UNIVERSITY OF TURKU

Enhancing Cybersecurity in Finnish Cruise Shipbuilding: Meyer Turku's Digital and Operational Resilience

Mechanical Engineering

Master's Thesis in Engineering and Technology

Faculty of Technology

Author:

Ville Lähde

06.03.2025

Turku

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin Originality Check service.

Master's thesis

Subject:
Author(s): Ville Lähde
Title: Enhancing Cybersecurity in Finnish Cruise Shipbuilding: Meyer Turku's Digital and Operational Resilience
Supervisors: Prof. Ville Leppänen, Dr. Anne-Maarit Majanoja, Prof. Jussi Kantola
Number of pages: 107 pages
Date: 06.03.2025

Abstract

This thesis examines cybersecurity in the Finnish shipbuilding industry, focusing on Meyer Turku and its cruise ship outfitting process. It explores key cybersecurity challenges such as unauthorized access, data breaches, and the growing complexity of digital systems in shipbuilding. The study applies the CIA triad principles (Confidentiality, Integrity, and Availability) to assess their role in securing both digital and physical operations at the shipyard.

The significance of this research lies in the rapidly evolving cybersecurity landscape of the maritime industry where the protection of sensitive design, operational, and contractual data is critical for operational efficiency, maintaining customer trust and regulatory compliance. Stakeholder management, including the roles of subcontractors and turnkey contractors, is highlighted as a key part in addressing cybersecurity risks.

A mixed-methods survey was conducted to understand how Meyer Turku employees and external stakeholders perceive cybersecurity, their awareness levels, and existing challenges. The results highlight gaps in cybersecurity training and differences in stakeholder priorities, offering insights into areas needing improvement. Based on these findings, the study proposes practical recommendations such as role-based training, secure data-sharing protocols, and collaborative audits. These measures aim to strengthen cybersecurity strategies within Meyer Turku’s stakeholder network while contributing to broader discussions on maritime cybersecurity resilience.

Keywords: Cybersecurity, Shipbuilding, Risk Management, Maritime Industry, Meyer Turku, CIA Triad, Digital Security, Stakeholder Management, Cruise Ship Outfitting, Data Protection, Cybersecurity Awareness, Maritime Regulations, IACS UR E26, Digital Resilience, Supply Chain Security, Subcontractor Collaboration, External Stakeholder Collaboration, Cyber Threat Mitigation, Secure-by-Design, Cyber Risk Assessment, Compliance Strategies, Industrial Control Systems (ICS) Security, Operational Technology (OT) Security, Compliance Strategies

Contents

1 Introduction

The shipbuilding industry, particularly in the construction of cruise ships, is undergoing a significant digital transformation. This transformation is driven by the need for efficiency, sustainability, and the ability to meet the high standards set by large ship owners like Royal Caribbean Cruise Lines. While these advancements offer operational benefits, they also introduce a host of cybersecurity challenges. Although there is a lack of specific literature on Finnish shipbuilding cybersecurity regulations, this thesis aims to provide an understanding of general cybersecurity practices in shipbuilding and their applicability to the Finnish context, specifically at Meyer Turku shipyard. This thesis pays particular attention to the outfitting process of cruise ships and covers key areas such as cybersecurity threats, risk management, and stakeholder cooperation.

The motivation behind the thesis is to study what is required in implementing new security systems for cruise ship building shipyards and to contribute to development of the security of the Finnish shipbuilding processes. Recent global events have shown the increasing importance for solid and trustworthy security processes and techniques, including cybersecurity.

In the context of this research, the novelty lies in the application of cybersecurity techniques to the specific challenges faced by the shipbuilding industry. Meyer Turku Shipyard will act as the focus point. While general cybersecurity principles like the CIA triad (Confidentiality, Integrity, Availability) are well-established, their application in the unique environment of a shipyard with its own set of stakeholders, physical and digital threats, and complex supply chains remains as an almost underexplored area. Therefore, this research aims to fill this gap by finding cybersecurity development suggestions to the specific needs and challenges of shipbuilding industry. Thereby contributing a novel perspective to the existing body of academic research. Especially in the context of rapidly evolving technologies and emerging threats, it is important to further advance knowledge and the develop effective solutions to real-world problems. In the realm of cybersecurity, this is particularly true given the changing landscape of cyber threats and vulnerabilities.

