European Research Studies Journal
Volume XXVII, Issue 3, 2024

pp. 1108-1123

Cybersecurity Threats and Practices in the Logistics Industry in Poland

Submitted 10/09/24, 1st revision 25/09/24, 2nd revision 01/10/24, accepted 15/12/24

Andrzej Szymonik[1], Artur Szymonik[2], Małgorzata Dymyt[3],
Marta Wincewicz-Bosy[4]

Abstract:

Purpose: *The purpose of this research was to evaluate and recommend security tools and protocols that enhance data protection and operational resilience. This paper examines the cybersecurity challenges facing logistics systems, particularly focusing on the risks associated with technologies such as the Internet of Things (IoT), cloud computing, and artificial intelligence (AI).*
Design/Methodology/Approach: *Research paper based on conclusions formulated on the basis of a review and analysis of scientific literature, sectoral documents and research conducted in 2023-2024 through comprehensive surveys and analysis.*
Findings: *Findings indicate that enhancing cybersecurity in logistics requires standardized approaches, including mandatory two-factor authentication, automated data backups, and robust encryption protocols. These measures are essential to minimize operational disruptions and protect sensitive information within the logistics sector.*
Practical implications: *This study addresses both theoretical and practical gaps in cybersecurity within the logistics industry in Poland, where limited research and resources have been dedicated to addressing these new vulnerabilities. The identified gaps highlight the need for model cybersecurity solutions tailored to Polish logistics and empirical research on current cybersecurity practices.*
Originality/Value: *This research contributes to the existing literature by highlighting the critical need for a proactive approach to cybersecurity in modern supply chains.*

Keywords: *Security, cybersecurity, threats, information systems, logistics.*

JEL codes: *O32, O33, M15.*

Paper type: *Research article.*

[1] *Lodz University of Technology, Poland, e-mail: dgw_szymonik@op.pl;*
[2] *General Tadeusz Kościuszko Military University of Land Forces, Poland, e-mail: artur.szymonik@awl.edu.pl;*
[3] *General Tadeusz Kościuszko Military University of Land Forces, Poland, e-mail: malgorzata.dymyt@awl.edu.pl;*
[4] *General Tadeusz Kościuszko Military University of Land Forces, Poland, e-mail: marta.wincewicz-bosy@awl.edu.pl;*

1. Introduction

Modern logistics, as part of Industry 4.0, is increasingly linked to frameworks like Logistics 4.0, Smart Logistics, and Smart Supply Chains (Strandhagen *et al.,* 2017; Lee *et al.*, 2016; Frank *et al.*, 2019). These frameworks rely heavily on advanced digital technologies, establishing interconnected systems that facilitate seamless communication between people, machines, and logistics networks (Winkelhaus and Grosse, 2020). However, as logistics systems integrate new technologies such as the Internet of Things (IoT), Cyber-Physical Systems (CPS), Unmanned Aerial Vehicles (UAVs), Artificial Intelligence (AI), blockchain, cloud computing, and 5G networks, they are increasingly susceptible to cyber threats.

Each technology poses unique cybersecurity challenges. For instance, IoT and Industrial IoT, using RFID and wireless sensor networks, enhance inventory management, warehousing, and vehicle tracking but increase the risk of unauthorized access and data breaches (Gowri, 2023).

CPS enables coordinated control between cybernetic and physical systems, yet opens potential entry points for attackers targeting logistics processes (Tan *et al.*, 2008). UAVs have advanced order fulfilment and customer service, yet remain vulnerable to cyber hijacking and other security risks (Rejeb *et al.*, 2021; Wang, Christen and Hunt, 2021; Coindreau, Gallay, and Zufferey, 2021; Agatz, Bouman, and Schmidt, 2018). Similarly, AI enhances logistics operations through analytics and database processing but also presents risks related to data exploitation and system manipulation (Chung, 2021; Toorajipour *et al.*, 2021; Min, 2010).

Blockchain technology, while secure and transparent, can be exploited if inadequately protected. As a decentralized data structure, blockchain enables direct, intermediary-free transactions across private, public, or hybrid clouds, but it is still susceptible to data interception (Rejeb *et al.,* 2021; Bode and Wagner, 2015; Treiblmaier, 2019; Tehrani and Gupta, 2021; Hald and Kinra, 2019; Kuhi, Kaare, and Koppel, 2018).

Cloud computing, a critical enabler of scalable data storage, is also vulnerable if not adequately secured (Szymonik and Stanisławski, 2023; Enache, 2023; Gomez, Grand, and Grivis, 2015). Finally, 5G technology, a high-speed data transmission standard, supports efficient logistics communication but also increases exposure to data theft and unauthorized network access (Ignar, 2019; Lagorio *et al.*, 2023).

While these digital technologies are transformative for logistics, their integration introduces cyber vulnerabilities that, if exploited, can disrupt supply chains, leading to data loss, compromised goods, financial losses, and reputational damage (Crosignani, Macchiavelli, and Silva, 2023). Effective security of information systems is essential for mitigating these risks and ensuring continuity in logistics operations.

