

Technology Management and Cybersecurity Governance in Sea Transportation Digital Systems

Fitri Mulyana ^{1*}, Fina Rahmatika ¹, Nurul Wahyuni ¹

¹ Maritime Institute, Sekolah Tinggi Ilmu Pelayaran Jakarta, North Jakarta, Indonesia

Alamat: STIP Indonesia - Transportation Human Resources Development Agency - Ministry of Transportation, Jl. Marunda Makmur, Cilincing, North Jakarta, DKI Jakarta, Indonesia

*Corresponding email: fitrimulyana2002@gmail.com

Abstract. As sea transportation operations increasingly rely on networked digital systems for navigation, cargo documentation, and port coordination, technology management in the sector must extend beyond adopting new tools to governing the risks those tools introduce, including cybersecurity exposure. This paper examines technology management and cybersecurity governance as dimensions of sea transportation management, using Akademi Maritim Djadayat and Sekolah Tinggi Manajemen Transportasi (STMT) Malahayati as reflective case settings for the period April 2025 to January 2026. Drawing on the technology management and information-security literature, together with institutional document review and field observation of digital-systems training and administrative practice at both institutions, the paper finds that technology adoption is proceeding steadily in both training and administrative functions, but that cybersecurity awareness and information security culture, increasingly recognized in the wider technology management literature as a precondition for safe digital adoption, are not yet formally integrated into either institution's curriculum or administrative governance. The paper argues that as sea transportation digitalizes, maritime training institutions carry a dual responsibility: managing their own administrative technology risk, and preparing graduates who will enter a workforce where shipboard and port digital systems are themselves potential cybersecurity targets. A phased governance framework is proposed to close this gap without requiring disruptive curriculum overhaul.

Keywords: technology management, cybersecurity governance, sea transportation, information security culture, digital transformation, maritime education

1. Introduction

Technology management in sea transportation has historically been framed around adoption: acquiring digital navigation aids, computerized cargo documentation, and networked port coordination systems to improve efficiency and safety. As these systems become more interconnected, however, the management question shifts from whether to adopt digital technology toward how to govern the risks that adoption introduces, cybersecurity chief among them. A navigation system, a port information platform, or an administrative record system that is digitally networked is also a system that can be compromised, disrupted, or manipulated, and the consequences of such compromise in a maritime operating context extend beyond data loss to potential safety and operational failure.

This paper examines technology management and cybersecurity governance as they apply to sea transportation, with particular attention to the role of maritime training institutions both as adopters of administrative technology and as the source of the workforce that will operate increasingly digital systems at sea and in port. Using Akademi Maritim Djadayat and STMT Malahayati as reflective case settings for the period April 2025 to January 2026, the paper draws on the technology management and information-security literature to interpret

institutional documentation and field observation from the stated period, asking what current technology management practice looks like at these institutions and where cybersecurity governance, specifically, remains underdeveloped relative to the wider literature's recommendations.

2. Literature Review

2.1 Technology Management as an Evolving Field

Shi et al. (2023), analysing the current status, hotspots, and future trends of technology management research, find that the field has shifted markedly in recent years from a primary focus on innovation adoption and diffusion toward an increasing focus on governance, risk, and organizational readiness for the technologies being adopted. Their bibliometric analysis identifies cybersecurity and information governance as among the fastest-growing hotspots within technology management scholarship, indicating that the management discipline itself now treats risk governance as inseparable from adoption strategy rather than as a secondary compliance concern to be addressed after adoption decisions are made. This shift is directly relevant to sea transportation, a sector where digital adoption has historically been evaluated primarily on efficiency and safety-improvement grounds without equivalent attention to the new risk surface each adopted system creates.