1.1 Research approach

The research approach of this thesis is a mixed-methods approach, combining quantitative and qualitative research methods. The goal is to provide an understanding of cybersecurity challenges in the Finnish shipbuilding industry, focusing on Meyer Turku shipyard. This approach enables both numerical data analysis and exploration of stakeholder perceptions and industry implications. Quantitative analysis provides objective and measurable insights into cybersecurity awareness and risk perception across different stakeholders. Qualitative analysis enables a deeper understanding of

stakeholder concerns, motivations, and industry-specific cybersecurity challenges. By using this research approach, the study provides both data-driven conclusions and contextual interpretations.

The quantitative approach involved conducting a survey to assess cybersecurity awareness, stakeholder perceptions, and perceived threats at Meyer Turku. The collected survey data was then analysed using statistical methods to identify trends, correlations, and differences between various stakeholder groups.

In the qualitative research, a literature review was carried out to explore existing studies on maritime cybersecurity, industry regulations, and best practices such as IACS UR E26 (International Association of Classification Societies, Unified Requirement, Electrical requirement number 26) and the CIA security principles. Additionally, open-ended survey responses were examined to gain deeper insights into individual experiences and opinions on cybersecurity at Meyer Turku.

The thesis is guided by the following research questions:

RQ1. How does the IACS UR E26 impact Finnish shipbuilding? - Investigates regulatory changes, compliance requirements, and industry adaptation.

RQ2. What types of cybersecurity threats does Meyer Turku face? - Identifies and categorizes digital and physical security risks within the shipyard.

RQ3. How do Meyer Turku employees and stakeholders perceive the security of digital and physical resources within the shipyard? - Examines confidence levels, concerns, and perceived vulnerabilities in shipyard operations.

RQ4. What level of cybersecurity awareness exists among Meyer Turku employees and stakeholders, and how do they perceive the importance of cybersecurity in shipyard operations? - Studies familiarity with cybersecurity principles and evaluates attitudes toward cybersecurity.

RQ5. How do different stakeholder groups differ in their perceptions of cybersecurity threats and priorities? - Analyses variations in cybersecurity awareness, concerns, and priorities across different groups within the shipyard ecosystem.

1.2 Organisational structure of Meyer Turku Outfitting

The organizational structure of a shipyard is designed to simplify complex operations. The goal is to ensure efficient management of production and design processes. Centralized under Project Management, the key operational areas include Design and Engineering, Hull Production, and Outfitting. Each division has its own part in the whole shipbuilding process and operation of the

shipyard. The process includes all tasks from concept design to production and final delivery of vessels, and guarantee period processes.

Outfitting plays a critical role as it connects the transition between structural completion and the operational readiness of the vessel. The Outfitting department coordinates with adjacent and earlier Production Departments and Detail Design Teams, ensuring that equipment, systems, and interior components are installed accordingly to rules and specifications. Its position within the organizational structure, as highlighted in the diagram (Figure 1), is to show that this thesis focuses on the Outfitting Department and its direct connections with Production Departments and Detail Design.

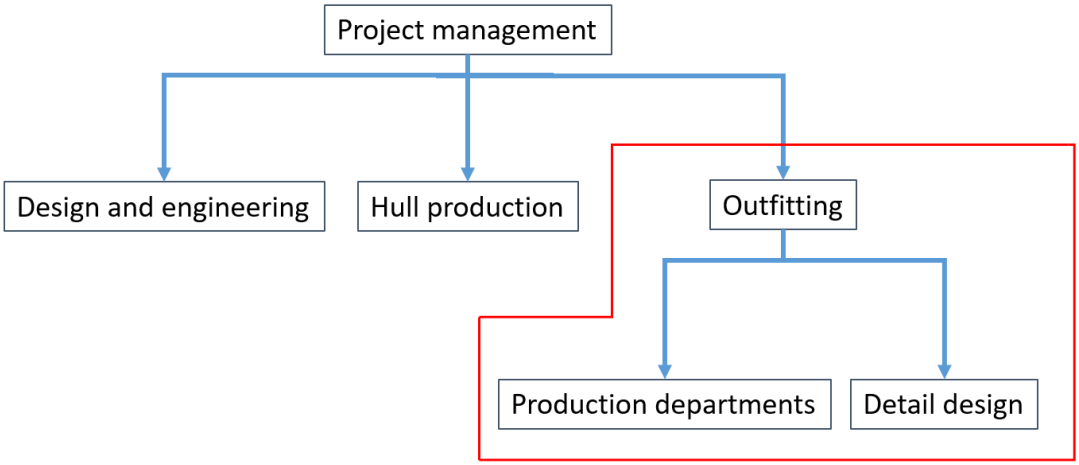


Figure 1 Organisational structure of Meyer Turku Outfitting

A significant portion of outfitting production and design is executed by Turnkey Contractors and specialized Subcontractors. These external stakeholders are responsible for delivering fully functional systems or modules, ranging from electrical and mechanical installations to interior outfitting and equipment implementation. The Turnkey Contractors focus on core structural and direct production project management tasks, which is largely associated with Finnish shipbuilding.

