Anchoring Security in Maritime: Defining and Protecting Critical Assets for Business Continuity

Ahti Mansner[1], Eino Kärkkäinen[1], Lara Ayodele[1], Aleksi Janhunen[1] and Ilkka Tikanmäki[1 1 2]
[1]Security and Risk Management, Laurea University of Applied Sciences, Espoo, Finland
[2]Department of Warfare, National Defence University, Helsinki, Finland

ilkka.tikanmaki@laurea.fi
ahti.mansner@student.laurea.fi
aleksi.janhunen@student.laurea.fi
eino.karkkainen@student.laurea.fi
lara.ayodele@student.laurea.fi

Abstract: This study highlights maritime operations increasingly relying on digital technologies, creating new cybersecurity vulnerabilities that threaten global trade. The study addresses this gap by developing a systematic approach to identify business-critical digital assets, focusing on cargo management systems that directly impact revenue generation. The methodology employs Attack Tree analysis, examining maritime digital assets through factors of production lens. Systems enabling cargo booking, loading, and revenue generation to determine criticality are analysed. Initial findings indicate that cargo management systems represent vital digital assets, directly impacting operational continuity. This study evaluates a framework for maritime operators to assess and protect their critical digital infrastructure, ensuring business continuity while bridging the gap between onshore and offshore cybersecurity requirements. Offshore maritime operators fall under International Maritime Organization (IMO) legislation. Onshore operations follow traditional frameworks, leaving no unified cybersecurity framework for maritime operators. The mixed methods approach combines qualitative interviews with maritime small and medium-sized enterprises (SMEs) and quantitative analysis of cybersecurity frameworks and risk management methods. Given SMEs' limited resources and expertise, the study focuses on implementing a suitable risk management concept to help SMEs ensure business continuity and protect essential operations. Findings revealed that maritime operations increasingly depend on digital technologies, a trend already evident in both onshore and offshore operations. When focusing on business continuity and examining typical frameworks used by maritime operators, gaps between onshore and offshore operations were identified. Research is centred on addressing this gap, specifically through the ISO 22301 framework. The findings highlight a notable distinction between onshore and offshore operations. This study shows that small maritime companies must protect their crucial digital systems, especially cargo management. Using a simple security framework (ISO 22301) helps these companies stay safe both onshore and offshore. This method aids SMEs in focusing on protecting what matters most. Future research should find cheaper, easier ways to help these companies improve their cybersecurity smoothly.

Keywords: Critical asset, ISO22301, Maritime onshore- and offshore operations, Risk management, Attack tree method

1. Introduction

Maritime operations represent one of the world's most critical infrastructures (De Felice et al., 2022), with trade volumes reaching 12,292 million tons in 2023 (United Nations, 2024). The increasing digitalisation of maritime operations, while enhancing efficiency, has introduced significant vulnerabilities that threaten global trade security (International Maritime Organization, 2022). This research reveals that cyber threats are particularly critical for Small and medium-sized enterprises (SMEs) in the maritime sector, where system breaches can lead to severe operational and financial consequences. The European Union supports research through its Research and Innovation programs, such as the Dynamic Resilience Assessment Method, including a combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors (DYNAMO) project (DYNAMO project, 2024).

This project aims to solve vulnerable parts of businesses, with this research specifically focusing on maritime operations and identifying a crucial gap between offshore operations governed by International Maritime Organization (IMO) legislation (International Maritime Organization, 2025), and onshore operations following traditional frameworks. Earlier studies in the domain have analysed, e.g. threats and vulnerabilities in the maritime domain (Bakir, 2007; Kapalidis et al., 2022).

The project employs two key components: Attack Tree analysis methodology (Ingoldsby, 2021) applied to a hypothetical maritime company for examining digital assets, and the ISO 22301 framework for comprehensive asset protection (ISO, 2019). These tools enable maritime operators to identify and protect their critical digital

[1]https://orcid.org/0000- 0001-8950-5221

infrastructure, with particular emphasis on cargo management systems that directly impact business continuity (ISO, 2022a, 2022b). This work-in-progress paper aims to present a systematic approach to identifying and protecting critical digital assets in maritime operations, focusing specifically on SME operators. After the introduction, section 2 examines the methodology, including the mixed-methods approach. Section 3 presents findings regarding digital technologies in maritime operations. Finally, section 4 concludes the paper and suggests future directions for implementation.

2. Methodology

Initially, the basics of navigation were studied, and it was discovered that a sailor, whether a single sailor or a large merchant ship, was not allowed to rely solely on electronic aids according to maritime regulations. The original assumption of a critical point in navigational aids was not confirmed. (Encyclopedia Britannica, 2025; Sleight, 2001)

First, a qualitative interview was conducted with a representative from a maritime SME to understand the practical challenges, resource constraints and specific vulnerabilities faced by typical maritime SME operators. This interview provided insights into the operational dynamics of both onshore and offshore environments and highlighted the disparities in cybersecurity preparedness. The interview also confirmed the initial assessment that the critical point of the shipping business is not in the ship's navigation systems but in the information systems that support and maintain the business. Second, a quantitative analysis of existing cybersecurity frameworks and risk management methodologies was performed to identify the most suitable strategies for protecting critical digital assets. Among these, the Attack Tree analysis method (Ingoldsby, 2021) was utilised to systematically identify vulnerabilities and assess potential threats to maritime SME operations, focusing particularly on cargo management systems that directly impact revenue and business continuity. With this information, the ISO 22301 framework was identified as a robust solution for bridging the cybersecurity gap. Its application ensures a structured approach to business continuity, emphasising risk assessment, resource allocation, and recovery planning, making it an ideal choice for maritime SMEs to safeguard operations efficiently and sustainably.

