6. Singh, S. K. (2018). Driver Behavior and Accident Research: A Human Factors Perspective. CRC Press.
7. Thomas, F. D., Blomberg, R. D., & Knodler, M. A. (2020). Evaluation of the Safe and Sober Campaign: A National Initiative to Reduce Impaired Driving. National Highway Traffic Safety Administration.
8. Transportation Research Board. (2020). Tire Safety: A Review of Regulatory and Enforcement Strategies. National Academies of Sciences, Engineering, and Medicine.
9. World Health Organization (WHO). (2023). Global Status Report on Road Safety 2023. World Health Organization.

SECURITY ISSUES IN LOGISTICS ENTERPRISES AND WAREHOUSES AND METHODS FOR THEIR SOLUTION

A. Reznyk, student

T.V. Gerasymchuk, PhD, Associate Professor

Kharkiv National Automobile and Highway University

Introduction The global logistics and warehousing sector forms the backbone of international trade and commerce, with an estimated market value exceeding $10 trillion annually. This complex network, while essential for economic growth, faces increasingly sophisticated security challenges that threaten supply chain integrity, corporate profitability, and consumer safety. From multinational corporations to small-scale distributors, security breaches can result in catastrophic financial losses, reputational damage, and operational disruptions. This comprehensive analysis examines the multifaceted security challenges confronting logistics enterprises and warehouses while proposing innovative, technology-driven solutions to address these vulnerabilities.

Critical Security Challenges Cargo Theft and Pilferage

Cargo theft represents one of the most persistent and costly security issues, with global losses estimated at $50 billion annually. Modern criminals employ increasingly sophisticated methods, including identity theft, cyber-enabled tracking, and insider collaboration. High-value electronics, pharmaceuticals, and luxury goods remain primary targets, with thefts often occurring during transit or through coordinated attacks on warehouse facilities. The problem is particularly acute in regions with

inadequate law enforcement and along major transportation corridors where cargo remains vulnerable during loading and unloading operations.

Cybersecurity Vulnerabilities The digital transformation of logistics operations has introduced unprecedented cybersecurity risks. Warehouse Management Systems (WMS), Transportation Management Systems (TMS), and Internet of Things (IoT) devices present attractive targets for cybercriminals. Recent incidents include ransomware attacks paralyzing distribution centers, data breaches exposing sensitive customer information, and manipulation of inventory systems causing widespread operational chaos. The interconnected nature of modern supply chains means a single vulnerability can compromise multiple organizations simultaneously.

Internal Threats and Employee-Related Risks Internal security breaches constitute approximately 45% of all logistics security incidents according to industry surveys. These range from petty theft by individual employees to sophisticated collusion networks involving multiple staff members and external criminals. Common issues include inventory shrinkage, data theft, credential sharing, and deliberate sabotage. The transient nature of warehouse employment and high staff turnover rates in many regions exacerbate these challenges, making comprehensive background checks and continuous monitoring difficult to implement effectively.

Physical Security Gaps Despite technological advancements, basic physical security remains a significant concern. Many warehouses operate with inadequate access control systems, insufficient lighting, and poorly maintained perimeter security. Common vulnerabilities include malfunctioning surveillance equipment, unsecured loading docks, and inadequate alarm systems. These physical security gaps create opportunities for unauthorized access, property damage, and organized theft operations.

Regulatory Compliance and Documentation Fraud The complex regulatory environment governing international logistics creates additional security challenges. Documentation fraud, including counterfeit bills of lading, manipulated customs declarations, and forged certificates of origin, enables cargo diversion and smuggling operations. Compliance with varying international security standards, such as the

Authorized Economic Operator (AEO) program and ISO 28000, presents ongoing challenges for multinational logistics providers.

Advanced Solutions and Implementation Strategies Integrated Technological Security Systems Modern logistics security requires a layered technological approach combining multiple systems:

- Artificial Intelligence and Machine Learning: AI-powered surveillance systems can analyze video feeds in real-time, identifying suspicious behavior patterns and potential security threats. Machine learning algorithms can predict high-risk periods for theft based on historical data and current operational parameters.

- Blockchain Technology: Implementing blockchain for documentation and transaction verification creates immutable records, significantly reducing opportunities for fraud and documentation manipulation.

- Internet of Things (IoT) Security: Advanced sensor networks and smart tracking devices provide real-time monitoring of cargo conditions and location. These systems can automatically trigger alerts for unauthorized access, environmental changes, or route deviations.

Comprehensive Personnel Management Addressing internal security threats requires a holistic approach to personnel management:

- Behavioral Analytics: Implementing systems that monitor for unusual behavioral patterns among employees can help identify potential security risks before incidents occur.

- Structured Incentive Programs: Developing security-focused reward systems and clear reporting mechanisms encourages employee participation in security maintenance.

- Continuous Training Programs: Regular, mandatory security training that evolves to address emerging threats ensures staff remain vigilant and informed about security protocols.

Physical Security Enhancements Modern physical security measures must integrate traditional and innovative approaches:

- Biometric Access Control: Implementing fingerprint, facial recognition, or iris scanning systems for restricted areas significantly reduces unauthorized access.

- Automated Perimeter Security: Advanced fence-mounted sensors, thermal imaging cameras, and drone surveillance provide comprehensive perimeter monitoring.