The use of Turnkey contractors ensures smooth workflow between production and detail design as they come as a one united package contract for individual areas in the vessels being built. Turnkey contractors especially coordinate closely with further external partners to ensure that their contract delivery is up to rules and ship specification. While this outsourcing model enhances flexibility and allows shipyards to leverage advanced technologies, it also introduces additional challenges in terms of coordination, communication, and cybersecurity.

1.3 Interior Outfitting Process

The first step involves understanding the requirements and expectations for the interior and public spaces. This includes the number of rooms, types of public areas, and any special features like theatres, pools, or restaurants.

The outfitting process begins from concept design that is made based of needs and concepts of the ship owner to visualize the spaces. These are often done in collaboration with interior designers and architects. After the concept design follows basic design and 3D-modelling of the areas. After comes detailed architectural designs and development of engineering plans. These plans include specifics like materials, dimensions, and technical specifications. The phase of basic design works as the foundation of detail design. All the basic design and detail design are presented to different authoritative stakeholders for approval. This includes the ship owner, usually a large cruise line, and any other parties like the class society involved in the project. The plans are reviewed to ensure they comply with maritime safety and other regulations. The detail design is then implemented during construction onsite the cruise ship.

Prior to actual design and construction subcontractor and turnkey procurement is performed. This usually goes hand in hand with material procurement. Materials, systems and companies are approved for the project. In Meyer Turku shipyard the interior spaces are built with a Turnkey concept where the ship is divided into areas that have usually one main contractor for the specific area in question. That turnkey company will then design, construct and handover the area after completion of the project. Detail design is often subcontracted and passes through many stakeholders in interior outfitting before, during and after area building inside a cruise ship construction.

Mechanical, electrical, and plumbing (MEP) systems installation including electrical wiring, plumbing lines, and heating, ventilation and air conditioning (HVAC) systems are part of the turnkey scope. After the structural and MEP work is complete, the interior finishing begins. This includes installing fixtures, painting, laying flooring, and so on. Furniture, lighting, and other amenities are added to the spaces. In public areas, this could also include installing things like bars, stages, or swimming pools.

Stakeholder approval follows throughout the way of the whole process from concept design to competition of the construction. Rigorous inspections are carried out to ensure that all work meets the specified standards and complies with regulations. After competition, only after everything is approved, the spaces are officially handed over to the ship owner, and the ship is ready for delivery.

The resources that require protection with cybersecurity measures during the outfitting process include contracts, specifications, basic design diagrams, design drawings, CAD files, 3D-models, certificates,

weight calculations, electrical and cabling data, system and product information and multitude of other miscellaneous confidential documentations including correspondence with stakeholders.

The outfitting process is also an important phase for building the vessel's cybersecurity infrastructure. During this stage, critical systems and networks that support the ship's cyber defences are installed and integrated into its overall design. These include physical components such as cabling, network hardware, and communication systems, as well as software for monitoring, intrusion detection, and system authentication.

As outfitting progresses, cybersecurity becomes a core part of the ship's operational setup. Key systems like navigation equipment, engine management software, and onboard IoT (Internet of Things) devices are installed and connected, creating the vessel's digital environment. To ensure this environment is secure, it must be built with secure-by-design principles, including measures like data encryption, network segmentation, and strict access controls.

The outfitting phase is not just about installing operational systems but also about creating a secure digital foundation for the ship. If cybersecurity is overlooked during this process, vulnerabilities can become part of the ship's infrastructure, putting its safety, reliability, and compliance with maritime cybersecurity regulations at risk. By focusing cybersecurity measures during outfitting, shipyards can ensure the vessel is well-protected against evolving cyber threats in the maritime industry.

1.4 Stakeholder management

Meyer Turku's complex stakeholder environment includes turnkey companies, subcontractors, partnership companies, and large ship owners. Effective stakeholder management is important in the shipbuilding industry, particularly concerning cybersecurity. The integration of advanced digital technologies in shipbuilding has heightened the importance of robust cybersecurity measures to protect sensitive data and ensure operational integrity. Proactively involving stakeholders such as shipbuilders, system integrators, and shipping companies ensures cybersecurity is embedded at every stage, from design to operation, reducing risks from digitalization. (WAGO, 2024).

