

ОБЩЕСТВЕНИ КОМУНИКАЦИИ И ИНФОРМАЦИОННИ НАУКИ
PUBLIC COMMUNICATIONS AND INFORMATION SCIENCES

ECONOMIC CHALLENGES FOR SECURITY IN THE SUPPLY CHAIN

Bernd Michael Engler

University of Library Studies and Information Technologies

<https://doi.org/10.70300/DCLJ8447>

Abstract: *Security in supply chains is a key component in ensuring that processes and process participants can interact seamlessly and without disruption. Disruptions can be caused by both intentional and unintentional actions. Disruptions in the process can lead to significant damage. This damage can be financial, reputational, or legal in nature. To avert such damage, participants in a supply chain are required to prevent disruptions or reduce them to a minimum. This article examines the economic challenges in the supply chain. Based on a systematic literature review, the risks are presented, followed by the security aspects in the supply chain. The subsequent analysis of the challenges involved in mitigating these risks focuses on cybersecurity. Existing and implemented measures to defend against cyberattacks are highlighted, along with an outlook for the future. It becomes clear that cybersecurity has been a challenge in the past and will remain one in the future.*

Keywords: *business processes; supply chain security; cybersecurity challenges; supply chain resilience*

INTRODUCTION

Global supply chains are important for companies and allow them to compete in the international market. To achieve this, global networks, information and material flows, and business processes throughout the entire supply chain must be maintained (Kotzab 2005, p. 48).

At the same time, the complexity of supply chains has increased significantly in the past, and with it, their vulnerability to disruptions. This became clear, for example, during the COVID-19 pandemic. In a survey conducted as part of a study, more than 60% of respondents stated that the pandemic had had a significant or very significant impact on their supply chains (Huth 2025, p. 2).

Cloud technologies are being used more and more in businesses. A milestone in the use of cloud services was the launch of Amazon Web Services in 2006. This adoption was made possible by the growing prevalence of mobile interactive applications, the ability to utilize parallel computing resources, greater analytical capabilities, and the ability to extend computationally intensive desktop applications through cloud services (Armbrust et al. 2009, pp. 6–8).

A representative empirical study surveying more than 600 companies revealed that by 2025, 90% of the companies surveyed will already be using them. This represents a 9% increase compared to 2024. The 90% consists of both public and private clouds, with 41% already operating using a multi-cloud approach – that is, utilizing multiple cloud providers. Twenty-nine percent are using cloud technology as a hybrid approach, meaning in combination with their existing IT applications. It is noted that 67% of companies would come to a standstill without the use of cloud technologies (Wintergest 2025, pp. 2–10).

However, deliberately caused disruptions, such as cyberattacks on companies' information technology (IT) systems, can also lead to significant disruptions in business processes (Sarkis 2024, p. 562).

This article aims to highlight the challenges in the supply chain related to security, specifically cybersecurity, and discuss how resilience can be strengthened.

RESEARCH METHODOLOGY

This section provides an introduction to the topic and presents the research question. Based on a qualitative study and a systematic literature review, the theoretical foundations regarding safety aspects within the supply chain are developed.

The search is limited to Google Scholar and freely accessible sources and literature published by Springer. Sources from German- and English-speaking countries published since 2000 have been included.

The search was conducted using the following search combinations:

– **Google Scholar:** “supply chain security” AND “cybersecurity challenges” AND “supply chain resilience”

– **Springer:** “supply chain security” AND “security challenges”

The search yielded the following results:

– **Google Scholar:** The search returned 162 results. After evaluating their relevance and to avoid duplicates, approximately 20 sources were determined to be relevant.

– **Springer:** The search yielded 72 results. Since this article does not focus on software, container, or AI security, the literature can be narrowed down to the following approximately 15 sources.

To ensure the information is up-to-date, the literature review is limited to sources published no earlier than 2020. This article includes books, articles, and academic publications. The selection of literature is based on a search of the platforms mentioned, followed by an evaluation of the title, keywords, and abstract. If the criteria are met, a comprehensive literature review is conducted.

The final result is a recommendation regarding which aspects of supply chain security should be given greater consideration.

