IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46ISM/2025/4622825/
Vol. 2025 (29), Article ID 4622825

Cyber Hygiene and Security Training in the Transport Sector under the NIS2 Directive: A Cross-Sectoral Perspective*

Rafał WACHNIK

WSB University, Dąbrowa Górnicza, Poland

Correspondence should be addressed to: Rafał WACHNIK, rwachnik@wsb.edu.pl

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

Abstract

The increasing digitalisation of the transport sector exposes organisations to growing cybersecurity threats. The NIS2 Directive establishes a set of cybersecurity risk management measures for essential and important entities, including the requirement to implement basic cyber hygiene practices and security training for personnel. This paper examines criterion 7 of Article 21 of the Directive, focusing on its application across different modes of transport, including rail, aviation, maritime, and road. By analysing regulatory guidance, sectoral reports, and academic studies, the paper highlights both common challenges and sector-specific approaches to human-centric cybersecurity. The findings demonstrate that cyber hygiene and training are fundamental to building cyber resilience, particularly in sectors where operational continuity is directly linked to safety.

Keywords: NIS2 Directive; Cyber hygiene; Security training; Transport sector;

Introduction

The digital transformation of the transport sector has created new opportunities for efficiency, interoperability, and innovation, while simultaneously exposing essential services to increased cyber risks. Cyber incidents in transport can affect not only data confidentiality but also operational safety, continuity of services, and public trust. According to the European Union Agency for Cybersecurity (ENISA), ransomware, phishing, and supply chain attacks have emerged as dominant threats across the transport ecosystem, frequently exploiting weaknesses in human behaviour and organisational procedures (ENISA, 2023).

The NIS2 Directive, formally Directive (EU) 2022/2555, sets out a harmonized framework for cybersecurity across the Union. Article 21 requires essential and important entities to implement ten categories of risk management measures. Among them, criterion 7 – basic cyber hygiene practices and security training – addresses the human factor, which is often considered the weakest link in cybersecurity management (European Union, 2022). Despite its significance, scholarly literature on transport cybersecurity has so far prioritized technical safeguards, incident handling, and supply chain security, leaving cyber hygiene and training relatively underexplored (Ruohonen, 2024).

This paper aims to fill this gap by providing a cross-sectoral analysis of criterion 7 in transport. It explores how cyber hygiene and training are understood in the regulatory framework, how they are implemented in different modes of transport, and what challenges and good practices can be identified. The analysis contributes to ongoing discussions on the operationalization of NIS2 requirements, offering insights for both policymakers and transport operators.

Cite this Article as: Rafał WACHNIK, Vol. 2025 (29) “Cyber Hygiene and Security Training in the Transport Sector under the NIS2 Directive: A Cross-Sectoral Perspective" Communications of International Proceedings, Vol. 2025 (29), Article ID 4622825, https://doi.org/10.5171/2025.4622825

Literature Review

The NIS2 Directive establishes a harmonised legal framework for cybersecurity risk management across the European Union. Article 21 specifies ten categories of organisational and technical measures, among which criterion 7 – basic cyber hygiene practices and security training – directly addresses the human factor (European Union, 2022). Cyber hygiene refers to routine practices such as secure configuration, software updates, patch management, password policies, and access control. Security training includes structured awareness programmes, continuous education, and exercises aimed at reducing the likelihood of human error or social engineering attacks.

The European Commission adopted Implementing Regulation (EU) 2024/2690 to provide more detailed requirements, while ENISA issued the Technical Implementation Guidance on Cybersecurity Risk Management Measures to support entities in operationalising these obligations (ENISA, 2025). This guidance links cyber hygiene and training to evidence types and key performance indicators that can be audited by supervisory authorities.