Furthermore, the concept of "cybersecurity by design" emphasizes the importance of incorporating security measures during the initial stages of ship design and construction. This approach involves analysing and selecting systems from a cybersecurity perspective, ensuring their proper integration and commissioning. By involving all relevant stakeholders, such as shipowners, shipyards, integrators, suppliers, certifiers, and external consultants, early in the process, the industry can address vulnerabilities that could compromise the confidentiality, integrity, or availability of critical data and systems (Aeromarine Cybersecurity, 2024).

Recent reports indicate a significant increase in cyber-attacks within the maritime sector, underscoring the need for heightened awareness and investment in cybersecurity. A survey highlighted that 31% of maritime professionals reported at least one cyber-attack in the 12 months leading up to October 2024, up from 17% over the previous five years. This trend has prompted stakeholders across the industry to enhance their cybersecurity measures, recognizing the critical role of stakeholder collaboration in protecting assets and operations (DNV, 2024).

In summary, effective stakeholder management in shipbuilding necessitates a collaborative approach to cybersecurity, integrating security considerations from the design phase through to daily operations. By doing so, the industry can better protect against the evolving cyber threats that accompany increased digitalization.

1.5 Structure of the Thesis

The study is designed to first establish a theoretical foundation, followed by an examination of industry challenges, an explanation of the research methodology, and finally, an analysis of the survey results leading to concrete development suggestions and conclusions.

The research begins with Chapter 2, which explores the cybersecurity threat landscape in shipbuilding. This chapter establishes the theoretical foundation by discussing key cybersecurity concepts, including the CIA triad (Confidentiality, Integrity, and Availability), and how these principles apply to the shipbuilding phase. It highlights how cybersecurity threats in shipbuilding differ from those encountered during a vessel's operational life. Understanding these threats is crucial for assessing the risks and vulnerabilities present during the construction process, making this chapter a background section for the analysis that follows.

Chapter 3 builds on the theoretical framework by addressing Research Question 1 (RQ1). This chapter focuses on the regulatory landscape, particularly the implications of the IACS UR E26 cybersecurity requirement for shipyards. It examines how the industry must adapt to comply with evolving regulations and highlights both challenges and opportunities that these new cybersecurity requirements introduce.

Following the exploration of theoretical and regulatory aspects, Chapter 4 details the research methodology. The study uses a mixed-methods approach, combining quantitative and qualitative methods to assess cybersecurity awareness, perceptions, and practices at Meyer Turku. This chapter explains how the survey was designed, conducted, and analysed, highlighting the research process. The methodological approach serves as the base for analysing stakeholder perspectives on cybersecurity in shipbuilding.

The core findings of the study are presented in Chapter 5, which addresses Research Questions 2–5 (RQ2–RQ5). This chapter analyses the survey results, providing insights into the current state of cybersecurity awareness, the perceived importance of cybersecurity, and differences in cybersecurity concerns across various stakeholder groups. The chapter highlights key findings related to cybersecurity training gaps, resource protection priorities, and areas where stakeholder collaboration could be improved. The analysis culminates in development suggestions, offering concrete recommendations for strengthening cybersecurity measures at Meyer Turku.

Finally, Chapter 6 presents the conclusion, summarizing the study's key findings and reflecting on the broader implications for cybersecurity in shipbuilding. This chapter consolidates the research contributions, discusses the practical significance of the findings, and identifies potential areas for future research.

The logic of the thesis structure is to move from theory and literature to research methods and data collection. From there to presenting the results and analysis. At the end if the thesis presents the conclusions and implications. The goal of this structure is to explore cybersecurity in Finnish shipbuilding by first establishing the necessary background and research framework before presenting findings and recommendations. The approach takes after the broader academic practice of moving from theory to practical analysis, ensuring clarity and depth in addressing cybersecurity challenges in the shipyard environment.

2 Cybersecurity threats in shipbuilding

The shipbuilding industry presents unique cybersecurity challenges that can differ from those in land-based construction or the operational phase of a ship's lifecycle. Unlike land construction, shipbuilding involves extensive collaboration among numerous stakeholders, such as subcontractors, turnkey contractors, and external partners, making it highly susceptible to cybersecurity threats. Furthermore, the nature of these threats often crosses the shipyard. Vulnerabilities introduced during construction potentially become security risks during the operational life of the vessel.

This chapter explores the CIA triad (Confidentiality, Integrity, and Availability) in shipbuilding and examines the cybersecurity threats specific to the shipbuilding phase, with a focus on Meyer Turku. By analyzing both theoretical frameworks, such as the CIA triad, and practical examples of digital threats, this chapter highlights the vulnerabilities inherent in shipbuilding.