This study addresses both theoretical and practical gaps in cybersecurity within the logistics industry in Poland, where limited research and resources have been dedicated to addressing these new vulnerabilities. The identified gaps highlight the need for model cybersecurity solutions tailored to Polish logistics and empirical research on current cybersecurity practices. This study aims to evaluate and recommend security tools and protocols that enhance data protection and operational resilience, based on research conducted in 2023-2024 through comprehensive surveys and analysis.

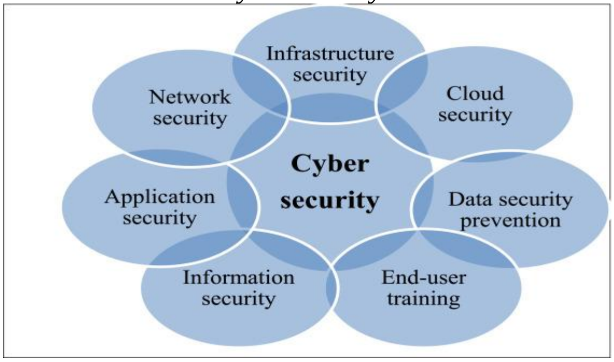
2. The Essence of Cybersecurity

Cybersecurity, evolving since the latter half of the 20th century, encompasses a range of practices and theories aimed at protecting information systems from various threats. Though definitions vary, common descriptions include:

(1) cybersecurity as the resilience of systems against breaches of confidentiality, integrity, and availability (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560);
(2) a suite of processes, best practices, and technologies protecting critical networks from digital attacks (Co to jest cyberbezpieczeństwo?, 2023);
(3) a set of defences spanning password management to advanced machine-learning-based tools that ensure safe access to digital resources (Co to jest cyberbezpieczeństwo?, 2023).

From these definitions, key cybersecurity functions include protecting information, networks, and data against unauthorized access, maintaining data integrity, and ensuring that only authorized personnel have access (Jamal *et al.*, 2021). Cybersecurity encompasses a wide array of measures, often organized into areas such as standards, technical security, IoT and cloud security, and personnel training (Figure 1) (Security bez tabu, 2022).

Figure 1. *Selected areas related to cybersecurity*



Source: *Own study on the basis: Li, Y., Liu Q. 2021, A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, ELSEVIER, Energy Reports 7, 8176–8188.*

Key frameworks include:

- standards and structures: ISO 27001, which governs information security management; ISO 27017, providing guidelines for secure cloud service use; and ISO 27018, which protects personal data in cloud services;
- technical security - clear physical security measures for devices to restrict access to authorized personnel;
- IoT security - requires secure systems for device communication, physical device security, authorization processes, and an integrated IoT security management system (Jurcut, Ranaweera, and Xu, 2020);
- cloud security - procedures and technologies that protect cloud environments from cyber threats (Singh and Chatterjee, 2017);
- application security - practices for embedding security features into software to deter various threats;
- endpoint security - protects network-connected devices, such as computers and mobile devices, from external threats (Kubera, 2023);
- data protection and access management - Data Loss Prevention (DLP) software safeguards sensitive information, while access management limits system access to authorized users only;
- database security - secures both the data within databases and the systems managing them from misuse, intrusion, or data damage;
- employee training - cybersecurity education for personnel is critical to maintaining secure systems and awareness of current threats.

3. Types of Threats to Information Systems in Logistics

Cyber threats in logistics encompass a wide range of malicious activities aimed at disrupting, damaging, or infiltrating information systems. Cyberattacks are typically defined as actions intended to infiltrate or disrupt computer networks, whether of corporations or governments, with identifiable targets, perpetrators, and intentions (Motsch *et al.,* 2020; Cao *et al.,* 2019). These attacks can vary from network breaches that appear benign while sending false responses (Quigley *et al.,* 2015) to offensive operations capable of causing physical or financial harm via botnets, malware, or traffic generation systems (Bullock *et al.*, 2021).

Cybersecurity threats can originate from diverse sources, including corporate spies, hacktivists, terrorists, hostile states, and disgruntled employees (7 Types of Cyber Security Threats, 2023). Many of these actions are classified as criminal under cybersecurity laws and include data breaches, unauthorized data acquisition, sabotage, piracy, and espionage (Bezpieczeństwo systemów komputerowych - wykład 1, 2023).

As digital technology in logistics advances, the variety of cyber threats expands, especially with the rise of mobile devices, IoT, cloud computing, and big data. Core cyber threats in this sector include (Baig, 2023; Types of Cyber Threat in 2023, 2023; Top 6 Cybersecurity Threats, 2023; Rosencrance, 2023):

- malicious software: ransomware (RaaS), Trojans, and spyware that perform harmful actions on user systems;
- social engineering attacks - techniques like phishing, spear phishing, smishing, and vishing aimed at deceiving users;
- web application exploits - including SQL Injection (SQLI), remote code execution (RCE), and cross-site scripting (XSS) (Różańska, 2023);
- supply chain attacks - exploiting third-party software or hardware vulnerabilities, including key loggers (Ohm *et al.*, 2020);
- denial of service (DoS) attacks - includes distributed DDoS, where multiple devices flood networks, and ransom-related DoS attacks (RDoS), where attackers demand payment to cease disruptions;
- man-in-the-middle (MitM) attacks - a hacker intercepts data between two parties without detection, using techniques like IP spoofing, DNS spoofing, and Wi-Fi eavesdropping (Różańska, 2023; Dajana, 2023).