ENISA's Transport Threat Landscape highlights the urgency of addressing criterion 7. Based on incidents reported between January 2021 and October 2022, ransomware accounted for 38% of incidents in transport, while data breaches accounted for 30%. Phishing and supply chain attacks each represented approximately 10% of incidents, demonstrating that human-related vulnerabilities are consistently exploited (ENISA, 2023). These findings suggest that without systematic training and cyber hygiene practices, transport operators remain highly exposed to common attack vectors.

Sectoral regulations reinforce the importance of human-centric measures. In the maritime domain, the International Maritime Organization (IMO) published its revised Guidelines on Maritime Cyber Risk Management in 2022 and 2025, emphasising the integration of training and awareness into the International Safety Management (ISM) framework (IMO, 2022; IMO, 2025). In aviation, the European Union Aviation Safety Agency (EASA) has integrated cybersecurity awareness and competence into its regulatory framework for safety management systems, recognising the interdependence of safety and cybersecurity (EASA, 2024). For road transport, UNECE Regulation No. 155 mandates that vehicle manufacturers implement cybersecurity management systems, including training and competence-building throughout the supply chain (UNECE, 2021).

The academic literature provides additional insights. Ruohonen (2024) conducted a systematic review of NIS2 research and noted a gap in empirical studies focusing on cyber hygiene and awareness training, especially in critical infrastructure sectors. In maritime transport, studies on training programmes such as the Maritime Cybersecurity Awareness (MarCy) framework demonstrated measurable improvements in crew competence when modular, scenario-based learning was applied (Oruc et al., 2024). In aviation, recent research identified training and human awareness as among the most cost-effective risk mitigation measures, highlighting their leverage effect on overall cybersecurity resilience (Mizrak & Akkartal, 2024). A systematic review of cybersecurity training methods further supports the effectiveness of phishing simulations, interactive learning, and periodic refreshers in changing user behaviour across sectors (Prümmer et al., 2024).

Taken together, regulatory frameworks and empirical studies converge on the recognition that cyber hygiene and training are essential components of cybersecurity resilience in transport. However, the literature also reveals a lack of comprehensive cross-sector analyses, with most studies addressing individual modes of transport in isolation. This paper therefore aims to bridge this gap by examining criterion 7 from a cross-modal perspective.

Research Assumptions and Objectives

The primary objective of this research is to investigate the implementation of criterion 7 of the NIS2 Directive—basic cyber hygiene practices and security training—within the European transport sector. The study seeks to provide a comparative understanding of how different modes of transport (rail, aviation, maritime, and road) approach this requirement, highlighting both commonalities and sector-specific challenges.

Three main research questions guide the analysis:

1. **How is criterion 7 of NIS2 operationalised across different transport subsectors?**

   This question addresses the extent to which regulatory obligations are translated into concrete organisational measures, focusing on cyber hygiene policies and training programmes.

2. **What are the similarities and differences in implementation between rail, aviation, maritime, and road transport?**

   The aim is to identify cross-sector patterns, while acknowledging the technical, organisational, and cultural specificities of each mode of transport.

3. **Which practices can be considered most effective in enhancing cybersecurity resilience, and how can they be harmonised across transport modes?**

   By evaluating existing approaches, the research seeks to formulate recommendations for improving sectoral practices and achieving a higher level of consistency in the application of NIS2.

The study is based on two key assumptions. First, it assumes that **the human factor remains the most critical vulnerability** in transport cybersecurity, and that cyber hygiene and training are among the most cost-effective countermeasures. This is supported by prior studies and sectoral reports indicating that phishing, weak credentials, and poor patch management are leading causes of incidents (ENISA, 2023; Prümmer et al., 2024). Second, it assumes that **embedding cyber hygiene and training into existing governance systems**—such as Safety Management Systems (SMS), Information Security Management Systems (ISMS), or Business Continuity Management Systems (BCMS)—is a prerequisite for sustainability and measurable improvement.

By addressing these objectives and assumptions, the paper aims to contribute to the growing body of knowledge on NIS2 implementation and to provide policy-relevant insights for regulators, operators, and industry associations in the European transport ecosystem.