2.2 Information Security Culture and Cybersecurity Governance

Zyoud and Lutfi (2024) examine the role of information security culture in the adoption of zero-trust cybersecurity architectures, finding that the technical effectiveness of a zero-trust or similarly rigorous security model depends heavily on whether the organization's personnel understand and internalize security-conscious behaviour, since even well-designed technical controls can be undermined by users who are not culturally oriented toward security practice. Their findings reinforce a point increasingly emphasized in the broader technology management literature: cybersecurity is not purely a technical implementation problem but an organizational culture and training problem, which places it squarely within the remit of institutions responsible for workforce preparation rather than solely within the remit of information-technology departments.

For sea transportation specifically, this literature suggests that cybersecurity readiness among future officers, engineers, and port personnel cannot be achieved through technical system design alone; it requires that the workforce entering the sector already carries a baseline information security culture from their training, in the same way that safety culture is instilled through training rather than left to be acquired entirely on the job.

2.3 Digital Transformation Governance in Administrative Contexts

Ciancarini et al. (2024), reviewing digital transformation in public administration contexts for a computer science audience, find that successful digital transformation programs consistently pair technology deployment with explicit governance structures, including designated accountability for data security and defined escalation procedures for system incidents, whereas programs that deploy technology without equivalent governance investment show higher rates of subsequent security incidents and user workarounds that undermine the intended benefits of digitalization. Although this literature addresses public administration broadly rather than maritime institutions specifically, its governance-pairing argument applies directly to any public-sector-adjacent institution, including state-affiliated maritime training providers, that is digitalizing administrative functions such as student records, cargo documentation training systems, or port-liaison platforms.

2.4 Digitalization Trends Specific to Maritime and Logistics Contexts

Elbouzidi et al. (2023), reviewing the role of artificial intelligence in warehouse digital twin systems, note that the growing sophistication of digital planning and monitoring tools in logistics contexts, closely related to the port and cargo-handling systems relevant to sea transportation, increases the value of the data these systems hold and therefore increases their attractiveness as a target for disruption or manipulation, reinforcing the case for treating cybersecurity as integral to any digitalization initiative rather than as an add-on. Sijabat and Simanjuntak (2025), examining collaboration and information sharing in smart eco-ports, similarly note that the safety and efficiency benefits of networked port information systems depend on the reliability and integrity of shared data, meaning that a cybersecurity failure at one contributing node can degrade the reliability of the wider network. Cahyadi et al. (2025), in their stakeholder-based analysis of sustainability and innovation adoption in maritime vocational education, add that technology initiatives in maritime training settings succeed only where stakeholders are aligned on how new systems will be used, maintained, and secured, echoing the governance-pairing argument of Ciancarini et al. (2024) within a maritime education setting specifically.

3. Methodology

This paper applies a qualitative, case-based management analysis to technology management and cybersecurity governance practice at Akademi Maritim Djadayat and STMT Malahayati over April 2025 to January 2026. Institutional documentation relating to digital-systems curriculum content, administrative information systems, and any formal cybersecurity policy or awareness programming was reviewed at both institutions. This review was

supplemented by field observation of digital-systems training and day-to-day administrative technology use during the stated period, reported descriptively, and interpreted against the technology management and information-security literature reviewed above. As with the companion workforce-readiness analysis, the two institutions are treated as a joint regional case setting rather than as a formal comparison, since the purpose is to characterize a shared institutional challenge rather than to rank the two providers.

4. Results and Discussion

4.1 Technology Adoption Is Proceeding Steadily

Both institutions showed continued digitalization of administrative functions during the observed period, including digital student records, electronic cargo-documentation training exercises, and, at STMT Malahayati in particular, logistics-management software used in coursework, consistent with the general technology management trend identified by Shi et al. (2023) of expanding digital adoption across institutional functions. This is a reasonable and expected pattern for maritime training institutions seeking to keep curricula aligned with the digitalized industry cadets will enter, and observation did not suggest any institutional reluctance toward digital adoption at either site.

