Spring 3-16-2024

Cybersecurity in the Maritime Industry: A Grounded Theory Exploration in the Hampton Roads Region

Michael Lapke

Christopher Kreider

Mohammad Almalog

Cybersecurity in the Maritime Industry: A Grounded Theory Exploration in the Hampton Roads Region

Michael Lapke
Christopher Newport University
michael.lapke@cnu.edu

Christopher Kreider
Christopher Newport University
chris.kreider@cnu.edu

Mohammad Almalog
Christopher Newport University
mohammad.almalag@cnu.edu

ABSTRACT

This study delves into the escalating cybersecurity concerns in the maritime sector as technology becomes more integrated with daily operations. Focused on the Hampton Roads region, it employs Grounded Theory to decipher the intricate dynamics of cybersecurity. Through interviews with key stakeholders and participant observation, it aims to grasp the challenges, risks, and remedies pertinent to maritime cybersecurity. Additionally, it scrutinizes existing frameworks and regulations to gauge their efficacy. Initial findings reveal resistance from organizations in complying with cybersecurity standards, hinting at pervasive vulnerabilities. The research promises to enrich scholarly dialogue and practical strategies for maritime entities, cybersecurity practitioners, and policymakers. By shedding light on the unique cybersecurity landscape of the Hampton Roads area, the study seeks to foster tailored approaches for bolstering cybersecurity resilience in maritime operations. This endeavor is crucial amid the digitalization wave, underscoring the imperative of safeguarding maritime activities for their safety, security, and sustainability.

Keywords

Maritime Industry, Cybersecurity, Grounded Theory

EXTENDED ABSTRACT

As the maritime industry increasingly relies on digital technologies, the threat landscape for cybersecurity has become a critical concern (Kechagias et al., 2022). This study aims to explore the multifaceted dynamics of cybersecurity in the maritime sector, specifically within the Hampton Roads region. Employing Grounded Theory as the research methodology, this investigation seeks to derive substantive theories from the data to comprehensively understand the unique challenges, risk factors, and potential solutions in the intersection of cybersecurity and the maritime industry (Glaser and Strauss, 2017).

The research will involve a multi-faceted approach, including interviews with key stakeholders such as maritime professionals, cybersecurity experts, and regulatory authorities. The study will also employ participant observation to gain insights into the day-to-day operations and challenges faced by maritime entities in ensuring cybersecurity resilience. Additionally, a thorough review of existing cybersecurity frameworks and regulations applicable to the maritime sector will be conducted (IMO, 2024).

Key objectives of the study include identifying the specific cyber threats faced by maritime organizations in the Hampton Roads region, understanding the current state of cybersecurity preparedness, and exploring the impact of regulatory frameworks on industry practices (Androjna, et al., 2020). Through an iterative process of data collection and analysis guided by Grounded Theory, the study aims to develop a nuanced understanding of the interplay between technological, organizational, and regulatory factors influencing cybersecurity in the maritime context.

At this stage of the research, initial interviews have been conducted and preliminary data has been collected. The researchers have encountered significant resistance in their efforts to recruit participants and organizations. There has been some success in the meta organization level (i.e. maritime associations) in lieu of actual maritime organizations and some important insight has been revealed with these meetings. It appears as though there is very little in the way of compliance with cybersecurity regulations and standards in the maritime industry and organizations are leery to reveal this.

The findings of this research will contribute to both academic discourse and practical implications for the maritime industry, cybersecurity professionals, and policymakers. By uncovering the intricacies of cybersecurity challenges in the Hampton Roads region, the study will provide valuable insights into developing tailored strategies for enhancing cybersecurity resilience within

the maritime sector. This research is essential in an era where the convergence of digitalization and maritime operations necessitates a comprehensive understanding of the cybersecurity landscape to ensure the safety, security, and sustainability of maritime activities.

REFERENCES

1. Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. Journal of Marine Science and Engineering, 8(10), 776.
2. Glaser, B., & Strauss, A. (2017). Discovery of grounded theory: Strategies for qualitative research. Routledge.
3. IMO (International Maritime Organization). (2024). "Maritime Cyber Risk" Retrieved from [IMO Website]:
4. https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx
5. Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. International Journal of Critical Infrastructure Protection, 37, 100526.