Methodology

This study adopts a qualitative and comparative research design to analyse the implementation of criterion 7 of the NIS2 Directive—basic cyber hygiene practices and security training—across different modes of transport. The methodological approach is based on three pillars: regulatory analysis, literature review, and cross-sectoral comparison.

First, a **regulatory analysis** was conducted to interpret criterion 7 within the broader framework of Article 21 of NIS2. The analysis relied on Directive (EU) 2022/2555 (European Union, 2022), Implementing Regulation (EU) 2024/2690, and ENISA's *Technical Implementation Guidance on Cybersecurity Risk Management Measures* (ENISA, 2025). In addition, sector-specific international regulations were considered, including IMO cyber risk management guidelines (IMO, 2022; IMO, 2025), EASA regulations on aviation cybersecurity (EASA, 2024), and UNECE Regulation No. 155 on road vehicle cybersecurity management systems (UNECE, 2021).

Second, a **systematic literature review** was applied to identify existing research on cyber hygiene and training in the transport sector. Sources included peer-reviewed academic journals, conference proceedings, and institutional reports. Searches were conducted in databases such as Scopus, Web of Science, and SpringerLink, with keywords combining "NIS2", "cyber hygiene", "cybersecurity training", and "transport". The review integrated studies addressing maritime training programmes (Oruc et al., 2024), systematic evaluations of cybersecurity education methods (Prümmer et al., 2024), and transport-sector specific analyses in aviation and rail (Mizrak & Akkartal, 2024; Ruohonen, 2024).

Third, a **cross-sectoral comparison** was undertaken. Each mode of transport—rail, aviation, maritime, and road—was examined separately to identify its sector-specific practices, regulatory frameworks, and empirical findings. This analysis focused on three categories:

1. **Cyber hygiene practices**, including patch management, password policies, access control, and multi-factor authentication.

2. **Security training programmes**, including scope, frequency, and methods such as phishing simulations, scenario-based training, or awareness campaigns.

3. **Integration with organisational management systems**, particularly safety management systems (SMS), information security management systems (ISMS), and business continuity management systems (BCMS).

The results from each sector were then synthesised to identify common challenges, best practices, and gaps across the transport ecosystem. This comparative method was chosen to provide a holistic understanding of criterion 7 implementation, rather than limiting the scope to a single transport mode.

Results – Sectoral Analysis

Rail Transport

In the railway sector, cybersecurity has traditionally focused on the protection of signalling systems, traffic management platforms, and supervisory control and data acquisition (SCADA) infrastructure. However, reports by ENISA and the European Union Agency for Railways (ERA) indicate that the maturity of organisational measures, including cyber hygiene and staff training, remains relatively low compared to other critical infrastructure domains (ENISA, 2020; ERA, 2021). Key weaknesses include the lack of systematic awareness programmes and insufficient integration of cybersecurity education into safety management systems. Although training initiatives exist, they are often limited to IT staff, while operational personnel such as drivers, dispatchers, and maintenance workers receive less structured education. This imbalance increases the likelihood of incidents linked to phishing or misconfigurations, which accounted for a significant portion of high-risk events identified in FMEA-based studies.

Aviation

The aviation sector has developed a more advanced approach to cyber hygiene and training, largely due to its long-standing culture of safety management. The European Union Aviation Safety Agency (EASA) requires the integration of cybersecurity into the Safety Management System (SMS), explicitly including awareness training and competence development (EASA, 2024). Academic research confirms that awareness and training constitute some of the most cost-effective measures in aviation cybersecurity, particularly in mitigating risks related to social engineering and insider threats (Mizrak & Akkartal, 2024). Training programmes are typically mandatory, recurrent, and scenario-based, reflecting the sector's emphasis on drills and exercises. The aviation domain thus provides a model for how criterion 7 of NIS2 can be operationalised in a systematic and measurable way.

