyfrowa przedsiębiorstw Zeszyt Naukowy. Wyższa Szkoła Zarządzania i Bankowości w Krakowie, Volumen 66, pp. 12-21.

Kulińska, E. 2007. Zarządzanie ryzykiem w łańcuchu dostaw. Logistyka, nr 1, pp. 18-21.

Nowicka, J., Ciekanowski, Z., Kudins, J., Dąbrowski P. 2024. Managing Organizational Security in the Era of Digital Transformation. European Research Studies Journal, Volume XXVII, Issue 3, pp. 460-471.

Myszak, J., Sowa, M. 2016. Zarządzanie ryzykiem w łańcuchu dostaw. PTiL, nr. 4/2016 (36), pp. 185-192.

Nermend, K., Łatuszyńska, M., Thalassinos, E. (Eds.). 2021. Decision-Making in Management: Methods and Behavioral Tools. Springer Nature.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w zw, iązku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Tyagi, P., Grima, S., Sood, K., Balamurugan, B., Özen, E., Thalassinos, E. (Eds.). 2023. Smart analytics, artificial intelligence and sustainable performance management in a global digitalised economy. Emerald Publishing Limited.

Urbaniak, M. 2011. Międzynarodowe standardy zarządzania w łańcuchu dostaw. Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 235, pp. 15-24.

Zarządzanie ryzykiem w łańcuchu dostaw - kompletny przewodnik, FourKites. https://www.fourkites.com/pl/supply-chain-risk-management/.