The rapid digitization in logistics has amplified the frequency and severity of these threats, particularly as secure supply chain continuity becomes essential. Key objectives for cybersecurity include maintaining data privacy, accessibility, and integrity, which are critical in mitigating the potential impact of cyber incidents. A well-implemented data protection strategy minimizes the risk of data loss, theft, or damage in the event of a breach.

Ultimately, while technical measures are crucial, common sense remains a vital defence against cyber threats, reinforcing security efforts across digital and logistical infrastructures.

4. Examples of Solutions Protecting IT Systems in Logistics

Traditional logistics communications relied on phone calls, faxes, and printed documents, but with digitalization, information exchange now primarily occurs via email, API interfaces, and software applications. While this shift has optimized supply chain operations, it has also introduced significant vulnerabilities to cyber threats. These digital connections expose logistics systems to hacking, risking the loss of sensitive information such as inventory data, shipment schedules, and operational details relevant to air, land, and sea transport (Ajagbe, Awotunde, Opadotun, and Adigun, 2023).

Implementing robust cybersecurity measures involves a structured approach to identify and protect critical IT resources, assess potential threats, and evaluate associated risks and costs. Key steps include:

- Identifying Resources: Determining what assets—such as computer hardware, data, and backups -require protection.
- Recognizing Threats: Assessing risks from sources like viruses, software vulnerabilities, human error, theft, or environmental factors.
- Evaluating Risks: Assessing potential losses and the likelihood of attacks, followed by a cost-benefit analysis of security investments.

Effective information security also requires understanding Threat Intelligence, categorizing threats into internal and external. Internal threats arise from within the organization and include both intentional and accidental actions, such as employees collaborating with external entities to cause harm, mishandling sensitive data, or abusing system access for personal gain. External threats encompass cyberattacks initiated outside the organization, posing significant risks to data integrity and security (Cybersecurity in the Logistics Industry, 2023). Notable vulnerabilities in logistics IT security include:

- *Applications with Hardcoded Credentials:* Many commercial off-the-shelf (COTS) systems in logistics include permanently encoded authentication, which can lead to unauthorized remote access (Harvard Business Review, 2021).
- *Shared Accounts:* As logistics increasingly adopts COTS/IoT technologies, shared accounts are expected to become common, complicating user tracking and accountability.
- *Remote Work:* Remote access, often unsecured, is particularly vulnerable to ransomware attacks, with prolonged access sessions posing higher security risks.

Neglecting IT infrastructure security in the logistics sector can cause serious, often irreversible consequences, such as system data loss, theft, and misuse, potentially leading to financial penalties for the organization. Table 1 outlines essential procedures for managing information system security, focusing on availability, reliability, confidentiality, and accessibility to safeguard operational continuity and data integrity.

Table 1. *Selected tools used in managing the security of an information system*

No.	**Content**	**Applies to/Method of implementation**
1	Strong password	Actions: Use a strong password, containing at least 12 to 14 characters; Use a separate password for your work and personal email account; Never disclose your passwords to anyone; Frequently change passwords (preferably at least every 90 days); Asing 3 random words is a good way to create a strong, unique password that you will remember; Do not use words that can be guessed (such as a child's name or pet's name); Include numbers and symbols.
2	Central	A way to protect critical data and valuable company resources. In a situation