Maritime

Maritime transport is characterised by a high degree of human involvement, with crews frequently rotating and operating in international contexts. The International Maritime Organization (IMO) has responded by issuing its *Guidelines on Maritime Cyber Risk Management*, revised in 2022 and 2025, which emphasise that cyber risk management must be integrated into the International Safety Management (ISM) framework (IMO, 2022; IMO, 2025). These guidelines stress the importance of cyber hygiene practices onboard, including secure use of removable media, patching procedures, and password management. Studies on training effectiveness in the maritime domain, such as the Maritime Cybersecurity Awareness (MarCy) programme, demonstrate that modular and scenario-based training can significantly enhance crew awareness and reduce vulnerabilities (Oruc et al., 2024). Nevertheless, challenges remain, particularly in ensuring continuity of training across multinational crews and aligning practices with diverse flag state requirements.

Road Transport

In road transport, the rapid digitalisation of vehicles and logistics systems has exposed operators to new vulnerabilities. UNECE Regulation No. 155 requires automotive manufacturers to implement cybersecurity management systems, explicitly including competence-building and awareness among staff involved in vehicle design, production, and maintenance (UNECE, 2021). However, awareness at the operational level, particularly among logistics companies and drivers, remains uneven. Industry reports highlight that phishing and social engineering campaigns targeting freight operators are increasing in frequency and sophistication, often exploiting weak password practices and insufficient awareness of digital threats (NMFTA, 2025). Unlike aviation or maritime, road transport lacks a strong regulatory culture of mandatory training, which hampers the systemic implementation of criterion 7.

Cross-Sector Comparison

The comparative analysis reveals both convergences and divergences in the implementation of cyber hygiene and training across transport modes. Aviation stands out as the most mature sector, with institutionalised training cycles and integration of cybersecurity into SMS. Maritime transport demonstrates progress through IMO guidelines and modular training initiatives, though it struggles with crew rotation challenges. Rail transport shows significant gaps in awareness outside IT staff, despite its designation as an essential entity under NIS2. Road transport remains the least developed, with regulatory obligations concentrated on manufacturers rather than operators.

Across all modes, phishing, weak credentials, and poor patching practices emerge as recurring risks, indicating that criterion 7 is central to resilience. However, the degree of integration of training and hygiene practices into broader management systems varies significantly. This finding underlines the need for harmonised standards and cross-sector learning mechanisms to ensure consistent implementation of NIS2 requirements in the transport ecosystem.

Example Implementation of Criterion 7 in a Railway Company

To comply with criterion 7 of NIS2, a railway company could establish a comprehensive policy framework and implement concrete actions that embed cyber hygiene and training into its organisational culture.

1. **Cyber Hygiene Policies**

The company should adopt formal cyber hygiene guidelines applicable to all employees, not only IT staff. These policies would cover:

- **Password and authentication management** – mandatory use of multi-factor authentication (MFA), password complexity and rotation rules, prohibition of password reuse (ENISA, 2025).
- **Patch and update management** – structured processes to ensure timely updates of both IT and OT systems, documented schedules for security patches (ISO/IEC 27002:2022).
- **Secure use of devices and media** – rules on removable media, endpoint protection, and secure mobile device management (ENISA, 2020).
- **Access control** – role-based access rights, regular reviews of privileges, segregation of duties (European Union, 2022).
- **Incident prevention routines** – policies requiring employees to lock terminals, log off after shifts, and avoid shadow IT applications.

2. **Security Training Programmes**

The company should establish a multi-tiered training strategy:

- **Induction training** for all new employees, covering phishing awareness, safe use of company systems, and reporting procedures (Oruc et al., 2024).
- **Regular refresher courses**, ideally annually, adapted to the role (drivers, dispatchers, maintenance staff, IT specialists).
- **Phishing simulations and exercises** to test awareness and provide immediate feedback to employees (Prümmer et al., 2024).
- **Tabletop exercises** combining cyber and safety scenarios, integrating incident response with operational continuity procedures (EASA, 2024).