- Smart Lighting Systems: Intelligent, motion-activated lighting systems combined with video surveillance enhance security while reducing energy costs.

Cybersecurity Implementation Protecting digital assets requires a multi-layered cybersecurity strategy:

- Regular Security Audits: Comprehensive vulnerability assessments and penetration testing should be conducted quarterly to identify and address potential weaknesses.

- Employee Cybersecurity Training: Continuous education programs focusing on phishing awareness, password security, and social engineering prevention are essential.

- Encrypted Communication Channels: Implementing end-to-end encryption for all digital communications and data storage protects sensitive information from interception.

Implementation Framework and Best Practices

Risk Assessment and Customization Each logistics enterprise must begin with a comprehensive risk assessment tailored to its specific operations, geographic location, and cargo types. This assessment should identify critical vulnerabilities and prioritize security investments based on potential impact and likelihood. Regular reassessments ensure the security framework adapts to evolving threats and operational changes.

Phased Implementation Approach Successful security enhancement typically follows a structured implementation timeline:

1. Immediate Actions (0-3 months): Address critical vulnerabilities, implement basic access controls, and establish emergency response protocols.

2. Short-term Improvements (3-12 months): Deploy surveillance systems, enhance employee training, and implement inventory tracking solutions.

3. Long-term Strategy (12+ months): Integrate advanced technologies, develop predictive analytics capabilities, and establish industry partnerships for information sharing.

Cost-Benefit Analysis and ROI Considerations While security implementations require significant investment, the return on investment becomes evident through:

- Reduced inventory shrinkage and theft losses
- Lower insurance premiums through demonstrated security improvements
- Enhanced customer trust and competitive advantage
- Avoided costs associated with operational disruptions and reputational damage

Conclusion The security challenges facing logistics enterprises and warehouses are complex and continually evolving. However, by implementing a comprehensive, technology-driven security framework that addresses both physical and digital vulnerabilities, organizations can significantly enhance their security posture. The most successful approaches combine advanced technological solutions with robust personnel management and continuous process improvement. As the logistics industry continues to digitalize and globalize, proactive security management will become increasingly crucial for maintaining operational efficiency, protecting assets, and ensuring business continuity. The implementation of these security measures represents not merely a cost center but a strategic investment in sustainable business operations and long-term profitability.

References

1. Boyes, H. (2015). Cybersecurity and cyber-resilience in supply chains. IET Engineering & Technology Reference.

2. Chopra, S., & Sodhi, M. S. (2014). Managing risk to avoid supply-chain breakdown. MIT Sloan Management Review, 56(1), 53-61.

3. Christopher, M., & Peck, H. (2004). Building the resilient supply chain. International Journal of Logistics Management, 15(2), 1-14.

4. Durocher, D. B. (2023). Effective warehouse security: Protecting your assets in the digital age. National Safety Council Press.

5. FreightWatch International. (2023). Global supply chain intelligence report: Logistics security trends. FreightWatch International.

6. Garcia, M. L. (2021). The design and evaluation of physical protection systems (3rd ed.). Butterworth-Heinemann.

7. Hollinger, R. C., & Davis, J. L. (2022). National Retail Security Survey: Current trends in inventory shrinkage and employee theft. University of Florida.
8. International Organization for Standardization. (2023). ISO 28000:2022 - Security management systems for the supply chain. ISO.
9. Kshetri, N. (2018). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 42(11), 901-915.
10. Manuj, I., & Mentzer, J. T. (2022). Global supply chain risk management strategies. International Journal of Physical Distribution & Logistics Management, 52(3), 234-260.
11. Peck, H. (2023). Drivers of supply chain vulnerability: An integrated framework. International Journal of Physical Distribution & Logistics Management, 53(2), 145-167.
12. Purpura, P. P. (2021). Security and loss prevention: An introduction (7th ed.). Butterworth-Heinemann.
13. Rice, J. B., & Caniato, F. (2023). Building a secure and resilient supply chain. Supply Chain Management Review, 27(1), 22-29.
14. Sheffi, Y. (2022). The resilient enterprise: Overcoming vulnerability for competitive advantage. MIT Press.
15. Trend Micro Research. (2023). Securing the supply chain: Cybersecurity in logistics operations. Trend Micro Incorporated.
16. Transported Asset Protection Association. (2023). Global cargo theft threat assessment. TAPA EMEA.
17. Williams, B. D., Roh, J., & Tokar, T. (2022). Emerging technologies in logistics security: AI, IoT and blockchain applications. Journal of Business Logistics, 43(4), 515-538.
18. World Customs Organization. (2023). SAFE Framework of Standards to secure and facilitate global trade. WCO.

HISTORY OF LAND TRANSPORTATION IN UKRAINE AND KHARKIV

M. Myroshnychenko, student

T.V. Gerasymchuk, PhD, Associate Professor

Kharkiv National Automobile and Highway University

The history of land transportation in Ukraine and Kharkiv reflects the evolution of transportation methods that significantly influenced industrial development, urban infrastructure, and public life. Situated at the crossroads of Europe and Asia, Ukraine's transport history mirrors its geopolitical significance, with Kharkiv emerging as a crucial hub in both imperial and Soviet eras.

Early History: From Carts to Railroads Until the late 19th century, horse-drawn transport—including various types of carts, carriages, and wagons—served as the