	password management	where there are accounts in the organization that have administrative access to all content and the rights of other users, it is very important to monitor their behaviour. This is served by Privileged Access Management (PAM), i.e., a privileged password manager. Thanks to this solution, people monitoring the behaviour of so-called privileged accounts can efficiently detect the abuse of privileges and actions to the detriment of the company.
3	Two-factor authentication (often shortened to 2FA)	Two-Factor Authentication (2FA) is a method used by online services to enhance user protection. A person logging into the service using 2FA must confirm their identity in not one, but two ways.
4	Backup	Create backups of your personal data on a separate disk, not directly on the computer or in a secure cloud storage with 2FA authentication enabled.
5	Antivirus programs	A barrier protecting the user from the operation of malicious software. It is a computer program whose main task is to detect, remove, or combat so-called computer viruses, i.e., unwanted computer programs that, to operate, use, among others, the operating system and various types of applications. Currently, antivirus software is part of a package that also protects the computer from other threats.
6	emails	Actions: always thoroughly check your emails and avoid opening unwanted attachments; are aware of social engineering: scammers collect personal data from the Internet and use it to impersonate friends or authorities; do not click on links blindly; if you click an unwanted link that takes you to a login page, do not log in (remember, if it sounds too good to be true, it probably is).
7	IoT sensors and devices	The increasing use of sensors and Internet of Things (IoT) devices currently used in logistics companies is a potential target for cybercriminals, who can intercept connections between sensors and the IT system in order to collect data and offer it to the competition.
8	Encrypted drives	Data encryption on a disk means encrypting the entire hard drive on a computer. This means that everything on it will be encoded - every folder, every file, and every bite of data. Everything that is visible and everything that is not visible. Disk data encryption even hides metadata, such as sizes, names, file creation dates, and directory structures.
9	Safe browsers	A browser, handling a large amount of sensitive personal data, should secure privacy and safety. A good browser should not collect data about the viewed pages or pass them on to third parties. It should also not expose us to malicious and annoying ads, or other types of threats. There are various safe browsers available on the market, which include: Microsoft Edge, Opera, Chrome, Brave, Chromium, and others.
10	Only legal software	This is software that we purchase with an appropriate license and an activation key from the manufacturer. Legal software in a company is associated with many benefits. Among them, it is worth highlighting: a sense of security, help from manufacturers, certainty of trouble-free installation, the possibility of using discounts on the purchase of subsequent products, protection against viruses, protection against hacker attacks.

11	Physical security	The area includes: • he proper location for computers and server rooms (appropriate walls, ceilings, windows, doors, locks, keys, alarms, fire protection, good air conditioning, lighting); • he use of intelligent systems, e.g., Smart Keeper type, which offers the highest level of security through physical protection of input/output ports, such as USB ports, network ports, or access ports of internal devices; • n effective Faraday cage.
12	Firewall	A Firewall, literally translated as a fire wall, is also commonly referred to as a network or fire barrier. It is a type of network security that continuously filters network traffic, blocking connections that may pose a potential threat and risk. The firewall allows for precise filtering of access at the level of the local network (LAN), home, and individual computers. It is a basic security measure for network devices against scanning and establishing unwanted connections by third parties.
13	Emergency power supply	Devices or a system of devices used to protect selected receivers from power supply disturbances from the power grid, which could result in disruption or interruption of their operation.
14	Shredder for confidential documents	These are shredders equipped with cutting blades made using special technology and complex in design, allowing for the destruction of documents at the highest levels of secrecy - Level 6 and 7 according to DIN 66399. The degree of secrecy in these classes is determined by the dimension of the cut surface or its boundary dimensions.
15	Staff training	The training includes an introduction to the subject of cybersecurity, basic concepts and principles, legal aspects, and practical elements. The subject matter covers issues: information technology, the Internet, methods of operation of cybercriminals (including elements of psychology, social engineering, and manipulation), and ways to protect against cyberattacks. The training includes a practical part, during which scenarios of attacks and phishing campaigns are presented. Participants analyse cyber risks and prepare a response plan for incidents with the trainer. The training does not require technological knowledge, anyone can participate in it.

Source: *Own study based on: Mii J., 8 easy cybersecurity tips to protect your logistics data, Available at: https://geodis-com.translate.goog/pl/en/blog/technology-automation/8-easy-cybersecurity-tips-protect-your-logistics-data?_x_tr_sl=enand_x_tr_tl=pland_x_tr_hl=pland_x_tr_pto=sc; Nord VPN, Available at: https://nordvpn.com/pl/blog/uwierzytelnianie-dwuskladnikowe/; Encyklopedia zarządzania, Available at: https://mfiles.pl/pl/index.php/Program_antywirusowy; It Solution, Available at: https://itsf.com.pl/pojecia-itsf/centralne-zarzadzanie-haslami; Jablonka M., Co to jest szyfrowanie danych i kiedy warto je stosować?, Available at: https://bitdefender.pl/co-to-jest-szyfrowanie-danych-i-kiedy-warto-je-stosowac; Różańska J., Top 13 najbezpieczniejszych przeglądarek dbających o Twoją prywatność w 2023, Available at: https://nordvpn.com/pl/blog/bezpieczne-przegladarki-2023/. Szkolenia z zakresu cyberbezpieczeństwa, Available at: https://kicb.pl/nasza-oferta/szkolenia-z-cyberbezpieczenstwa.*

In practice, there are many tools that allow for continuous improvement of processes securing computer systems against hackers. One of them is the OODA method (Observe-Orient-Decide-Act). The components of this method are (Figure 2) (Baever, 2023, Lewandowski, 2023).

