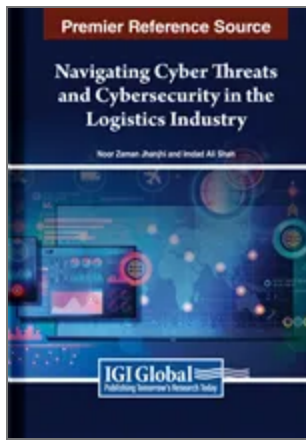


Digital Safeguards: Navigating Cyber Threats in the Logistics Industry Framework

Muhammad Tayyab, Khizar Hameed (</affiliate/khizar-hameed/464538/>), Noor Zaman Jhanjhi (</affiliate/noor-zaman-jhanjhi/415447/>), Amer Zaheer, Faizan Qamar

Source Title: Navigating Cyber Threats and Cybersecurity in the Logistics Industry (</gateway/book/337386>)

Copyright: © 2024

Pages: 42

ISBN13: 9798369338162 ISBN13 Softcover: 9798369347218 EISBN13: 9798369338179

DOI: 10.4018/979-8-3693-3816-2.ch010

Cite Chapter 

Favorite 

[View Full Text HTML >](#)

(</gateway/chapter/full-text-html/341421>)

[View Full Text PDF >](#)

(</gateway/chapter/full-text-pdf/341421>)

Abstract

The rapid integration of internet and technological advancements over the past two decades has reshaped the global landscape, leading to transformative changes in various sectors. The emergence of Industry 4.0, conceptualized in 2011, has particularly revolutionized manufacturing and logistics by advocating for systematic digitalization technology integration to enhance efficiency and reduce costs. However, this technological evolution, while fostering efficiency and process optimization, also introduces vulnerabilities to cyber threats. The logistics sector, heavily reliant on interconnected systems like internet of things, faces potential risks from cyberattacks that target sensitive data across the interconnected supply chain. This chapter aims to address the intricate relationship between digitalization and the logistics sector, emphasizing the crucial role of digital safeguards in navigating cyber dangers. Furthermore, the chapter delves into the significance of visibility in supply-chain operations and explores technologies and practices for enhancing supply-chain visibility.

Request access from your librarian to read this chapter's full text.



1. Introduction

Internet and technological advancements have been widely adopted for the past two decades, and the world has been redefined as a result of technological advancements, which have allowed for the expansion of teleconferencing, telemedicine, and telemarketing, as well as altered the nature of human interactions. An idea for the increasing digitization of industrial processes called “Industry 4.0” emerged in 2011 from a German technological innovation initiative (Kagermann, 2014). Industry 4.0, the fourth industrial revolution, posits that businesses in the manufacturing and logistics sectors can achieve better efficiency and reduced costs by systematically integrating digitalization technology into their operations. Ultimately, this integration will help the business develop and maintain its competitive edge in the long run. Numerous enabling technologies associated with Industry 4.0 have also played a role in the dramatic shift in the corporate environment (Mubarak & Petraite, 2020). A significant technology in this context is the Internet of Things (IoT), which describes networks of networked, uniquely identifying devices that may communicate with each other dynamically and intelligently (Atzori et al., 2017). It is a network design that includes hardware components, software applications, and platforms that intelligently connect and share data amongst themselves; the term “Industrial Internet of Things” (IIoT) describes its common use in industrial settings like production and supply chains (Barreto et al., 2017). It is anticipated that by the year 2027, the global expenditure on the digital transformation of the logistics industry will amount to approximately \$95 billion (Wolak et al., 2019). According to the digital industries barometer, the logistics and transport sector is positioned fifth globally out of eleven industries, with a digital transformation adoption score of 6.61 (Du et al., 2023).

Increased efficiency and process optimization are hallmarks of modern logistics, which depend highly on digital technologies and communication infrastructure (Lu et al., 2003). With the help of these innovations, online retailers can keep tabs on shipments, communicate with clients and business associates, and easily collect vital sales data (Cheung & Michael, 2021). On the other hand, growing dependence on technology makes systems more vulnerable to cyberattacks, which can negatively affect businesses and the services they provide to their customers. Cyberattacks can target sensitive data in several locations due to the interconnected nature of the logistics business (Alshurideh et al., 2023). The more connections there are in a supply chain, the more susceptible it is to attacks. Integrating systems allows for the exchange of information, and supply chains are a vital part of this complex global network. For example, fraudsters can break into a company’s network, steal sensitive information, and then demand payment to decrypt the data by using information about inventory, delivery and arrival timings, and locations (Zhang et al., 2023).