RESULTS

If supply chains do not function properly, a disruption occurs. These supply chain disruptions can be divided into four categories. They are:

- Environmental risks
- External risks
- Collaboration risks, as well as
- Internal risks

While environmental risks relate to the company or its underlying supply chain (e.g., natural disasters), external risks relate to demand and supply risks (e.g., transportation, delivery, or quality, as well as payment and sales conditions). Cooperation risks include both cultural differences between cooperation partners and divergent objectives, while internal corporate risks include management risks (e.g., poor decision-making) as well as disruptions to value-adding processes (Wellbrock und Ludin 2025, p. 10).

To ensure a smoothly functioning supply chain, the following security considerations must be taken into account:

Physical security: This term encompasses several aspects under the umbrella of VUCA (volatility, uncertainty, complexity, ambiguity) (Fig. 1). It involves fluctuations in variables within the supply chain, uncertainties due to missing input data needed for decision-making, and changes in the variety or overall clarity of the available information (Huth 2025, pp. 52–57).

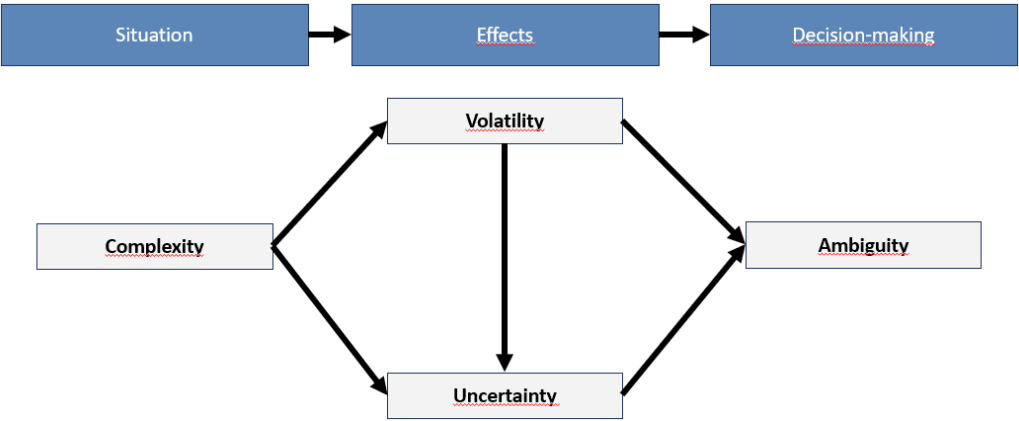


Fig. 1. VUCA Terms and Relationships (Huth 2025, p. 57)

Furthermore, the area of physical security also covers product piracy, theft, or illegal distribution, as well as the tampering of hardware. A distinction is made between attacks on customers and suppliers. The former refers to physical attacks, such as those involving counterfeit or tampered hardware or break-ins, while the latter refers more to theft, tampering, and counterfeiting with the aim of modifying or destroying such (Khokhar et al. 2024, pp. 255–260).

Cybersecurity: Here, various aspects are considered as input variables for cybersecurity, categorized into vectors (Fig. 2). The causes can stem from the network (e.g., network congestion), software vulnerabilities (e.g., malware), in hardware (e.g., due to tampered computer chips), through social engineering (e.g., via phone calls or phishing emails), and in the field of big data (e.g., when using very large amounts of data that require special protection due to their complexity). It is important to note that a disruption can be caused either intentionally or unintentionally (Hammi und El Madhoun 2026, pp. 5–14).