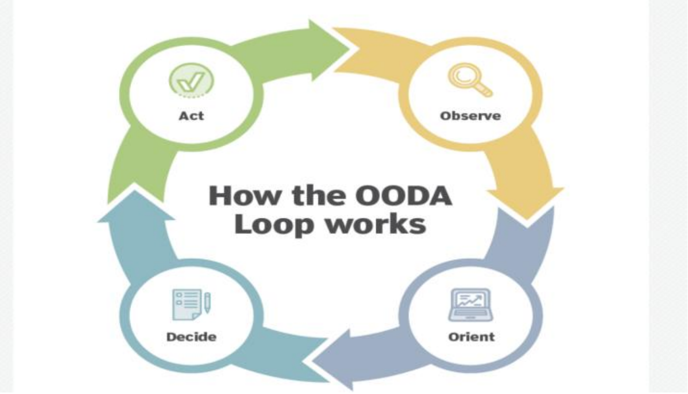
Observation involves the collection of data (resources) related to network traffic, applications, and tools that ensure security. An important link is also the ability to monitor in real time what happens before, during, and after a security breach event.

Orientation is a detailed, systematic analysis of the collected resources, confronting them with reality and filtering them so that they are useful for assessing potential threats and the effects of attacks carried out. Such actions facilitate effective decision-making in the next step.

Decision is an action resulting from a choice, based on the information gathered. At this stage, critical business decisions are made, including what should be done and what should not be done, in terms of response actions in the context of computer system security. Decision-makers can refer to security policies, standards, agreements, and compliance requirements to ensure that their actions will bring the intended effect. The end result is the development of a clear and understandable remedial action plan. Depending on the situation, decision-makers may be forced to reuse incident response solutions and related security tools.

Action - these are conscious steps (undertakings) that need to be taken to remedy threats and minimize risk using incident response instruments by applying appropriate security tools. Helpful instruments can be: anti-malware software, backup and recovery, collection and securing of forensic evidence, SOAR tools, training to increase security awareness.

Figure 2. *Components of the OODA system*



Source: *Authors study based on: Beaver K., Top incident response tools: How to choose and use tchem, https://www.techtarget.com/searchsecurity/feature/Incident-response-tools-How-when-and-why-to-use-them.*

It should be emphasized that on the one hand, computerization provides the opportunity to be better than others, including competition and to achieve greater profits. On the other hand, however, it poses a great threat, if only because of the possibility of losing access to data or making them available to unauthorized persons, as well as financial losses. In order to ensure the security of the IT infrastructure in logistics operations, professional support is necessary. Currently, IT outsourcing, a service offered by IT companies specializing in providing IT solutions for business, is increasingly chosen by entrepreneurs (Mageto, 2022).

5. Protection Against Attacks – Own Research

The research initiated with a thorough literature review to identify key gaps and issues in the field of cybersecurity within Poland's logistics sector. This review revealed a critical underestimation of cybersecurity's importance in Poland, demonstrated by the limited number of publications and studies on the subject. Based on these findings, two main research gaps were identified.

The first gap is theoretical, highlighting the lack of standardized cybersecurity models suited for Polish logistics companies. The second gap is practical, underscoring the need for empirical research assessing cybersecurity practices within the logistics sector, specifically regarding the evaluation and effectiveness of existing security measures.

To address these gaps, the study was conducted in 2023–2024 and aimed to evaluate cybersecurity tools and practices that effectively protect information systems in Polish logistics companies. The research utilized a survey with a customized questionnaire and engaged 173 randomly selected companies. Data collection methods included CAWI (Computer-Assisted Web Interviewing), in-person sessions, and individual interviews.

The adoption of digital technologies, such as the Internet of Things (IoT), cloud computing, artificial intelligence, and blockchain, has enhanced operational efficiency in logistics. However, it also exposes the sector to cyber threats. Survey results indicate that:

- 27% of companies do not use strong passwords or are uncertain of their strength, significantly increasing the risk of unauthorized account access;
- 52% of companies lack or do not regularly create data backups, exposing their data to irretrievable loss in case of an attack;
- 18% of respondents indicated they either do not use or are unsure about the use of antivirus software, which lowers their protection level against malware threats.

The survey, reveals gaps in security awareness and practices, particularly in password management, data backups, and encryption:

- about 42% of respondents do not regularly change passwords, increasing the risk of credential theft;
- only 98 companies (57%) report regularly updating their passwords;
- 83 companies (48%) do not regularly back up their data, indicating inadequate security protocols, which could lead to significant losses in the event of a cyberattack;

Survey responses highlight specific risk areas and domains that require strengthening:

- lack of password management policies: although 126 companies (73%) claim to use strong passwords, only half of them change passwords regularly; this is a significant risk, as static passwords are vulnerable to brute-force attacks or data breaches;
- lack of systematic data backups: 48% of companies admit to not regularly creating backups; implementing automated backups could substantially mitigate data loss risks;
- low encryption adoption: only 78 respondents (45%) use encryption, leaving critical data unprotected; this poses a serious risk, especially for sensitive information, such as customer data and operational details.

6. Discussion

The survey results indicate a concerning gap between awareness of cybersecurity practices and their actual implementation in the logistics sector. While companies recognize the importance of foundational measures like strong passwords and antivirus software, there is inconsistent application in critical areas such as data backups, encryption, and regular password updates. These gaps can be attributed to various factors, including limited budgets, lack of dedicated cybersecurity staff, and inadequate employee training programs.

