Supply Chain Manager of the Future." International Journal of Logistics Management, 16(2), pp. 178-191.
7. McKinsey & Company. (2022). Supply Chain Resilience: How Are Companies Performing? New York: McKinsey & Company.
8. Veen, A., Barratt, T. and Goods, C. (2020). "Platform-Capital's 'App-etite' for Control: A Labour Process Analysis of Food-Delivery Work in Australia." Work, Employment and Society, 34(3), pp. 388-406.

SECURITY ISSUES IN LOGISTICS: ESSENTIAL INSIGHTS AND PROTECTION STRATEGIES

N. Dvornik, student,

T. Gerasymchuk, Ph.D, Associate professor,

Kharkiv National Automobile and Highway University

Logistics security is a battlefield with invisible front lines. Every day, billions of dollars in goods traverse global supply chains, passing through warehouses, ports, border crossings, and neighborhoods. At each node and along every link, vulnerabilities exist—vulnerabilities that criminal enterprises, cyber attackers, and even insider threats are increasingly sophisticated at exploiting. Security in logistics is not a single problem with a single solution; it is a multidimensional challenge encompassing physical protection, cybersecurity, personnel integrity, and supply chain resilience.

The consequences of security failure are severe. Beyond the immediate financial loss of stolen cargo, breaches disrupt operations, damage customer trust, expose companies to regulatory penalties, and in the worst cases, threaten human life. According to the Transported Asset Protection Association, cargo theft in the Europe, Middle East, and Africa region alone generated losses exceeding €172 million in 2022, with food and beverage, electronics, and pharmaceuticals among the most targeted categories (TAPA EMEA, 2023). Yet theft is only one dimension of a far broader threat landscape. This article examines the critical security issues facing logistics operations and outlines strategies that leading organizations deploy to protect their people, assets, and supply chains.

Cargo Theft: The Persistent Physical Threat Cargo theft remains the most visible and costly security challenge in logistics. Theft tactics have evolved far beyond

opportunistic pilferage. Organized criminal networks now employ strategic, intelligence-driven methods, including fictitious pickups—where fraudsters pose as legitimate carriers to collect loads—and cyber-enabled theft, where shipment data is intercepted to identify high-value targets.

The Federal Bureau of Investigation estimates that cargo theft costs U.S. businesses between $15 billion and $30 billion annually, though precise figures are elusive due to underreporting (FBI, 2023). High-value, easily resold commodities such as pharmaceuticals, electronics, apparel, and food products are disproportionately targeted. Theft hotspots concentrate around major logistics hubs, truck stops, and unsecured parking areas, particularly along key freight corridors.

Effective countermeasures begin with layered physical security: GPS tracking with geofencing alerts, covert tracking devices hidden within high-value shipments, high-security locks and trailer seals, and secure, well-lit parking facilities. However, technology alone is insufficient. A study by Ekwall and Lantz (2016) demonstrated that supply chain security investments must be matched with robust processes and personnel training to yield measurable reductions in theft losses. Driver awareness training, verification protocols for carrier identity, and established procedures for reporting suspicious activity are essential components of a comprehensive anti-theft strategy.

Cybersecurity: The Expanding Digital Attack Surface As logistics digitizes, cyber risk escalates. Transportation management systems, warehouse management systems, telematics platforms, and Internet of Things (IoT) sensors create an interconnected digital ecosystem that adversaries can exploit. Ransomware attacks on logistics providers have disrupted operations for days, freezing shipment processing and exposing sensitive customer data. NotPetya's crippling of Maersk in 2017, which forced the complete reinstallation of 4,000 servers and 45,000 PCs, remains the industry's most notorious cautionary tale—a cyberattack that cost the shipping giant an estimated $300 million in lost revenue (Greenberg, 2018).

Phishing campaigns targeting logistics employees seek credentials to penetrate corporate networks. Supply chain cyberattacks, where adversaries compromise a trusted vendor's software to reach a primary target, represent an escalating threat vector.

The National Institute of Standards and Technology recommends a defense-in-depth approach: network segmentation, multi-factor authentication, regular vulnerability assessments, incident response planning, and employee cybersecurity awareness training (NIST, 2018). For logistics companies, cyber resilience also means ensuring operational continuity—having offline backup systems and manual fallback procedures when digital infrastructure is compromised.

Insider Threats: The Enemy Within Insider threats are among the most difficult security challenges to address because they exploit legitimate access. Disgruntled employees may sabotage operations or steal cargo; financially pressured workers may collude with external criminals; negligent staff may inadvertently expose sensitive shipment data or leave facilities unsecured.

Effective mitigation begins with rigorous hiring practices, including background checks and employment verification. However, insider threat programs must extend beyond screening. The Centre for the Protection of National Infrastructure advocates a continuous monitoring approach that combines technical controls—such as access logs and anomaly detection systems—with management practices that foster a positive workplace culture and provide channels for reporting concerns (CPNI, 2021). When employees feel valued and understand the importance of security, they become the strongest defense against insider risk rather than its weakest link.

Supply Chain Integrity: Counterfeit, Contraband, and Tampering The integrity of goods flowing through logistics networks faces threats beyond outright theft. Counterfeit products infiltrate legitimate supply chains, particularly in pharmaceuticals, automotive parts, and luxury goods. Contraband smuggling exploits logistics channels, with criminal organizations hiding narcotics, weapons, or illicit wildlife products within legitimate freight. Product tampering—whether motivated by malice or extortion—poses risks to consumer safety and brand reputation.