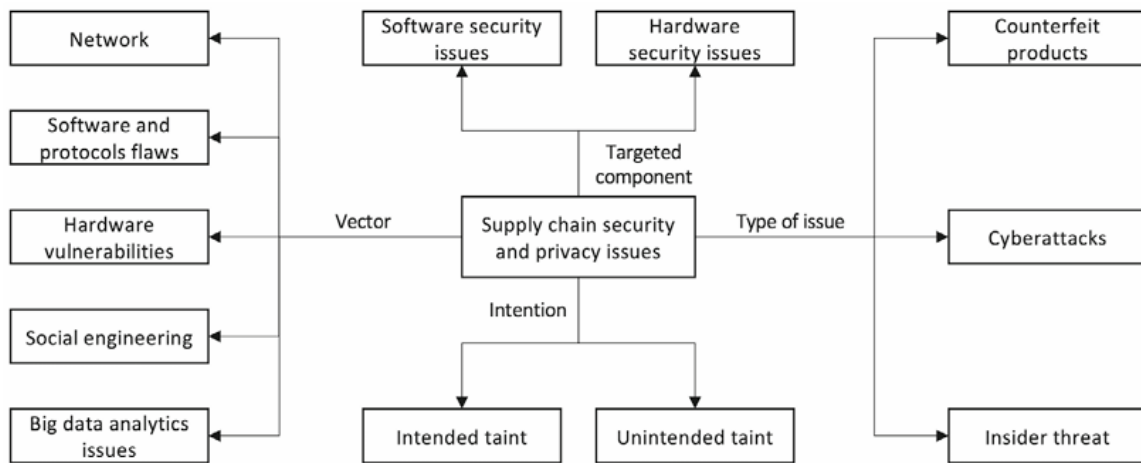


Fig. 2. Classification of Causes of Supply Chain Security Issues (Hammi und El Madhoun 2026, p. 7)

Cyber threats encompass a broad spectrum of attack vectors and vulnerabilities that jeopardize the availability, confidentiality, and integrity of supply chain processes and data. Since every component within the system is vulnerable to cyberattacks, the threats and vulnerabilities associated with the cyber supply chain (CSC) pose significant challenges to supply chain security. Risk-based approaches are necessary for risk assessment and mitigation. Particular emphasis is placed on the risks associated with malware, cyberterrorism, and data theft. For example, machine learning (ML) and cyber threat intelligence are cited here as tools for predicting and countering cyber threats (Nwankwo et al. 2024, pp. 1–3).

However, the increasing connectivity and digitization of supply chains also pose security risks. Attacks on the Internet of Things (IoT) are specifically mentioned in this context. Cyber threats in supply chain management (SCM) are multi-layered, diverse, and constantly evolving (Layode et al. 2024, pp. 1962–1963). In this area, they target vulnerabilities within the supply chain with the aim of disrupting services. These attacks can lead to the distribution of compromised products, disruptions in the supply process, and ultimately damage to a company’s reputation (Odimarha et al. 2024, p. 27).

Product Safety: Product safety is based on the premise that there can be no such thing as absolute product safety. Nevertheless, the law requires that risk be kept below the threshold risk. The threshold risk is the maximum acceptable risk. People, animals, and property must be protected from this risk. The hazards involved are classified as stochastic (random risks, such as component failure) and deterministic (predetermined hazards, such as those associated with the proper operation of a chainsaw) (Bauer 2018, p. 277).

Product safety can no longer be guaranteed due to attacks on the supply chain. Because of the interdependence and inherent complexity of the supply chain, the weakest link can cause damage to the entire supply chain. Sensitive data can be compromised, and damage can be caused (Alshammari und Mahinderjit Singh 2025, p. 67667–67668).

Compliance: In the strictest sense, compliance refers to adherence to standards, guidelines, and ethical values (Fig. 3). Some companies use a Code of Conduct (CoC) to establish internal corporate guidelines. Failure to comply with compliance regulations can have drastic consequences for the supply chain (for example, in cases of human rights violations or corruption). Moreover, due to the increased reach of the media, compliance violations are reaching more and more people (Wellbrock und Ludin 2025, p. 191–201).