2.1 CIA: confidentiality, integrity, availability

The CIA triad (Confidentiality, Integrity, and Availability) serves as the foundation for information security and risk management in industrial environments (NCCoE, 2019). In shipbuilding this model takes on particular importance, as security breaches can affect not only digital assets but also physical operations, intellectual property, and supply chain integrity. Meyer Turku, one of Finland’s leading shipbuilders, is part of a rapidly digitizing maritime industry. The use of advanced digital and operational technologies improves efficiency but also increases the risk of cyber threats by creating more potential entry points for attacks. The introduction of automated manufacturing systems, digital supply chain management, and cloud-based collaboration platforms increases the risk of data leaks, system manipulation, and operational disruptions. The CIA triad provides a structured approach to mitigating these risks, ensuring that shipbuilding operations remain secure and resilient (Maritime Executive, 2024). As shipbuilding companies adapt to regulations such as IACS UR E26, cybersecurity must be embedded into ship design, production, and supply chain management (Bureau Veritas, 2023).

Confidentiality in shipbuilding cybersecurity refers to the protection of sensitive data, intellectual property, and operational information from unauthorized access. Shipyards manage large amounts of proprietary data, including CAD designs, material procurement lists, client contracts, and regulatory compliance documents. A breach of confidentiality could expose Meyer Turku to corporate espionage, legal liabilities, and loss of competitive advantage. Cybersecurity threats such as phishing attacks, insider leaks, and supply chain vulnerabilities have increasingly targeted the shipbuilding industry. A notable example is the 2016 data breach involving the U.S. Navy, where a contractor’s compromised laptop led to the exposure of personal data for over 134,000 sailors. This incident underscores the risks

associated with third-party access and subcontractor vulnerabilities that could lead to issues when ships enter operation after delivery (USNI News, 2016). Similarly, the 2023 cyberattack on Huntington Ingalls Industries, which resulted in leaked sensitive shipbuilding data, highlights the potential consequences of inadequate supply chain security (ClearanceJobs, 2023).

To safeguard confidentiality, shipyards must adopt strong access control mechanisms, data encryption, and secure communication channels. Implementing Role-Based Access Control (RBAC) ensures that employees and subcontractors can only access information relevant to their specific roles, reducing the risk of unauthorized exposure. Data encryption both in storage and transmission prevents interception and unauthorized access to sensitive information. Conducting regular third-party security assessments strengthens supply chain resilience, ensuring that subcontractors and vendors adhere to cybersecurity standards. Without these measures, breaches in confidentiality could compromise not only shipyard operations but also national security in the case of naval or government-affiliated shipbuilding projects (IBM, 2024).

Integrity within the CIA triad ensures that data and systems remain accurate, consistent, and reliable. In shipbuilding compromised data integrity can lead to severe operational and safety risks. Unauthorized modifications to engineering blueprints, procurement records, or digital control systems could result in defective ship components, incorrect material usage, or structural failures. Cyber threats such as malware, ransomware, and insider sabotage pose a significant risk to integrity. A real-world example is the 2023 ransomware attack on Fincantieri Marinette Marine, which encrypted critical shipbuilding files, leading to significant operational delays and data loss (ClearanceJobs, 2023). Such incidents emphasize the need for tight cybersecurity measures to ensure data remains unaltered and trustworthy.

Maintaining integrity in shipbuilding operations requires a multi-layered approach. Digital signatures and cryptographic hashing provide verification mechanisms to detect unauthorized changes in critical documents and software systems. Version control systems for CAD designs and procurement logs ensure that any modifications are documented and traceable. Regular cybersecurity audits, combined with automated monitoring systems, help detect anomalies in data and prevent malicious alterations. Additionally, secure backup strategies must be implemented to allow rapid restoration of accurate data in the event of ransomware attacks or accidental corruption. The consequences of integrity failures in shipbuilding are not limited to financial losses but extend to safety hazards and potential regulatory non-compliance, making it imperative for shipyards to incorporate integrity-focused cybersecurity practices (Digital WarRoom, 2024).

Availability is the third pillar of the CIA triad, ensuring that critical systems, data, and infrastructure remain accessible to authorized users when needed. In shipbuilding any disruption in availability can lead to significant financial losses, production delays, and reputational damage. Digital shipbuilding

processes rely on ERP (Enterprise Resource Planning) systems, supply chain management platforms, and industrial control systems to coordinate operations (NCCoE, 2020). A cyberattack that compromises availability, such as a Distributed Denial of Service (DDoS) attack or ransomware incident, could halt production and disrupt supply chains. In 2022, a European shipyard faced a severe ransomware attack that locked engineers out of their ERP systems for over a week, delaying a high-value cruise ship project (Security Week, 2022).