Moreover, the logistics industry’s reliance on interconnected systems and third-party vendors increases its exposure to complex supply chain attacks, making it vital for companies to establish comprehensive cybersecurity frameworks. Despite many companies adopting two-factor authentication (2FA) and basic antivirus protection, the low prevalence of encryption and automated backups suggests that data integrity and continuity planning are not yet adequately prioritized.

These findings point to the need for a cultural shift within the industry, where cybersecurity is viewed as an essential investment rather than an operational expense. Companies that strengthen their cybersecurity protocols, especially in areas identified as vulnerable, are likely to experience improved resilience against cyber threats, securing not only their data but also their reputation and customer trust in an increasingly digital logistics environment.

7. Conclusions

Based on the survey findings and analysis, the following recommendations can significantly improve cybersecurity standards in the logistics sector:

- Mandatory cybersecurity training: regular training on cyber threats and defensive techniques should be implemented across all companies; such training could reduce the risk of phishing attacks, which is critical given the high percentage of companies reporting low employee awareness of cyber risks;
- Increased Use of Two-Factor Authentication (2FA): 140 companies (81%) already use 2FA, a positive indicator; however, the remaining companies should implement this technology to restrict unauthorized access;
- Automating Data Backups: introducing automated backups could address the issue faced by 83 companies (48%) that lack regular data backups, thereby significantly improving data security;
- Mandatory data encryption: to secure sensitive data, companies should implement mandatory encryption; valuable data, such as customer information, should always be stored in encrypted form.

The survey analysis highlights a generally insufficient level of cybersecurity practices implemented in many logistics companies. While there is some awareness of threats and basic protections, such as strong passwords and antivirus software, there are notable gaps in regular backups, encryption, and password management. Implementing the recommended measures could significantly reduce risk and enhance system resilience against cyber threats, ultimately elevating security standards in the digital landscape of logistics.

In conclusion, it should be stated that the research results allowed the formulation of a number of practical conclusions and recommendations, which constitute the basis for further research on this current and important problem. Despite the limitations, the analyses carried out in the article have shown that the issue of cybersecurity in logistics systems is particularly important and, due to its developmental nature, requires further in-depth research in the interdisciplinary area.

References:

7 Types of Cyber Security Threats. Available at: https://onlinedegrees-und-edu.translate.goog/blog/types-of-cyber-security-threats/?_x_tr_sl=enand_x_tr_tl=pland_x_tr_hl=pland_x_tr_pto=sc.

Agatz, N., Bouman, M., Schmidt, M. 2018. Optimization Approaches for the Traveling Salesman Problem with Drone. Transportation Science, 52(4).

Ajagbe, S.A., Awotunde, J.B., Opadotun, A.T., Adigun, M.O. 2023. Cybersecurity in the Supply Chain and Logistics Industry: A Concept-Centric Review. In: Advances in:

Mishra, A., Gupta, D., Chetty, G. (Eds.). IoT and Security with Computational Intelligence. ICAISA 2023. Lecture Notes in Networks and Systems, vol. 755, Singapore: Springer.

Baig, A. 7 Biggest Cybersecurity Threats of the 21st Century. Available at: https://cybersecurity-att-com.translate.goog/blogs/security-essentials/7-biggest-cybersecurity-threats-of-the-21st-century?_x_tr_sl=enand_x_tr_tl=pland_x_tr_hl=pland_x_tr_pto=sc.

Beaver, K. 2023. Top Incident Response Tools: How to Choose and Use Them. Available at: https://www.techtarget.com/searchsecurity/feature/Incident-response-tools-How-when-and-why-to-use-them.

Bezpieczeństwo systemów komputerowych - wykład 1: Wprowadzenie do problematyki bezpieczeństwa systemów komputerowych. Available at: https://wazniak.mimuw.edu.pl/index.php?title=Bezpiecze%C5%84stwo_system%C3%B3w_komputerowych_-_wyk%C5%82ad_1:Wprowadzenie_do_problematyki_bezpiecze%C5%84stwa_system%C3%B3w_komputerowych.

Bode, C., Wagner, S.M. 2015. Structural Drivers of Upstream Supply Chain Complexity and the Frequency of Supply Chain Disruptions. Journal of Operations Management, 36, 215-228.

Bullock, J.A., Haddow, G.D., Capola, D.P. 2021. Cybersecurity and Critical Infrastructure Protection. In: Introduction to Homeland Security: Principles of All-Hazards Risk Management, 6th ed., Elsevier, pp. 425-497.

Cao, Y., Huang, Z., Ke, C., Xie, J., Wang, J. A. 2019. Topology-Aware Access Control Model for Collaborative Cyber-Physical Spaces: Specification and Verification. Computers and Security, 87, 101478.

Chung, S.H. 2021. Applications of Smart Technologies in Logistics and Transport: A Review. Transportation Research Part E: Logistics and Transportation Review, 153, 102455.

Co to jest bezpieczeństwo aplikacji? - definicja z Techopedia. Available at: https://pl.theastrologypage.com/application-security.