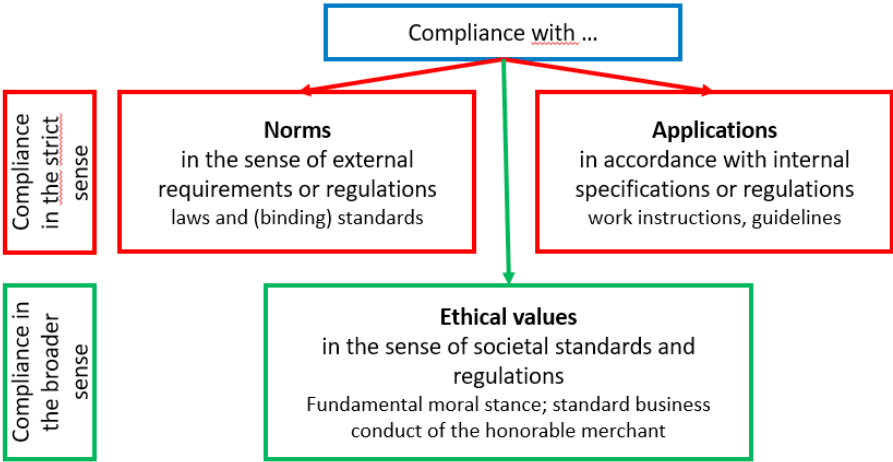


Fig. 3. Areas of Compliance (Wellbrock und Ludin 2025, p. 191)

It is emphasized that risk management must take into account unforeseeable and dynamic threats, as failure to do so could expose companies to the risk of serious operational disruptions, non-compliance with legal requirements, or a loss of customer trust. Standards serve as the foundation for compliance. For example, threat modeling is conducted using the STRIDE model (Spoofing, Tampering, Repudiation, Information Disclosure, Elevation of Privilege). This includes an adaptive and traceable system architecture that applies GS1 traceability standards. The third-party risk assessment also notes that the risk assessment of partners is likewise a part of compliance (Almohaimeed et al. 2025, p. 58–66).

Resilience: Resilience involves compensating for unforeseen disruptions or attaining a superior system state. It focuses on responding to disruptions while maintaining continuous business processes to enhance the supply chain’s competitiveness and performance. Responses can be categorized into proactive strategies (e.g., collaboration or workforce management) and reactive strategies (e.g., agility or redundant systems) (Biedermann und Kotzab 2021, pp. 9–10).

There are approaches aimed at revolutionizing resilience and security – for instance, in the power supply sector – through digital technologies. IoT-based methods can significantly enhance the resilience of interconnected microgrids. By creating a virtual replica of the physical microgrid via a digital twin (DT) that continuously receives data from IoT sensors, the system can generate real-time analyses and forecasts. These enable effective defense against cyberattacks based on proactive decision-making. ANGEL frameworks operate in a similar manner, detecting potential failures and anomalies (Achuthan et al. 2025, p. 9).

To ensure resilience, structured frameworks are crucial for addressing supply chain risks; existing guidelines and standards can be adopted and tailored to specific needs. The process begins by identifying vulnerabilities and critical resources to pinpoint critical attack vectors assessments that are regularly updated to reflect current operational environments. On this basis, continuous security measures are implemented to ensure the ongoing monitoring of cybersecurity incidents (Nwankwo et al. 2024, pp. 3–4).

Challenges in Ensuring Supply Chain Security

Companies across the board are facing complex, novel security challenges that span the entire supply chain. Globalized and increasingly complex supply chains are primary drivers of rising security risks. These risks involve a wide range of entities, including hardware and software vendors,

external service providers, internal departments, and the manufacturers themselves manifesting in everything from insider threats to counterfeit products entering the market (Roy et al. 2025, p. 185).

When risks arise across the entire supply chain model compounded by the globalization of companies' extensive value chains, the risk throughout the supply chain is multiplied. Similarly, the widespread use of IoT networks or interconnected systems creates further points of vulnerability for attacker (Latsiou und Lambrinoudakis 2026, p. 40).

In addition, the growing volume of data, the variety of data streams, and increasing speeds offer attackers additional potential (Charul und Bhatia 2026, p. 328).

Failure to consider the resulting risks can lead to significant damage. Resilient supply chains are required to withstand digital disruptions. Proactive supply chain security is essential for managing these risks. Conventional security measures are no longer sufficient today; a comprehensive perspective that takes both technical and non-technical factors into account is necessary. This entails viewing the entire supply chain ecosystem starting with the establishment of long-term relationships with partners and suppliers and extending to adherence to strict security standards at every stage, from goods receipt to final delivery (Adewusi et al. 2022, pp. 489–496).