Ensuring availability requires a combination of redundancy planning, proactive threat mitigation, and disaster recovery strategies. Implementing failover systems and redundant network architectures ensures that critical shipyard operations can continue even if primary systems are compromised. Regular cloud-based backups protect against data loss, allowing rapid recovery after cyber incidents. Cyber resilience drills and penetration testing help identify weaknesses in infrastructure, ensuring that security teams are prepared to respond to potential disruptions (Unitrends, 2023). By integrating availability focused cybersecurity measures into daily operations, shipyards can better their resilience against both targeted cyberattacks and unforeseen technical failures.

In shipbuilding, the CIA triad extends beyond traditional IT security to encompass cyber-physical systems, supply chain management, and industrial automation. Confidentiality ensures that sensitive ship designs and intellectual property remain protected, integrity guarantees the accuracy and reliability of operational data, and availability safeguards the uninterrupted functionality of shipbuilding processes. For Meyer Turku, a cybersecurity strategy following the CIA triad is essential for maintaining its competitive edge, protecting stakeholder trust, and ensuring compliance with international regulations such as IACS UR E26. The maritime industry's increasing reliance on digital technologies necessitates a proactive approach to cybersecurity, with continuous adaptation to emerging threats and evolving regulatory landscapes.

2.2 Digital threats

In today's interconnected world, digital threats have become increasingly sophisticated. This poses significant risks to various sectors, including the shipbuilding industry. Meyer Turku, like other industrial companies, faces a multitude of digital threats, including malware attacks, data breaches, phishing attempts, Internet of Things (IoT) vulnerabilities, and deep learning vulnerabilities.

Malicious software, or malware, is designed to infiltrate or damage computer systems causing a threat to integrity. In shipbuilding, malware can disrupt critical software systems used in design and construction, leading to delays and financial losses. For instance, ransomware attacks threat availability for example by locking down navigation systems or access to digital logs, disrupting maritime operations (Darktrace, n.d.).

Unauthorized access to sensitive data, such as ship designs and customer information, can have severe repercussions, including legal consequences and loss of reputation. The increasing digitization of ships and the use of internet devices have opened new vulnerabilities, making the industry more vulnerable to such breaches (Financial Times, 2024).

Phishing involves tricking individuals into revealing sensitive information through deceptive emails or messages. Employees may be targeted through phishing emails that can compromise internal networks if not properly managed. These attacks can lead to unauthorized access to the ship's systems and sensitive data (Darktrace, n.d.).

The increasing use of IoT devices in shipbuilding introduces significant security challenges. These devices often lack strong security features, making them susceptible to cyber-attacks. For instance, vulnerabilities in IoT devices can be exploited by cybercriminals to gain unauthorized access to connected networks, compromising critical data and systems (Fortinet, n.d.).

In the context of shipbuilding, the adoption of Industry 4.0 technologies such as IoT, sensors, and data analytics, has enhanced operational efficiency but also increased susceptibility to digital threats like data breaches and unauthorized access. Because these technologies are connected, they can give attackers more ways to access systems if security is weak. (Cyber Consultancy, n.d.).

While many cybersecurity concerns in shipbuilding pertain to the construction process, it is important to recognize that IoT vulnerabilities can also affect the operational phase of ships. Ensuring the cybersecurity of IoT devices during both construction and operation is crucial for maintaining the overall security and resilience of maritime vessels.

The application of artificial intelligence, particularly deep learning, holds great promise for enhancing cybersecurity. However, these technologies also present new types of cyber threats that have not been systematically examined in previous surveys. Adversaries can exploit vulnerabilities in deep learning models, leading to potential security breaches (Ruan et al., 2023).

2.3 Physical threats

The open environment of Meyer Turku shipyard, which allows relatively free movement, increases the risk of unauthorized physical access to sensitive areas. This is particularly concerning given the large number of stakeholders involved, such as turnkey companies, subcontractors, and partnership companies (Melnyk et al., 2023). As much attention is often given to digital threats such as malware, phishing, and data breaches, physical threats are equally critical if not some of the root causes for accessing digital resources in need of protection. Physical threats can have devastating consequences, especially in complex environments like shipyards where cruise ships are constructed. Types of physical threats can be unauthorized access, sabotage, theft and social engineering.