3. **Integration with Management Systems**

For railway companies already operating under a Safety Management System (SMS) and often ISO-certified Information Security Management System (ISMS), criterion 7 measures should be embedded into these structures. For example:

- Cyber hygiene checklists integrated into safety audits and inspections.

- Training effectiveness monitored via key performance indicators (e.g., percentage of employees completing courses, phishing simulation success rates).

- Incident post-mortems incorporating human factor lessons, leading to adjustments in training curricula.

4. Governance and Oversight

A Chief Information Security Officer (CISO) or equivalent should be responsible for overseeing cyber hygiene and training programmes. Regular reports to top management and supervisory boards would ensure accountability and alignment with NIS2 requirements. Independent audits and compliance reviews should be conducted periodically to evaluate effectiveness (ENISA, 2025).

Comparative Perspective: Implementing Criterion 7 Across Transport Modes

The implementation of cyber hygiene practices and security training in a railway company provides a useful reference point for examining the adaptation of criterion 7 in other transport domains. While the underlying principles—password management, patching, access control, phishing awareness, and training integration—remain consistent, each mode of transport exhibits specific characteristics that influence implementation.

Rail Transport

In the railway sector, the coexistence of legacy operational technology and modern IT platforms creates a fragmented environment where cyber hygiene is challenging. Policies must therefore account for long life-cycle assets that are difficult to patch, and for operational staff who often lack cybersecurity awareness. Training strategies need to target diverse groups, including drivers, dispatchers, and maintenance personnel, in addition to IT staff (ENISA, 2020; ERA, 2021).

Aviation

In aviation, the integration of cybersecurity into the Safety Management System (SMS) facilitates the institutionalisation of cyber hygiene and training. For airlines and airport operators, access control and secure authentication measures are already tightly regulated due to safety requirements, which supports the adoption of NIS2-aligned hygiene practices. Training in aviation tends to be recurrent and scenario-based, making it easier to embed phishing simulations and cybersecurity drills within existing competence management systems (EASA, 2024; Mizrak & Akkartal, 2024).

Maritime Transport

Maritime operations are distinguished by the high mobility and turnover of crews, as well as the multinational composition of personnel. This makes standardised training more difficult to maintain. The IMO's guidelines emphasise the need for continuous crew awareness and hygiene practices, such as secure use of removable media and strict password policies (IMO, 2022; IMO, 2025). Modular, short-cycle training programmes, such as Maritime Cybersecurity Awareness (MarCy), are particularly suitable in this environment, as they can be delivered flexibly to rotating crews (Oruc et al., 2024).

Road Transport

Road transport presents unique challenges. While UNECE Regulation No. 155 obliges manufacturers to implement cybersecurity management systems that include competence-building, operational staff such as truck drivers or logistics operators often work in decentralised contexts where systematic training is difficult to enforce (UNECE, 2021). Cyber hygiene policies for this sector must therefore emphasise lightweight, easy-to-use measures, such as secure mobile device management, awareness of phishing attempts targeting logistics companies, and straightforward password protocols. Unlike aviation or maritime, training is not embedded in a global regulatory framework, which creates disparities in implementation (NMFTA, 2025).

Cross-Sector Insights

The comparison reveals three critical insights. First, the railway model of integrating cyber hygiene into both organisational policies and staff training can serve as a template for other transport modes, provided it is adapted to sector-specific constraints. Second, aviation demonstrates the benefits of embedding cybersecurity into safety governance structures, a lesson that could be transferred to rail and maritime. Third, while road transport lacks strong regulatory enforcement of training, simple and accessible hygiene practices could yield significant resilience benefits given the distributed and resource-constrained nature of the sector.

Overall, criterion 7 emerges as a unifying measure across transport modes, but its operationalisation must account for the distinctive organisational, technical, and regulatory environments of each subsector.