The importance of authoring this book chapter is to highlight the role of digitalisation in the logistics sector, followed by a discussion of the landscape of digital safeguards and how to navigate cyber dangers in the logistics industry. To that end, we established the following goals, which resulted in the following essential noteworthy contributions. It begins with an in-depth examination of the current cybersecurity scenario in the logistics sector. Furthermore, it offers a thorough understanding of the logistics business structure, as well as the ramifications of rising connection and technology use. Furthermore, it includes a thorough overview of digital safeguards for cybersecurity in logistics, as well as risk assessment, tactics, and communication patterns in logistics. Aside from that, this chapter discusses the importance of visibility in supply-chain operations, as well as the technology and methods for improving supply-chain visibility. This chapter also includes a full examination of incident response and recovery in logistics. Finally, toward the end, various open challenges and potential opportunities in the logistics sector are discussed.

The specific contributions of the chapter are as follows.

[Continue Reading \(/gateway/chapter/full-text-html/341421\)](/gateway/chapter/full-text-html/341421)

References

- | | |
|------------------|---|
| Follow Reference | Abhay K. (2023). Grover. Out of the frying pan and into the fire? uncovering the impact of fsma’s sanitary food transportation rule on the food logistics industry. <i>Business Horizons</i> , 66(2), 203–214. 10.1016/j.bushor.2022.06.003 |
| Follow Reference | Afenyo M. Livingstone D. (2023). Caesar. Maritime cybersecurity threats: Gaps and directions for future research. <i>Ocean and Coastal Management</i> , 236, 106493. 10.1016/j.ocecoaman.2023.106493 |

Follow Reference	Al-Banna A. Rana Z. A. Yaqot M. Menezes B. (2023). Interconnectedness between supply chain resilience, industry 4.0, and investment. <i>Logistics</i> , 7(3), 50. 10.3390/logistics7030050
Follow Reference	Ali S. M. Ashraf M. A. Hasin M. M. T. Ahmed S. (2023). Drivers for internet of things (iot) adoption in supply chains: Implications for sustainability in the post-pandemic era. <i>Computers & Industrial Engineering</i> , 183, 109515. 10.1016/j.cie.2023.109515
Follow Reference	Alqahtani F. Selviaridis K. Stevenson M. (2023). The effectiveness of performance-based contracting in the defence sector: A systematic literature review. <i>Journal of Purchasing and Supply Management</i> , 29(5), 100877. 10.1016/j.pursup.2023.100877
Follow Reference	Alshurideh M. Alquqa E. Alzoubi H. Kurdi B. Hamadneh S. (2023). The effect of information security on e-supply chain in the uae logistics and distribution industry. <i>Uncertain Supply Chain Management</i> , 11(1), 145–152. 10.5267/j.uscm.2022.11.001
Follow Reference	Atzori L. Iera A. Morabito G. (2017). Understanding the internet of things: Definition, potentials, and societal role of a fast evolving paradigm. <i>Ad Hoc Networks</i> , 56, 122–140. 10.1016/j.adhoc.2016.12.004
	Axestrack. (n.d.). <i>The 6 Major Components of Logistics Management</i> . Axestrack.
Follow Reference	Barreto L. Amaral A. Pereira T. (2017). Industry 4.0 implications in logistics: An overview. <i>Procedia Manufacturing</i> , 13, 1245–1252. 10.1016/j.promfg.2017.09.045
Follow Reference	Cheng L. T. Tei Z. Yeo S. F. Lai K.-H. Kumar A. Chung L. (2023). Nexus among blockchain visibility, supply chain integration and supply chain performance in the digital transformation era. <i>Industrial Management & Data Systems</i> , 123(1), 229–252. 10.1108/IMDS-12-2021-0784
Follow Reference	Cheung K.-F. Michael G. H. (2021). Bell, and Jyotirmoyee Bhattacharjya. Cybersecurity in logistics and supply chain management: An overview and future research directions. <i>Transportation Research Part E, Logistics and Transportation Review</i> , 146, 102217. 10.1016/j.tre.2020.102217
Follow Reference	Cichosz M. Wallenburg C. M. Michael Knemeyer A. (2020). Digital transformation at logistics service providers: Barriers, success factors and leading practices. <i>International Journal of Logistics Management</i> , 31(2), 209–238. 10.1108/IJLM-08-2019-0229
	Closs & McGarrell. (2004). <i>Enhancing security throughout the supply chain</i> . IBM Center for the Business of Government.
Follow Reference	Colicchia C. Creazza A. David A. (2019). Managing cyber and information risks in supply chains: Insights from an exploratory analysis. <i>Supply Chain Management</i> , 24(2), 215–240. 10.1108/SCM-09-2017-0289
Follow Reference	Darmayanti N. L. Dwipayana A. D. (2023). Logistics industry readiness in application policy over dimension overloading (odol). <i>ASTONJADRO</i> , 12(2), 454–460.
	Digital, C. (n.d.). <i>The Digital Transformation of Logistics: An Overview of Technologies and Trends</i> . copperdigital.medium.com (http://copperdigital.medium.com)
Follow Reference	Ding S. Lu S. Xu Y. Korkali M. Cao Y. (2023). Review of cybersecurity for integrated energy systems with integration of cyber-physical systems. <i>Energy Conversion and Economics</i> , 4(5), 334–345. 10.1049/enc2.12097