Co to jest cyberbezpieczeństwo. Available at: https://www.microsoft.com/pl-pl/security/business/security-101/what-is-cybersecurity.

Co to jest cyberbezpieczeństwo? Available at: https://nordvpn.com/pl/cybersecurity.

Coindreau, M.C., Gallay, O., Zufferey, N. 2021. Parcel Delivery Cost Minimization with Time Window Constraints Using Trucks and Drones. Networks: An International Journal 78 (4)**.**

Crosignani, M., Macchiavelli, M., Silva, A.F. 2023. Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chain. Journal of Financial Economics, 147(2), 432-448.

Cybersecurity in the Logistics Industry. Available at: https://krontech-com.translate.goog/cybersecurity-in-the-logistics-industry?_x_tr_sl=enand_x_tr_tl=pland_x_tr_hl=pland_x_tr_pto=sc.

Dajana. Atak Man-in-the-Middle. Available at: https://www.omegasoft.pl/blog/atak-man-in-the-middle/.

Enache, G.L. 2023. Logistics Security in the Era of Big Data, Cloud Computing and IoT. Proceedings in Business and Economics, 17(1), 188-199.

Encyklopedia zarządzania, Available at: https://mfiles.pl/pl/index.php/Program_antywirusowy.

Frank, A.G., Dalenogare, L.S., Ayala, N.F. 2019. Industry 4.0 Technologies: Implementation Patterns in Manufacturing Companies. International Journal of Production Economics, 210, 15-26.

Gomez, M., Grand, A., Grivis, S. 2015. Digitalisation in Logistics and the Role of Cloud Computing. FHNW.

Gowri, Ms.K. 2023. Impact of the Internet of Things (IoT) on Logistics. Journal of Image Processing and Intelligent Remote Sensing, 3(1).

Hald, K.S., Kinra, A. 2019, How the Blockchain Enables and Constrains Supply Chain Performance. International Journal of Physical Distribution and Logistics Management, 49(4), 376-397.

Harvard Business Review. 2021. Bringing Blockchain, IoT, and Analytics to Supply Chains. Available at: https://hbr.org/2021/12/bringing-blockchain-iot-and-analytics-to-supply-chains.

Ignar, M. Technologia 5G - czym jest? Available at: https://www.komputronik.pl/informacje/co-to-jest-5g-zalety-i-zagrozenia-sieci-5g.

It Solution, Available at: https://itsf.com.pl/pojecia-itsf/centralne-zarzadzanie-haslami.

Jablonka, M. 2020. Co to jest szyfrowanie danych i kiedy warto je stosować? Available at: https://bitdefender.pl/co-to-jest-szyfrowanie-danych-i-kiedy-warto-je-stosowac.

Jamal, A.A., Majid, A.A.M., Konev, A., Kosachenko, T., Shelupanov, A. 2021. A Review on Security Analysis of Cyber Physical Systems Using Machine Learning. Materials Today: Proceedings, 2302-2306.

Jurcut, A.D., Ranaweera, P., Xu, L. 2020. Introduction to IoT Security. In: IoT Security: Advances in Authentication, Springer, pp. 27-64.

Kubera, G. 2020. Ochrona punktów końcowych - co trzeba o niej wiedzieć. Available at: https://www.computerworld.pl/news/Ochrona-punktow-koncowych-co-trzeba-o-niej-wiedziec,411609.html.

Kuhi, K., Kaare, K., Koppel, O. 2018. Ensuring Performance Measurement Integrity in Logistics Using Blockchain. In: Proceedings of the 2018 IEEE International Conference on Service Operations and Logistics, and Informatics, Singapore, 31 July–2 August, pp. 256-261.

Lagorio, A., Cimini, C., Pinto, R., Cavalieri, S. 2022. 5G in Logistics 4.0: Potential Applications and Challenges. ScienceDirect, 4th International Conference on Industry 4.0 and Smart Manufacturing, Upper Austria University of Applied Sciences, Hagenberg Campus, Linz, Austria, 2-4 November.

Lee, S., Kang, Y., Prabhu, V.V. 2016. Smart Logistics: Distributed Control of Green Crowdsourced Parcel Services. International Journal of Production Research, 54(23), 6956-6968.

Lewandowski, P. Pętla OODA. Available at: https://nimbless.pl/blog/ooda-loop.

Li, Y., Liu, Q. A. 2021. Comprehensive Review Study of Cyber-Attacks and Cyber Security: Emerging Trends and Recent Developments. Energy Reports, 7, 8176-8188.

Mageto, J. 2022. Current and Future Trends of Information Technology and Sustainability in Logistics Outsourcing. Sustainability, 14(13), 7641.

Mii, J. 2020. 8 easy cybersecurity tips to protect your logistics data, Available at: https://geodis-com.translate.goog/pl/en/blog/technology-automation/8-easy-cybersecurity-tips-protect-your-logistics-data?_x_tr_sl=enand_x_tr_tl=pland_x_tr_hl=pland_x_tr_pto=sc.