Discussion

The comparative analysis of transport subsectors demonstrates that cyber hygiene and security training (criterion 7 of Article 21 of NIS2) are implemented unevenly across the transport ecosystem. While the general principles of cyber hygiene—such as patch management, secure authentication, password policies, and phishing awareness—are universal, sector-specific characteristics significantly affect the depth and quality of implementation.

In **aviation**, cybersecurity awareness and training are deeply embedded into existing governance structures. The European Union Aviation Safety Agency (EASA) requires the integration of cybersecurity into the Safety Management System (SMS), ensuring that cyber hygiene is addressed alongside operational safety. Regular, scenario-based training and competence assessments are already standard practice, making the aviation sector a benchmark for criterion 7 implementation (EASA, 2024; Mizrak & Akkartal, 2024).

In **maritime transport**, the International Maritime Organization (IMO) has strengthened requirements through its revised guidelines, which demand the integration of cybersecurity measures into the International Safety Management (ISM) framework (IMO, 2022; IMO, 2025). Training remains a central challenge due to the high turnover and international composition of crews. Modular and flexible training initiatives, such as Maritime Cybersecurity Awareness (MarCy), have proven effective in enhancing awareness (Oruc et al., 2024). Nevertheless, inconsistencies persist because training practices often depend on flag states and individual shipping companies.

In the **railway sector**, cyber hygiene and training remain less mature. Reports from ENISA and ERA underline that awareness programmes are often limited to IT staff, while operational personnel such as drivers and dispatchers receive less systematic education (ENISA, 2020; ERA, 2021). Given the coexistence of legacy operational technology with modern IT platforms, the railway sector faces unique challenges in applying patch management and enforcing cyber hygiene policies. Without comprehensive training across all roles, vulnerabilities such as phishing or misconfiguration remain highly probable.

In **road transport**, UNECE Regulation No. 155 obliges manufacturers to adopt cybersecurity management systems that include training and competence building (UNECE, 2021). However, the operational reality of logistics companies shows persistent gaps in awareness and hygiene. Truck drivers and logistics operators often lack systematic training, and industry analyses reveal that phishing and ransomware campaigns frequently target this sector (NMFTA, 2025). Unlike aviation or maritime, where strong regulatory oversight ensures training consistency, road transport remains fragmented, relying largely on voluntary initiatives by companies.

Cross-sector comparison highlights three overarching findings. First, aviation demonstrates how criterion 7 can be effectively operationalised when integrated into robust safety cultures and management systems. Second, maritime shows the potential of modular and scenario-based training but also illustrates the difficulties of ensuring continuity across mobile and multinational workforces. Third, rail and road remain the weakest links, due to organisational fragmentation, legacy infrastructure, and insufficient institutionalisation of training. Despite these differences, common weaknesses—such as poor password management, insufficient phishing awareness, and irregular patching—persist across all transport modes.

From a regulatory perspective, the results underscore the need for harmonisation of training requirements across transport sectors. ENISA's technical guidance already links cyber hygiene and training to measurable indicators and audit evidence (ENISA, 2025), but sector-specific adaptations are required to account for operational realities. Lessons from aviation and maritime suggest that embedding training into established safety or risk governance frameworks and employing recurrent, scenario-based methods significantly improve resilience. Applying such approaches to rail and road transport could close the maturity gap and ensure more consistent implementation of NIS2.

Recommendations

The findings of this study highlight that while criterion 7 of the NIS2 Directive—basic cyber hygiene practices and security training—is universally applicable, its implementation requires sector-specific adjustments. Recommendations are therefore presented at two levels: cross-sectoral actions that apply to all transport domains, and tailored actions reflecting the particularities of rail, aviation, maritime, and road transport.