Follow Reference	Du S. Zhang H. Kong Y. (2023). Sustainability implications of the arctic shipping route for shanghai port logistics in the post-pandemic era.Sustainability (Basel), 15(22), 16017. 10.3390/su152216017
Follow Reference	Duggineni S. (2023). Data integrity and risk.Open Journal of Optimization, 12(2), 25–33. 10.4236/ojop.2023.122003
	Gihon. (n.d.). <i>The Weak Link: Recent Supply Chain Attacks Examined</i> . cy-berint.com
Follow Reference	Gregory N. (1998). Logistics, strategy and structure: A conceptual framework.International Journal of Operations & Production Management, 18(1), 37–52. 10.1108/01443579810192772
	Grima, Thalassinos, Cristea, Kadlubek, Maditinios, & Peiseniece. (2023). <i>Digital transformation, strategic resilience, cyber security and risk management</i> . Academic Press.
	Hameed, K., Haseeb, J., Tayyab, M., & Junaid, M. (2017). Secure provenance in wireless sensor networks-a survey of provenance schemes. In <i>2017 International Conference on Communication, Computing and Digital Systems (C-CODE)</i> (pp. 11–16). IEEE.
Follow Reference	Huang Q. (2023). Enhancing university logistics management through iot technology in the context of bioinformatics engineering.Journal of Commercial Biotechnology, 28(3).
Follow Reference	Iqbal H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: Current and future prospects.Annals of Data Science, 10(6), 1473–1498. 10.1007/s40745-022-00444-2
Follow Reference	Jaiswal N. Misra A. Khang A. Misra P. K. (2023). The role of internet of things technologies in business and production. In <i>AI-Aided IoT Technologies and Applications for Smart Business and Production</i> (pp. 1–13). CRC Press. 10.1201/9781003392224-1
Follow Reference	Junejo A. K. Breza M. Julie A. (2023). McCann. Threat modeling for communication security of iot-enabled digital logistics.Sensors (Basel), 23(23), 9500. 10.3390/s2323950038067872
Follow Reference	Kadrich M. (2007). Endpoint security. Addison-Wesley Professional.
Follow Reference	Kagermann H. (2014). Change through digitization—value creation in the age of industry 4.0. In <i>Management of permanent change</i> (pp. 23–45). Springer.
Follow Reference	Kalaiarasan R. Agrawal T. K. Olhager J. Wiktorsson M. Hauge J. B. (2023). Supply chain visibility for improving inbound logistics: A design science approach.International Journal of Production Research, 61(15), 5228–5243. 10.1080/00207543.2022.2099321
Follow Reference	Kalkha H. Khiat A. Bahnasse A. Ouajji H. (2023). The rising trends of smart e-commerce logistics.IEEE Access : Practical Innovations, Open Solutions, 11, 33839–33857. 10.1109/ACCESS.2023.3252566
Follow Reference	Kaur R. Gabrijelčič D. Klobučar T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions.Information Fusion, 97, 101804. 10.1016/j.inffus.2023.101804
	Key Elements of Logistics Management. (n.d.) https://www.mojro.com/resource-key-elements-of-logistics-management
Follow Reference	Liu Y. Tao X. Li X. Colombo A. Hu S. (2023). Artificial intelligence in smart logistics cyber-physical systems: State-of-the-arts and potential applications. IEEE Transactions on Industrial Cyber-Physical Systems.