Transparency is a crucial factor. Traceability across the entire supply chain is required. Companies are encouraged to invest in transparency using various approaches. It is also important to ensure transparency among the partners involved. Furthermore, partners and suppliers must be regularly and accurately vetted to ensure compliance with relevant security regulations in accordance with the security profile (Sreenivasulu Gajula 2025, pp. 3–8).

In addition, there is the integration of standard cybersecurity practices across all stages of the supply chain process. Sensitive data requires encryption, while intrusion detection systems are needed to monitor data traffic, and firewalls are essential to prevent unauthorized access (Roy et al. 2025, pp. 186–187).

It is particularly important to conduct regular security checks or audits to identify new vulnerabilities. In the late 20th century, manual testing could uncover complex vulnerabilities that automated tests missed. Automated security scanning tools revolutionized the detection of security vulnerabilities in the early 21st century. Modern application architectures and distributed components pushed existing approaches to their limits. Today, security mechanisms are being further developed with the aid of AI. Each new era addresses the limitations of the preceding one while simultaneously bringing new challenges (Ramachandran 2026, pp. 502–503).

Since, despite significant efforts, the possibility of security incidents cannot be entirely ruled out, companies should have emergency plans in place that cover all such scenarios. In the event of a cybersecurity breach or other incident, these plans should outline the initial steps to be taken, based on defined roles and responsibilities and identified stakeholders (Roy et al. 2025, p. 187).

Taking safety aspects into account, the aim is to examine the challenges within the supply chain when discussing the topic of safety.

CONCLUSION

The literature review aims to clarify the research question regarding the challenges associated with supply chain security. It has been shown that supply chain risks can be categorized into environmental risks, external risks, cooperation risks, and internal corporate risks. Security aspects must be taken into account to minimize these risks. These security aspects have been divided into four groups. **Physical security** addresses the product itself, considering factors such as VUCA-related challenges or product tampering. Another group focuses on **product safety**; this highlights that while product risk can never be entirely eliminated, the “limit risk” representing the maximum acceptable level of risk must not be exceeded. A further aspect concerns the scope of **compliance**, specifically the mandatory adherence to standards, directives, and ethical values throughout the entire supply chain. **Resilience** is also considered, focusing on the supply chain's ability to withstand disruptions and the necessity of proactive and reactive measures to avert potential issues. **Cybersecurity** receives significant attention in this article, particularly regarding the safeguarding of the supply chain; managing the various attack vectors is becoming increasingly difficult due to rising complexity and

data volumes. Cybersecurity measures must be effective against both intentional and unintentional disruptions. Consequently, risk strategies must be developed to minimize potential damage to the company. Transparency among all supply chain partners is essential for the early identification of disruptions. Firewalls and intrusion detection systems must employ state-of-the-art technology and be adapted to current conditions. Regular reviews of standards through audits and penetration tests are required. Since absolute security is unattainable despite the best efforts, companies must have emergency plans in place and be capable of implementing them when necessary. Ultimately, it becomes evident that while each new era resolves risks associated with the preceding one, it also introduces new challenges. For future research, it is recommended not to rely solely on a literature review but to also gain insights through, for example, semi-structured interviews with companies. Additionally, the number of articles evaluated could be increased by adjusting the time frame. The scope of cybersecurity in the context of artificial intelligence also offers further potential for investigating a new topic.

