MIDI 2025 Conference

Beyond Firewalls: Building Cyber Resilience for Logistics Operations in Cognitive Cities

Abstract

With the growing reliance of cognitive cities on digital systems for logistics management, it is crucial to address potential vulnerabilities that can lead to severe financial and operational consequences.

This research investigates the cybersecurity risks in the logistics sector, focusing on the threats that endanger operations and supply chains. The study begins by identifying key cyber risks, including ransomware, data breaches, phishing, and third-party vulnerabilities. These risks have been analyzed in-depth to understand their impact on the logistics industry, as well as their likelihood of occurrence. Following the analysis, a prioritization of these threats was carried out based on their potential damage to operations and the urgency with which they need to be addressed. This research also explores the various methods used to mitigate and manage these risks. This includes the adoption of robust cybersecurity policies, enhanced authentication systems, and employee awareness programs. Additionally, it stresses the importance of regularly updating security systems and conducting thorough risk assessments to stay ahead of emerging cyber threats. The findings underscore the necessity for logistics companies to not only invest in cybersecurity technologies but also to foster a culture of security within the organization. The recommendations provided are designed to guide businesses in developing a comprehensive cybersecurity strategy that ensures both operational efficiency and data protection. Finally, the research concludes with a call to action for logistics firms to take immediate steps toward strengthening their cybersecurity infrastructure to safeguard their operations and maintain customer trust in an increasingly digital world.