4.2 Cybersecurity Governance Has Not Kept Pace with Adoption

Document review found no formal information security policy or structured cybersecurity awareness training at either institution during the observed period, despite the expanding administrative and instructional use of digital systems described above. This pattern is consistent with the general finding of Shi et al. (2023) that governance attention often lags adoption, and it mirrors the specific risk Zyoud and Lutfi (2024) identify: technical systems were being deployed without an equivalent investment in the information security culture that determines whether those systems are used safely. Neither institution's cadet curriculum included content on cybersecurity awareness for the digital navigation, documentation, or port-coordination systems cadets were being trained to use, representing a gap directly analogous to the one Zyoud and Lutfi (2024) describe: technically capable future operators entering the workforce without a corresponding security-culture foundation.

Consistent with Ciancarini et al.'s (2024) governance-pairing argument, this gap did not appear to have caused an observed incident during the study period, but its absence represents latent risk rather than demonstrated safety, since the absence of an incident is not evidence of the absence of vulnerability.

4.3 An Opportunity to Integrate Security Culture Without Curriculum Overhaul

Following the reasoning of Sijabat and Simanjuntak (2025) and Cahyadi et al. (2025), the interconnected nature of port and logistics information systems means that a cybersecurity gap at either institution is not solely an internal risk but a potential weak point in the wider regional maritime information network both institutions' graduates will eventually operate within. This paper suggests that closing the gap identified above does not require a dedicated new course; consistent with Ciancarini et al.'s (2024) governance-pairing model, basic information security culture content, covering safe data handling, credential hygiene, and recognition of common manipulation tactics, could be embedded within the existing digital-systems coursework already present at both institutions, alongside a simple designated-accountability structure for administrative system security of the kind Ciancarini et al. (2024) find distinguishes successful digital transformation programs from unsuccessful ones.

5. Conclusion

Technology management in sea transportation is shifting, in line with the wider technology management literature, from a primary focus on adoption toward an equally important focus on governance and risk, with cybersecurity as a central concern. The case of Akademi Maritim Djadayat and STMT Malahayati over April 2025 to January 2026 indicates that both institutions are adopting digital systems steadily in both administrative and instructional functions, but that formal cybersecurity governance and information security culture-building have not kept pace with that adoption, mirroring a pattern documented more broadly in the technology management literature. Because maritime training institutions both manage their own administrative technology risk and prepare the workforce that will operate the sector's increasingly networked digital systems, this paper recommends embedding basic information security culture content into existing digital-systems coursework and establishing simple administrative accountability structures for system security, as a proportionate and low-disruption first step toward closing this gap at both institutions.

References

- Cahyadi, T., Winarno, W., Barasa, L., Suranta, N., Simanjuntak, M., Herawati, S., & Simanjuntak, M. B. (2025). Integrating sustainability and innovation in maritime vocational education through stakeholder-based analysis. *BIO Web of Conferences*, 186. <https://doi.org/10.1051/bioconf/202518602004>
- Ciancarini, P., Giancarlo, R., & Grimaudo, G. (2024). Digital transformation in the public administrations: A guided tour for computer scientists. *IEEE Access*, 12, 20890–20915.

- Elbouzidi, A. D., Artiba, A., Pellerin, R., Lamouri, S., Valencia, E. T., & Bélanger, M.-J. (2023). The role of AI in warehouse digital twins: Literature review. *Applied Sciences*, 13(11), 6746.
- Shi, Y., Ramayah, T., Hongmei, L., Zhang, Y., & Wang, W. (2023). Analysing the current status, hotspots, and future trends of technology management. *Heliyon*, 9(9), e19922.
- Sijabat, P. S., & Simanjuntak, M. B. (2025). Enhancing collaboration and information sharing in smart eco-ports. *Journal of Maritime Research*, 22(3), 346–351.
- Zyoud, B., & Lutfi, S. L. (2024). The role of information security culture in zero trust adoption. *IEEE Access*, 12, 68775–68790.