Unauthorized access in open environments like shipyards poses significant risks, including the potential for unauthorized individuals to gain physical access to critical areas. This threat encompasses both external intruders and internal actors. Those could be such as employees who may either have malicious intent or be careless with their access credentials. The implications of unauthorized access are extensive, affecting not only data integrity but also the safety of personnel and the entire shipbuilding process. Consequences can include sabotage, theft, or even espionage. Deliberate acts of sabotage can cause physical damage to hardware systems, disrupt operations, and lead to financial losses. The theft of critical hardware, such as servers or specialized machinery, can also result in financial loss and compromise the security of the entire system (Dunlevie, 2023).

Physical threats often involve social engineering tactics, where individuals manipulate employees to gain unauthorized access to secure areas or information (Yamout et al., 2023). These attacks often exploit human psychology rather than technological vulnerabilities. In a shipyard environment, this could mean tricking employees into revealing secure access codes or leaving secure areas unlocked. Social engineering attacks are particularly challenging to defend against because they exploit human vulnerabilities. These attacks can be highly targeted and may involve extensive research on the employees being targeted. In a shipyard, where there is a mix of permanent staff and temporary contractors, the risk is even higher.

Physical infrastructure, such as power supplies and network cables, can be targeted to disrupt operations. These vulnerabilities can have real-world consequences and can be detrimental to both human and environmental security (Safitra et al., 2023). The physical infrastructure is often the backbone of any organization, and its security is paramount. In a shipyard, this can include not just the IT infrastructure but also the machinery and equipment used in shipbuilding.

3 The Impact of IACS UR E26 on Finnish Shipbuilding

The introduction of the International Association of Classification Societies' (IACS) Unified Requirement E26 (UR E26) represents a major regulatory shift in the maritime industry, particularly for Finnish shipbuilders such as Meyer Turku. This chapter directly addresses Research Question 1 (RQ1): How does the IACS UR E26 impact Finnish shipbuilding? by analysing its technological, regulatory, and operational consequences. As UR E26 applies to ships contracted for construction on or after January 2024, Finnish shipbuilders must adapt their cybersecurity frameworks, supply chain security, and compliance strategies to align with these new industry standards. This chapter explores these aspects, illustrating how Finnish shipyards should be responding to UR E26 and what challenges and opportunities the regulation presents for the industry.

Finnish shipbuilding companies, especially Meyer Turku, operate in a specialized industry focused on quality, innovation, and strict compliance with national and international regulations. As modern ships become more digitally advanced and interconnected, new cybersecurity risks emerge during construction. These risks are different from those faced when a ship is in operation, but if not properly managed, they can carry over and create security issues throughout the ship’s lifecycle.

This chapter examines how Finnish shipbuilders must adapt to UR E26, focusing on the regulatory, technological, and operational implications. Key themes include the alignment of shipbuilding practices with cybersecurity requirements, the investment needed in technologies and workforce training, and the long-term benefits of compliance. By addressing these issues, this chapter highlights how Finnish shipbuilders can navigate this regulatory change to ensure both compliance and competitive advantage in the global maritime industry.

The maritime industry is increasingly becoming digitized, with ships now featuring complex computer-based systems for navigation, control, and other critical functions. This digital transformation, while beneficial in many ways, also opens new vulnerabilities. The vulnerabilities are visible particularly in the realm of cybersecurity. Recognizing this, the International Association of Classification Societies (IACS) has introduced new Unified Requirements, including UR E26, aimed at enhancing the cyber resilience of ships (ABS Group, 2023).

The UR E26 sub-goals

- Identify: Manage cybersecurity risk to onboard systems, people, assets, data, and capabilities.
- Protect: Implement safeguards against cyber incidents.
- Detect: Measures to detect and identify the occurrence of a cyber incident onboard.

- Respond: Act regarding a detected cyber incident onboard.
- Recover: Restore capabilities or services necessary for shipping operations that were impaired due to a cyber incident (ABS Group, 2023).

Finnish shipbuilding companies have a long history of innovation and quality. The country is home to some of the world's leading shipyards and maritime technology companies (Trusted Docks, n.d.). Finnish shipbuilding is renowned for its advanced ship designs and technological expertise, with a strong emphasis on sustainability and safety (Forum Marinum, n.d.). However, the introduction of IACS UR E26 poses unique challenges for these companies, given the already complex regulatory landscape in the European Union and the high standards of quality that Finnish shipbuilders are known for (IACS, 2024).

For Finnish shipbuilders, strategic investments in cybersecurity will be crucial. Companies will need to allocate resources not just for compliance but also for ongoing monitoring and management of cyber risks. This could include investments in advanced security software, specialized personnel, and continuous training programs. While these investments will increase operational costs, they are essential for long-term sustainability and competitiveness (DNV GL, 2022).