Cross-Sectoral Recommendations

Across all modes of transport, three overarching actions are recommended. First, **institutionalising cyber hygiene policies** by embedding password rules, patching routines, and access control into formal procedures aligned with ISO/IEC 27002 and ENISA guidance (ENISA, 2025). Second, **systematic training and awareness programmes** should be mandatory for all staff, not limited to IT departments, with a focus on phishing awareness, reporting procedures, and incident prevention (Prümmer et al., 2024). Third, **integration with management systems** is essential: cybersecurity training should be linked to Safety Management Systems (SMS), Information Security Management Systems (ISMS), and Business Continuity Management Systems (BCMS), thereby ensuring sustainability and auditability (European Union, 2022).

Sector-Specific Recommendations

Rail Transport

Railway operators should extend cyber hygiene training beyond IT specialists to include operational personnel such as drivers, dispatchers, and maintenance staff. Specific emphasis should be placed on phishing awareness, misconfiguration prevention, and secure handling of legacy operational technology. Embedding training modules into existing safety certification schemes could improve uptake (ENISA, 2020).

Aviation

Aviation should continue to leverage its mature safety culture by expanding scenario-based training to cover hybrid threats that combine safety and cybersecurity risks. Regulators should mandate recurrent cyber hygiene assessments as part of SMS audits. This approach would reinforce aviation's position as a benchmark sector (EASA, 2024; Mizrak & Akkartal, 2024).

Maritime Transport

For maritime operators, modular and flexible training programmes are recommended to accommodate crew rotation and multinational composition. The IMO's guidelines should be supplemented by EU-level monitoring to ensure consistent implementation across flag states. Priority should be given to reinforcing password policies, patching practices, and secure use of removable media onboard (IMO, 2022; Oruc et al., 2024).

Road Transport

In road transport, simple and accessible hygiene measures should be prioritised, such as mobile device management, password hygiene, and phishing awareness for logistics staff. As UNECE Regulation No. 155 applies primarily to manufacturers, EU regulators should encourage logistics companies and operators to adopt voluntary but standardised training frameworks. Industry associations could play a coordinating role in promoting awareness programmes across fragmented supply chains (UNECE, 2021; NMFTA, 2025).

Policy Implications

At the regulatory level, the European Commission and ENISA should consider developing **harmonised training standards for transport**, defining minimum curricula and learning outcomes for cyber hygiene. Cross-sector benchmarking, with aviation as a reference model, could accelerate maturity in rail and road transport. In addition, establishing EU-wide **cybersecurity awareness campaigns** for transport employees could address common weaknesses, particularly phishing susceptibility and poor password practices.

Conclusions

This paper examined the implementation of criterion 7 of the NIS2 Directive—basic cyber hygiene practices and security training—across the transport sector. The analysis revealed that while cyber hygiene and training are universally recognised as cost-effective measures for reducing cyber risk, their implementation remains uneven across transport modes. Aviation demonstrates the highest maturity, supported by a long-standing safety culture and recurrent, scenario-based training embedded in regulatory frameworks. Maritime transport has advanced through IMO guidelines and modular training initiatives but struggles with consistency due to crew mobility and international regulatory diversity. Rail transport lags behind, with training often restricted to IT staff and insufficient attention given to operational personnel who face daily cyber risks. Road transport remains the least developed, with regulatory requirements focused on manufacturers rather than operators, leaving significant gaps in awareness among logistics companies and drivers.

Three cross-cutting findings emerge. First, integration of cyber hygiene and training into existing governance systems such as SMS, ISMS, and BCMS is decisive for sustainability and compliance. Second, common weaknesses—such as poor password management, inadequate patching, and low awareness of phishing—persist across all modes, underlining the foundational role of criterion 7 in building resilience. Third, sector-specific challenges require tailored approaches: modular training for maritime, extended awareness for rail, simplified measures for road, and hybrid threat preparedness for aviation.

From a policy perspective, the results suggest the need for harmonised training frameworks across the EU transport ecosystem. Lessons from aviation and maritime can inform the development of sectoral standards, while ENISA's technical guidance offers a baseline for measurable and auditable implementation. Future research should focus on developing cross-sector training models, evaluating their effectiveness through longitudinal studies, and exploring the integration of digital tools such as e-learning platforms, phishing simulations, and gamified training into daily operations.