Min, H. 2010. Artificial Intelligence in Supply Chain Management: Theory and Applications. International Journal of Logistics Research and Applications, 13(1), 13-39.

Motsch, W., Alexander, D.A., Sivalingam, K., Wagner, A., Ruskowski, M. 2020. Approach for Dynamic Price-Based Demand Side Management in Cyber-Physical Production Systems. Procedia Manufacturing, 51, 1748-1754.

Nord VPN, Available at: https://nordvpn.com/pl/blog/uwierzytelnianie-dwuskladnikowe/.

Ohm, M., Plate, H., Sykosch, A., Meier, M. 2020. Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks. In Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2020, Maurice, C., Bilge, L., Stringhini, G., Neves, N., Eds., Lecture Notes in Computer Science, vol. 12223, Springer, Cham.

Quigley, K., Burns, C., Stallard, K. 2015. Cyber Gurus: A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection. Government Information Quarterly, 32(2), 108-117.

Ray, T. 2020. Database Security. Available at: https://www.imperva.com/learn/data-security/database-security/.

Rejeb, A., Rejeb, K., Simske, S., Treiblmaier, H. 2021. Blockchain Technologies in Logistics and Supply Chain Management: A Bibliometric Review. Logistics, 5(4).

Rejeb, A., Rejeb, K., Simske, S.J., Treiblmaier, H. 2021. Drones for Supply Chain Management and Logistics: A Review and Research Agenda. International Journal of Logistics Research and Applications, 708-731.

Rosencrance, L. 2020. Top 10 Types of Information Security Threats for IT Teams. Available at: https://www-techtarget-com.translate.goog/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams?_x_tr_sl=enand_x_tr_tl=pland_x_tr_hl=pland_x_tr_pto=sc.

Różańska, J. 2023. Top 13 najbezpieczniejszych przeglądarek dbających o Twoją prywatność w 2023, Available at: https://nordvpn.com/pl/blog/bezpieczne-przegladarki-2023/.

Różańska, J. 2020. Cross-site Scripting - Czym jest i jak się przed nim chronić? Available at: https://nordvpn.com/pl/blog/xss-atak/.

Security bez tabu. 2022. Co się składa na Cybersecurity? Available at: https://securitybeztabu.pl/co-sie-sklada-na-cybersecurity/#Z_czego_sklada_sie_cyberbezpieczenstwonbsp.

Singh, A., Chatterjee, K. 2017. Cloud Security Issues and Challenges: A Survey. Journal of Network and Computer Applications, 79, 88-115.

Strandhagen, J.O., Vallandingham, L.R., Fragapane, G., Strandhagen, J.W., Stangeland, A.B.H., Sharma, N. 2017. Logistics 4.0 and Emerging Sustainable Business Models. Advances in Manufacturing, 5(4), 359-369.

Szkolenia z zakresu cyberbezpieczeństwa, Available at: https://kicb.pl/nasza-oferta/szkolenia-z-cyberbezpieczenstwa.

Szymonik, A., Stanisławski, R. 2023. Supply Chain Security: How to Support Safety and Reduce Risk in Your Supply Chain Process, Routledge/Taylor and Francis Group: New York, NY, USA.

Tan, Y., Goddard, S., Pérez, L.C. 2008. A Prototype Architecture for Cyber-Physical Systems. ACM SIGBED Review, 5, Article No. 26.

Tehrani, M., Gupta, S.M. 2021. Designing a Sustainable Green Closed-Loop Supply Chain under Uncertainty and Various Capacity Levels. Logistics, 5(2), 20.

Toorajipour, R., Sohrabpour, V., Nazarpour, A., Oghazi, P., Fischl, M. 2021. Artificial Intelligence in Supply Chain Management: A Systematic Literature Review. Journal of Business Research, 122, 502-517.

Top 6 Cybersecurity Threats. Available at: https://www-checkpoint-com.translate.goog/cyber-hub/cyber-security/what-is-cybersecurity/top-6-cybersecurity-threats/?_x_tr_sl=enand_x_tr_tl=pland_x_tr_hl=pland_x_tr_pto=sc.

Treiblmaier, H. 2019. Blockchain Technology and the Physical Internet to Achieve Triple Bottom Line Sustainability: A Comprehensive Research Agenda for Modern Logistics and Supply Chain Management. Logistics 2019, 3(1).

Types of Cyber Threat in 2023. Available at: https://www-itgovernance-co-uk.translate.goog/cyber-threats?_x_tr_sl=enand_x_tr_tl=pland_x_tr_hl=pland_x_tr_pto=sc.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018, poz. 1560).

Wang, N., Christen, M., Hunt, M. 2021. Ethical Considerations Associated with “Humanitarian Drones”: A Scoping Literature Review. Science and Engineering Ethics.

Winkelhaus, S., Grosse, E.H. 2020. Logistics 4.0: A Systematic Review towards a New Logistics System. International Journal of Production Research, 58(1), 18-43.