REFERENCES

- ACHUTHAN, K., GUPTA, B. B. and RAMAN, R., 2025. Bridging cybersecurity with digital twin technology: A thematic analysis. *International Journal of Information Security*. [viewed 12 June 2026].
- ADEWUSI, A. O., CHIEKEZIE, N. and EYO-UDO, N., 2022. Cybersecurity threats in agriculture supply chains: A comprehensive review. *World Journal of Advanced Research and Reviews*. [viewed 14 June 2026]. Available from: https://www.researchgate.net/profile/adebunmi-adewusi/publication/384049365_cybersecurity_threats_in_agriculture_supply_chains_a_comprehensive_review/links/67001a8df599e0392fb66b83/cybersecurity-threats-in-agriculture-supply-chains-a-comprehensive-review.pdf
- ALMOHAIMEED, M., ALBALWY, F., ALHARBI, R., ALQARNI, A. and ALJOHANI, A., 2025. *Developing a Comprehensive Cyber Risk Assessment Framework for Supply Chains: Insights into Third-Party Vulnerabilities and Security Gaps*. Available from: https://www.researchgate.net/profile/Aisha-Alqarni-3/publication/397720422_Developing_a_Comprehensive_Cyber_Risk_Assessment_Framework_for_Supply_Chains_Insights_into_Third-Party_Vulnerabilities_and_Security_Gaps/links/692f250918a6405a30fa85a5/Developing-a-Comprehensive-Cyber-Risk-Assessment-Framework-for-Supply-Chains-Insights-into-Third-Party-Vulnerabilities-and-Security-Gaps.pdf
- ALSHAMMARI, B. and MAHINDERJIT SINGH, M., 2025. A Systematic Literature Review on Tackling Cyber Threats for Cyber Logistic Chain and Conceptual Frameworks for Robust Detection Mechanisms. *IEEE Access*, vol. 13, pp. 67661–67692. DOI: <https://doi.org/10.1109/ACCESS.2025.3552689>
- ARMBRUST, M., FOX, A., GRIFFITH, R., JOSEPH, A. D., KATZ, R. H., KONWINSKI, A. et al., 2009. *Above the Clouds: A Berkeley View of Cloud Computing*. Berkeley: University of California. Available from: <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html>
- BAUER, M., 2018. *Das Recht des Technischen Produkts: Praxishandbuch für Unternehmensjuristen*. Wiesbaden: Vieweg. Available from: <https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=5488844>
- BIEDERMANN, L. and KOTZAB, H., 2021. Supply Chain Risk Management und Supply Chain Resilienz. *WIST*, vol. 50, issue 4, pp. 4–12. DOI: <https://doi.org/10.15358/0340-1650-2021-4-4>
- CHARUL, K. M. and BHATIA, M. (eds.), 2026. *A Scientometric Exploration of Threats to IoT Security Landscape*. Springer US. [viewed 14 June 2026]. Available from: <https://www.springerprofessional.de/a-scientometric-exploration-of-threats-to-iot-security-landscape/52545850>
- HAMMI, B. and EL MADHOUN, N. (eds.), 2026. *Securing the Digital Supply Chain: Advances, Challenges, and Solutions*. 1st ed. Cham: Springer Nature Switzerland.
- HUTH, M., 2025. *Resilienz in Supply Chains: Effektive Strategien und Methoden für robuste und agile Lieferketten*. Wiesbaden; Heidelberg: Springer Gabler. Available from: <https://link.springer.com/978-3-658-47009-8>
- KHOKHAR, R. H., RANKOTHGE, W., RASHIDI, L., MOHAMMADIAN, H., GHORBANI, A., FREI, B. et al., 2024. *A survey on supply chain management: Exploring physical and cyber security challenges, threats, critical applications, and innovative technologies*. Available from: <https://search.proquest.com/openview/dccaf40b0731630dcd3e86ca3995d0a1/1?pq-origsite=gscholar&cbl=2045302>
- KOTZAB, H. (ed.), 2005. *Research Methodologies in Supply Chain Management*. Heidelberg: Physica-Verlag.
- LATSIOU, A. and LAMBRINOUDAKIS, C., 2026. Cyber Supply Chain Risk Management: From Threats to Treatment. *International Journal of Information Security*, vol. 25, issue 1, Article 40. DOI: <https://doi.org/10.1007/s10207-025-01207-9>