Overall, the analysis confirms that cyber hygiene and training are not peripheral obligations but essential enablers of cyber resilience in transport. Ensuring that criterion 7 is implemented consistently and effectively across all transport modes will strengthen not only compliance with NIS2 but also the safety, continuity, and trustworthiness of critical mobility services in the European Union.

References

- **Directive (EU) 2022/2555 (NIS2).** 2022. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. *Official Journal of the European Union*, L333, pp. 80–152. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.
- **EASA (European Union Aviation Safety Agency).** 2024. *Easy Access Rules for Information Security (Regulation (EU) 2023/203 and Regulation (EU) 2022/1645)*. Cologne: EASA. Available at: https://www.easa.europa.eu/en/document-library/easy-access-rules/ear-information-security.
- **ENISA (European Union Agency for Cybersecurity).** 2020. *Railway Cybersecurity: Security measures in the railway transport sector*. Athens: ENISA. Available at: https://www.enisa.europa.eu/publications/railway-cybersecurity.
- **ENISA (European Union Agency for Cybersecurity).** 2021. *Railway Cybersecurity – Good Practices in Cyber Risk Management*. Athens: ENISA. Available at: https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management.
- **ENISA (European Union Agency for Cybersecurity).** 2023. *ENISA Threat Landscape: Transport Sector 2023*. Athens: ENISA. Available at: https://www.enisa.europa.eu/publications/transport-threat-landscape.
- **ENISA (European Union Agency for Cybersecurity).** 2025. *Technical Implementation Guidance on Cybersecurity Risk Management Measures*. Athens: ENISA. Available at: https://www.enisa.europa.eu/publications/technical-implementation-guidance-on-cybersecurity-risk-management-measures.
- **ERA (European Union Agency for Railways).** 2021. *Taking cybersecurity challenges into account in railway safety*. Valenciennes: ERA. Available at: https://www.era.europa.eu/library/taking-cybersecurity-challenges-account-railway-safety_en.
- **IMO (International Maritime Organization).** 2022. *Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3/Rev.2*. London: IMO. Available at: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2.pdf.

- **IMO (International Maritime Organization).** 2025. *Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3/Rev.3*. London: IMO. Available at: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.3.pdf.
- **NMFTA (National Motor Freight Traffic Association).** 2025. *2025 Trucking Cybersecurity Trends Report*. Alexandria, VA: NMFTA. Available at: https://nmfta.org/2025-trucking-cybersecurity-trends-report/.
- **Oruc, A., Chowdhury, N., & Gkioulos, V.** 2024. A modular cyber security training programme for the maritime domain. *International Journal of Information Security*. Available at: https://doi.org/10.1007/s10207-023-00799-4.
- **Oruc, A., Chowdhury, N., & Gkioulos, V.** 2024. Evaluation of Maritime Cyber Security (MarCy) Training Programme. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, 18(4). Available at: https://transnav.am.gdynia.pl/Article/Evaluation-of-Maritime-Cyber-Security-Oruc,74,1396.html.
- **Prümmer, J., van Steen, T., & van den Berg, B.** 2024. A systematic review of current cybersecurity training methods. *Computers & Security*, 136, 103585. Available at: https://doi.org/10.1016/j.cose.2024.103585.
- **Ruohonen, J.** 2024. A Systematic Literature Review on the NIS2 Directive. *arXiv preprint*, arXiv:2412.08084. Available at: https://arxiv.org/abs/2412.08084.
- **UNECE (United Nations Economic Commission for Europe).** 2021. *UN Regulation No. 155 – Cyber Security and Cyber Security Management System*. Geneva: UNECE. Available at: https://unece.org/transport/standards/vehicle-regulations-wp29/un-regulation-no-155.

Funding

This research received no external funding.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

The data presented in this study are available on request from the corresponding author.

Conflicts of Interest

The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.