Blockchain technology is emerging as a powerful tool for supply chain integrity, creating immutable, transparent records of custody and provenance. Research by Kshetri (2018) on blockchain applications in supply chain management highlights its potential to reduce counterfeiting and enhance traceability, though widespread adoption

faces interoperability and data quality challenges. Other protective strategies include tamper-evident packaging, chain-of-custody documentation, and supplier auditing programs that extend security requirements to upstream partners.

Facility and Infrastructure Security Warehouses, distribution centers, and freight terminals are high-value targets requiring comprehensive physical security. Perimeter fencing, access control systems, CCTV with video analytics, and 24/7 monitoring are foundational. The International Organization for Standardization's ISO 28000 series provides a framework for security management systems in the supply chain, encompassing facility security assessments, threat evaluation, and continuous improvement processes (ISO, 2022).

Critical infrastructure—ports, airports, and intermodal hubs—faces additional threats, including terrorism and sabotage. The International Ship and Port Facility Security Code, implemented under the International Maritime Organization, mandates security assessments and plans for port facilities handling international traffic. Compliance with these frameworks is not merely a regulatory obligation but a competitive necessity, as shippers increasingly require evidence of security protocols from their logistics partners.

The Human Element: Security Culture and Training Technology and procedures are essential but insufficient. Security is ultimately a human endeavor. The most advanced intrusion detection system is worthless if an employee props open a secure door for convenience. The most sophisticated cargo tracking platform cannot prevent a driver from being deceived at a fraudulent pickup if the driver has not been trained to verify credentials.

Building a security culture requires sustained leadership commitment. Employees at all levels must understand not only security protocols but the reasons behind them. Regular training, realistic drills, and clear communication about threats and incidents foster vigilance without fear. Post-incident analysis that focuses on systemic improvement rather than individual blame encourages reporting of security concerns that might otherwise go unvoiced.

Research on organizational security culture by Williams et al. (2019) found that

organizations with strong security cultures experience fewer and less severe security incidents, lower staff turnover, and greater stakeholder trust—outcomes that translate directly to competitive advantage.

Conclusion: Security as a Value Driver Security in logistics has historically been viewed as a cost burden—an insurance policy paid grudgingly. This perspective is obsolete. In an interconnected, digitalized, and threat-rich environment, security is a strategic enabler. Organizations that demonstrate robust security practices win contracts from risk-conscious shippers. They avoid the operational disruption, reputational damage, and regulatory penalties that follow security breaches. They attract and retain the trust of employees, customers, and insurers.

Protection is not achieved through any single technology or policy but through a holistic approach that integrates physical security, cybersecurity, personnel integrity, and supply chain resilience into a unified framework. The logistics industry moves the world's goods; securing them is not an optional extra but a fundamental obligation. Those who recognize this will not only protect their operations but differentiate themselves in an increasingly security-conscious marketplace.

References

1. Centre for the Protection of National Infrastructure. (2021). Insider Threat Assessment: Developing a Holistic Approach. London: CPNI.
2. Ekwall, D. and Lantz, B. (2016). "Supply Chain Security: The Role of Technology in Reducing Cargo Theft." Journal of Transportation Security, 9(1), pp. 1-18.
3. Federal Bureau of Investigation. (2023). Cargo Theft: A Billion-Dollar Problem. Washington, DC: FBI Criminal Investigative Division.
4. Greenberg, A. (2018). "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." WIRED, 22 August.
5. International Organization for Standardization. (2022). ISO 28000:2022 – Security and Resilience — Security Management Systems — Requirements. Geneva: ISO.
6. Kshetri, N. (2018). "Blockchain's Roles in Meeting Key Supply Chain Management Objectives." International Journal of Information Management, 39, pp. 80-89.
7. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: NIST.
8. Transported Asset Protection Association EMEA. (2023). TAPA EMEA Incident Information Service: Annual Report 2022. Hoofddorp: TAPA EMEA.

9. Williams, L., Botha, A. and Thatcher, A. (2019). "Assessing the Security Culture of an Organization." Information & Computer Security, 27(4), pp. 509-528.

OUTBOUND LOGISTICS: THE FINAL FRONTIER OF CUSTOMER SATISFACTION

A. Kholod, student,

Voronova Ye.M, Associate professor,

Kharkiv National Automobile and Highway University

Outbound logistics is where the supply chain meets the customer. It encompasses every process required to move finished goods from a company's warehouse or production facility to the end consumer—order processing, picking and packing, transportation, and final delivery. While inbound logistics focuses on bringing raw materials in, outbound logistics focuses on getting finished products out, and its execution directly shapes customer experience, brand perception, and revenue realization.

In an era of Amazon Prime expectations, same-day delivery, and real-time package tracking, outbound logistics has been elevated from a back-office cost center to a competitive battleground. A supply chain can manufacture flawlessly and manage inventory brilliantly, but if the outbound leg fails—if the order arrives late, damaged, or incomplete—the customer's verdict is unforgiving. Research by PwC found that 59% of consumers will abandon a brand after several bad experiences, and 17% will leave after just one (PwC, 2022). Outbound logistics is not merely about moving boxes; it is about keeping promises.

The Components of Outbound Logistics Outbound logistics is a chain of interdependent activities, each with its own performance requirements and failure points.

Order Processing: The Starting Gun The outbound journey begins when a customer places an order. Order processing encompasses order capture, validation, credit checks, and transmission to the warehouse management system. Speed and accuracy at this stage determine everything that follows. Manual order entry, still prevalent in B2B environments, introduces errors that propagate downstream—wrong