3. Findings

The research began with a focus on understanding the critical assets of maritime operators, recognising the growing reliance on digital technologies in the sector. This dependence on digital systems is evident across both onshore and offshore operations, highlighting the importance of robust strategies to ensure business continuity. However, when examining frameworks commonly employed by maritime operators to support business continuity, a significant gap was identified between the practices used for onshore and offshore operations. To investigate this gap further, the Attack Tree method was utilised within a hypothetical maritime company (Ingoldsby, 2021). This method allowed the systematic identification of critical assets and assessment of vulnerabilities within the context of business continuity. The analysis revealed a pronounced disparity in how onshore and offshore operations are managed, particularly in terms of preparedness and resilience. Onshore operations often have well-defined continuity frameworks supported by advanced infrastructure and centralised management systems.

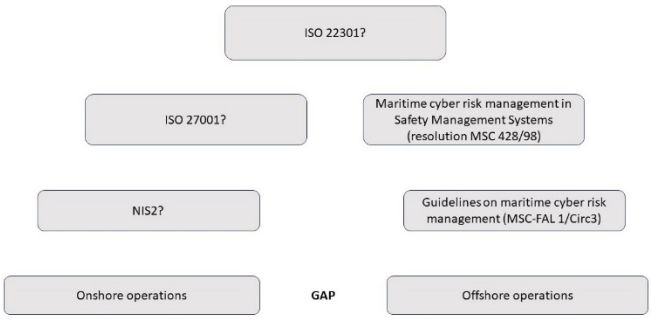

Figure 1*: GAP between onshore and offshore*

In contrast, offshore operations frequently face limited resources, harsher environmental conditions, and less robust continuity planning. This gap between onshore and offshore operations represents a critical vulnerability in the maritime sector, where the interconnected nature of these domains demands seamless integration and consistent resilience measures. Recognising the need for a unified approach, this research identified ISO 22301 as a potential solution to bridge this gap. ISO 22301 is the international standard for Business Continuity

Management Systems (BCMS), providing a structured framework for organisations to ensure the resilience of critical functions during disruptions. (ISO, 2019). By applying ISO 22301, maritime operators can create a cohesive strategy that addresses the unique challenges of both onshore and offshore environments. This standard emphasises risk assessment, resource allocation, and recovery planning, offering a comprehensive solution to bolster operational continuity. Findings underscore the urgent need to address the gap between onshore and offshore operations. Implementing ISO 22301 can not only mitigate risks but also enhance overall operational reliability, ensuring maritime operators are better prepared to navigate the complexities of modern digital dependencies.

4. Conclusions

This research highlights the importance of identifying and protecting critical digital assets in maritime operations, especially for SMEs with limited cybersecurity resources. Using the Attack Tree method, it was found that in this example, cargo management systems were the most essential assets, directly affecting revenue and business continuity.

The ISO 22301 framework provides a practical solution to bridge the cybersecurity gap between onshore and offshore operations. While this approach ensures continuity, SMEs may face challenges due to limited resources and expertise. However, the proposed method helps SMEs focus on securing key operations and managing risks effectively. Thus, a comprehensive threat and vulnerability analysis is necessary for both onshore and offshore systems.

Compared to onshore operations, offshore operations are often more limited and lack robust continuity planning. Seamless integration and resilience measures are necessary to address this critical vulnerability in the maritime industry.

Future research should explore simpler and more affordable solutions tailored to SMEs to make this approach more accessible. This would ensure they can adopt cybersecurity measures easily while safeguarding their critical systems and ensuring smooth maritime operations.

Acknowledgements

This study has received funding from the European Union project DYNAMO, the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101069601. The views expressed are those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

References

Bakir, N.O., 2007. A Brief Analysis Of Threats And Vulnerabilities In The Maritime Domain, in: Linkov, I., Wenning, R.J., Kiker, G.A. (Eds.), Managing Critical Infrastructure Risks. Springer Netherlands, Dordrecht, pp. 17–49. https://doi.org/10.1007/978-1-4020-6385-5_2

De Felice, F., Baffo, I., Petrillo, A., 2022. Critical Infrastructures Overview: Past, Present and Future. Sustainability 14. https://doi.org/10.3390/su14042233

DYNAMO project, 2024. DYNAMO Mission and Objectives [WWW Document]. URL https://horizon-dynamo.eu/about/ (accessed 1.9.24).

Encyclopedia Britannica, 2025. Navigation - Definition, History, Measurements, & Facts [WWW Document]. Navigation Technology. URL https://www.britannica.com/technology/navigation-technology (accessed 1.8.25).

Ingoldsby, T.R., 2021. Attack tree-based threat risk analysis.

International Maritime Organization, 2025. The International Safety Management (ISM) Code [WWW Document]. The International Safety Management (ISM) Code. URL https://www.imo.org/en/OurWork/HumanElement/Pages/ISMCode.aspx (accessed 1.8.25).

International Maritime Organization, 2022. Guidelines on Maritime Cyber Risk Management (Guidelines No. MSC-FAL.1/Circ.3/Rev.2). International Maritime Organization, London UK.

ISO, 2022a. ISO/IEC 27001 Standard – Information Security Management Systems.

ISO, 2022b. ISO 23806:2022 - Ships and marine technology — Cyber safety.

ISO, 2019. ISO 22301 - Business continuity.

Kapalidis, C., Karamperidis, S., Watson, T., Koligiannis, G., 2022. A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships. Journal of Marine Science and Engineering 10, 1486. https://doi.org/10.3390/jmse10101486

Sleight, S., 2001. Complete Sailing Manual, 1st ed. Dorling Kindersley Ltd, Singapore.

United Nations, 2024. Review of maritime transport 2024: Navigating maritime chokepoints (Review No. UNCTAD/RMT/2024). United Nations, Geneva, Switzerland.