- LAYODE, O., NAIHO, H. N. N., LABAKE, T. T., ADELEKE, G. S., UDEH, E. O. and JOHNSON, E., 2024. Addressing cybersecurity challenges in sustainable supply chain management: A review of current practices and future directions. *International Journal of Management & Entrepreneurship Research*, vol. 6, issue 6, pp. 1954–1981. Available from: https://www.researchgate.net/profile/Oluwabunmi-Layode/publication/384017002_Addressing_Cybersecurity_Challenges_in_Sustainable_Supply_Chain_Management_A_Review_of_Current_Practices_and_Future_Directions/links/66e4b3acfa5e11512cb88fed/Addressing-Cybersecurity-Challenges-in-Sustainable-Supply-Chain-Management-A-Review-of-Current-Practices-and-Future-Directions.pdf
- NWANKWO, C. O., CHIKWENDU, O. C. and IGBOKWE, N. C., 2024. Enhancing smart manufacturing supply chains through cybersecurity measures. *International Journal of Engineering Inventions*, vol. 13, issue 12, pp. 1–6.
- ODIMARHA, A. C., AYODEJI, S. A. and ABAKU, E. A., 2024. Securing the digital supply chain: Cybersecurity best practices for logistics and shipping companies. *World Journal of Advanced Science and Technology*, vol. 5, issue 1, pp. 26–30.
- RAMACHANDRAN, M., 2026. Application Security with Machine Learning. In: *Guide to AI for Cybersecurity*, pp. 499–545. DOI: https://doi.org/10.1007/978-3-032-17367-6_13
- ROY, N. R., SINGH, A., KUMAR, P. and KAUL, A. (eds.), 2025. *Cyber Security and Digital Forensics: Select Proceedings of the 2nd International Conference, ReDCySec 2024*. 1st ed. Singapore: Springer Nature Singapore.
- SARKIS, J. (ed.), 2024. *The Palgrave Handbook of Supply Chain Management*. Cham: Springer International Publishing; Palgrave Macmillan.
- GAJULA, S., 2025. Cybersecurity in Supply Chain Management: Role of Identity and Access Management, Zero Trust, and Blockchain. *Asian Journal of Computer Science Engineering*. Available from: https://www.researchgate.net/profile/sreenivasulu-gajula-2/publication/394356510_cybersecurity_in_supply_chain_management_role_of_identity_and_access_management_zero_trust_and_blockchain
- WELLBROCK, W. and LUDIN, D. (eds.), 2025. *Management von Risiko, Nachhaltigkeit und KI in der Beschaffung*. Wiesbaden: Springer Fachmedien Wiesbaden; Springer Gabler.
- WINTERGEST, R., 2025. *Cloud Report 2025: Status Quo und Trends in Wirtschaft und Politik*. Berlin: Bitkom Research. [viewed 12 June 2026]. Available from: <https://www.bitkom.org/sites/main/files/2025-06/bitkom-pressekonzferenz-cloud-report-2025-praesentation.pdf>

ИКОНОМИЧЕСКИ ПРЕДИЗВИКАТЕЛСТВА ПРЕД СИГУРНОСТТА ВЪВ ВЕРИГАТА НА ДОСТАВКИТЕ

Резюме: Сигурността във веригите на доставки е основен елемент, който позволява на процесите и участниците в тях да взаимодействат безпроблемно и без прекъсвания. При това прекъсванията могат да бъдат както умишлени, така и непреднамерени. Прекъсванията в процеса могат да доведат до значителни щети. Те могат да бъдат както финансови, така и свързани с външния имидж или правни. За да се предотврати нанасянето на щети, участниците във веригата на доставките са длъжни да предотвратяват смущенията или да ги сведат до минимум. В настоящата статия се разглеждат икономическите предизвикателства във веригата. Чрез систематично проучване на литературата се представят рисковете, последвани от аспектите на сигурността във веригата на доставките. В последващия анализ на предизвикателствата, свързани с управлението на рисковете, се обръща специално внимание на обхвата на киберсигурността. Представени са съществуващите и прилаганите мерки за защита срещу кибератаки, както и перспективи за бъдещето. Става ясно, че темата за киберсигурността е била предизвикателство в миналото и ще остане такова и в бъдеще.

Ключови думи: бизнес процеси; сигурност на веригата на доставките; предизвикателства пред киберсигурността; устойчивост на веригата на доставките

Бернд Михаел Енглер, докторант
Университет по библиотекознание и информационни технологии
София, България
E-mail: berengler@aol.com