Follow Reference	Lu J. Yu C.-S. Liu C. James E. (2003). Technology acceptance model for wireless internet. <i>Internet Research</i> , 13(3), 206–222. 10.1108/10662240310478222
	Malagon-Su´arez & Orjuela-Castro. (2023). Challenges and trends in logistics 4.0. <i>Ingenier´ia</i> , 28
	Martto, J., Diaz, S., Hassan, B., Mannan, S., Singh, P., Villasuso, F., & Baobaid, O. (2023). Esg strategies in the oil and gas industry from the maritime & logistics perspective opportunities & risks. In <i>Abu Dhabi International Petroleum Exhibition and Conference</i> . SPE.
Follow Reference	Meers J. Halliday S. Tomlinson J. (2023). “Creative non-compliance”: Complying with the “spirit of the law” not the “letter of the law” under the covid-19 lockdown restrictions. <i>Deviant Behavior</i> , 44(1), 93–111. 10.1080/01639625.2021.2014286
Follow Reference	Menoni S. Molinari D. Parker D. Ballio F. Tapsell S. (2012). Assessing multifaceted vulnerability and resilience in order to design risk mitigation strategies. <i>Natural Hazards</i> , 64(3), 2057–2082. 10.1007/s11069-012-0134-4
Follow Reference	Mubarak M. F. Petraite M. (2020). Industry 4.0 technologies, digital trust and technological orientation: What matters in open innovation? <i>Technological Forecasting and Social Change</i> , 161, 120332. 10.1016/j.techfore.2020.120332
Follow Reference	Panjehfouladgaran Frederick Lim . (2020). Reverse logistics risk management: identification, clustering and risk mitigation strategies. <i>Management Decision</i> , 58(7):1449–1474.
	Poyhonen, J., Simola, J., & Lehto, M. (2023). Basic elements of cyber security for a smart terminal process. In <i>The Proceedings of the... International Conference on Cyber Warfare and Security</i> . Academic Conferences International Ltd.
Follow Reference	Progoulakis, I., Nikitakos, N., Dalaklis, D., Christodoulou, A., Dalaklis, A., & Yaacob, R. (2023). Digitalization and cyber physical security aspects in maritime transportation and port infrastructure. In <i>Smart Ports and Robotic Systems: Navigating the Waves of Techno-Regulation and Governance</i> (pp. 227–248). Springer. 10.1007/978-3-031-25296-9_12
Follow Reference	Rangaraju S. (2023). Ai sentry: Reinventing cybersecurity through intelligent threat detection. <i>EPH- International Journal of Science And Engineering</i> , 9(3), 30–35. 10.53555/ephijse.v9i3.211
Follow Reference	Remko V. H. (2020). Research opportunities for a more resilient post-covid-19 supply chain–closing the gap between research findings and industry practice. <i>International Journal of Operations & Production Management</i> , 40(4), 341–355. 10.1108/IJOPM-03-2020-0165
Follow Reference	Sharma M. Luthra S. Joshi S. Kumar A. Jain A. (2023). Green logistics driven circular practices adoption in industry 4.0 era: A moderating effect of institution pressure and supply chain flexibility. <i>Journal of Cleaner Production</i> , 383, 135284. 10.1016/j.jclepro.2022.135284
Follow Reference	Shrivastava S. (2023). Recent trends in supply chain management of business-to-business firms: A review and future research directions. <i>Journal of Business and Industrial Marketing</i> , 38(12), 2673–2693. 10.1108/JBIM-02-2023-0122
Follow Reference	Suja A. (2022). Machine learning-based wearable devices for smart healthcare application with risk factor monitoring. In <i>Empowering Sustainable Industrial 4.0 Systems With Machine Intelligence</i> (pp. 174–185). IGI Global.



- Follow Reference Suman O. P. Saini L. K. Kumar S. (2023). Cloud-based data protection and secure backup solutions: A comprehensive review of ensuring business continuity. In 2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC) (pp. 821–826). IEEE. 10.1109/ICSCCC58608.2023.10176503
- Supply Chain Vulnerability: Identifying and Mitigating Risks. (n.d.). magaya.com
- Follow Reference Syed N. F. Syed W. (2022). Traceability in supply chains: A cyber security analysis. Computers & Security, 112, 102536. 10.1016/j.cose.2021.102536
- Follow Reference Taeihagh A. Hazel S. M. L. (2019). Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks. Transport Reviews, 39(1), 103–128. 10.1080/01441647.2018.1494640
- Tayyab, Marjani, Jhanjhi, Abaker, Hashem, & Usmani. (n.d.). *A watermark-based secure model for data security against security attacks for machine learning algorithms*. Academic Press.
- Tayyab M. Marjani M. (2021a). A light-weight watermarking-based framework on dataset using deep learning algorithms. In 2021 National Computing Colleges Conference (NCCC) (pp. 1–6). IEEE.
- Follow Reference Tayyab M. Marjani M. (2021b). Cryptographic based secure model on dataset for deep learning algorithms. CMC Comput. Mater. Contin, 69, 1183–1200.
- The most common entry points for a cyber attack . (n.d.). guptadeepak.com
- Wang, Li, Liu, & Zhang. (n.d.). Real-time cyber-physical security solution leveraging an integrated learning-based approach: An integrated learningbased cyber-physical security solution. *ACM Transactions on Sensor Networks*.
- Wolak, Lysionok, Kosturek, Wi'sniewski, Wawryszak, Kawa, Davidson, Ma'ckowiak, Starzyk, & Kulikowska-Wielgus. (2019). *Technological revolution. Directions in the development of the transport-forwarding-logistics (tfl) sector*. Academic Press.
- Follow Reference Zhang Q. Shi L. Sun S. (2023). Optimization of intelligent logistics system based on big data collection techniques. In The International Conference on Cyber Security Intelligence and Analytics (pp. 378–387). Springer. 10.1007/978-3-031-31860-3_40

Request Access

You do not own this content. Please login to recommend this title to your institution's librarian or purchase it from the IGI Global bookstore (/chapter/digital-safeguards/341421).

Username or email:

Password:

Log In >

Forgot individual login password? (/gateway/login/reset-password/)

Create individual account (/gateway/login/create-account/)



Research Tools

Database Search (/gateway/) | Help (/gateway/help/) | User Guide (/gateway/user-guide/) | Advisory Board (/gateway/advisory-board/)



User Resources

Librarians (/gateway/librarians/) | Researchers (/gateway/researchers/) | Authors (/gateway/authors/)

Librarian Tools

COUNTER Reports (/gateway/librarian-tools/counter-reports/) | Persistent URLs (/gateway/librarian-tools/persistent-urls/) | MARC Records (/gateway/librarian-tools/marc-records/) | Institution Holdings (/gateway/librarian-tools/institution-holdings/) | Institution Settings (/gateway/librarian-tools/institution-settings/)

Librarian Resources

Training (/gateway/librarian-corner/training/) | Title Lists (/gateway/librarian-corner/title-lists/) | Licensing and Consortium Information (/gateway/librarian-corner/licensing-and-consortium-information/) | Promotions (/gateway/librarian-corner/promotions/)

Policies

Terms and Conditions (/gateway/terms-and-conditions/)

([http://www.facebook.com/pages/IGI-](http://www.facebook.com/pages/IGI-Global/138206739534176?ref=sgm)

[Global/138206739534176?ref=sgm](http://www.facebook.com/pages/IGI-Global/138206739534176?ref=sgm))

(<http://twitter.com/igiglobal>)

(<https://www.linkedin.com/company/igiglobal>)



(<http://www.world-forgotten-children.org>)

(<https://publicationethics.org/category/publisher/igi-global>)

Copyright © 1988-2024, IGI Global - All Rights Reserved