Given the complexity and evolving nature of cyber threats, collaboration between industry stakeholders and governmental agencies will be vital. Finnish shipbuilders could benefit from public-private partnerships that facilitate knowledge sharing, research, and development of best practices in maritime cybersecurity. Such collaborative efforts could also lead to the development of standardized protocols and guidelines that are more aligned with the needs and capabilities of the industry (Bureau Veritas, 2023).

The implementation of UR E26 will also have implications for supply chain management. Shipbuilders will need to ensure that all components and systems integrated into the ships are compliant with cybersecurity requirements. This could necessitate changes in supplier contracts and quality assurance processes. Companies may also need to conduct regular audits of their suppliers to ensure compliance (DNV GL, 2022).

UR E26 introduces both challenges and opportunities for Finnish shipbuilding. Compliance requires significant financial investment, operational restructuring, and the implementation of cybersecurity policies and training programs across the industry. Ensuring that shipbuilders, subcontractors, and other stakeholders meet these requirements can be resource-intensive and may disrupt existing workflows. However, despite these challenges, UR E26 provides a structured framework for strengthening cybersecurity resilience and improving risk management. By embedding cybersecurity measures into ship design, production, and supply chain security, Finnish shipbuilders can not only

reduce exposure to cyber threats but also enhance regulatory trust and international competitiveness. Those who successfully integrate UR E26-compliant cybersecurity practices may gain a strategic advantage in global markets, where secure and resilient shipbuilding is becoming an increasingly critical selection criterion. The demand for ships with robust cyber resilience features is only expected to grow, offering significant economic opportunities for those who can deliver on these requirements (Offshore Energy, 2023).

3.1 Technological Challenges

To understand how IACS UR E26 impacts Finnish shipbuilding (RQ1), it is necessary to evaluate the technological challenges it introduces. UR E26 requires Finnish shipyards, including Meyer Turku, to enhance cybersecurity for both IT and OT systems.

Modern ships have evolved into complex systems integrated with advanced technologies for navigation, communication, and operation. This integration enhances operational efficiency but also increases the attack surface for potential cyber threats, making it challenging to secure every component effectively. The maritime industry's increased connectivity through satellite communications, onboard systems, and shore-based operations creates numerous entry points for cybercriminals. Common threats include malware, phishing, and unauthorized access to critical systems (MarineLink, 2024).

The adoption of Information and Communications Technology (ICT) in the shipping industry has led to an explosion of cyber risks. Systems such as navigation, communication, and control are interconnected, each with its own set of vulnerabilities. For instance, the Automatic Identification System (AIS), which is used for vessel tracking, operates without any authentication or integrity checks, making it susceptible to fake messages. This vulnerability can be exploited by attackers to gain unauthorized access or disrupt operations (Trend Micro, 2013).

Addressing these cybersecurity challenges requires a comprehensive approach that includes implementing robust security measures, regular system audits, and continuous monitoring to detect and respond to threats promptly. Additionally, fostering a culture of cybersecurity awareness among crew members and stakeholders is essential to mitigate risks effectively (Mission Secure, n.d.).

Despite the increasing awareness of cyber risks, the maritime industry lacks standardized security protocols. The International Association of Classification Societies (IACS) has issued guidelines for cyber resilience in ship design and construction, but these are not universally adopted (Aeromarine Cybersecurity, 2024). The absence of standardized protocols makes it difficult for shipbuilders to implement effective cybersecurity measures.

The pace of technological advancements in the maritime sector is another challenge. As new technologies are introduced, older systems become obsolete, and their security measures may no longer be effective. This creates a moving target for cybersecurity, requiring constant updates and revisions to security protocols (Maritime Executive, 2024).

The human element is often the weakest link in cybersecurity. Ship operators may lack the training or awareness to follow best practices, making the systems more vulnerable to attacks. A lack of a cybersecurity culture can be beneficial to any attacker that wants to gain access to a vessel and its systems (Atlantic Council, 2022).

3.2 Regulatory Challenges

The maritime industry is subject to a myriad of regulations that vary by jurisdiction. For instance, the EU's Network and Information Systems (NIS) 2.0 Directive, effective from January 2022, mandates EU Member States to implement new cybersecurity laws by October 2024. Similarly, the UK Government has updated its Network and Information Systems Regulations (NIS Regulations) to strengthen cyber risk governance. In the United States, the Securities and Exchange Commission (SEC) is expected to publish new cybersecurity risk management regulations that will affect public maritime organizations (Lexology, 2023).

One of the primary challenges is the complexity involved in complying with multiple sets of regulations. Companies operating across different jurisdictions must navigate a labyrinth of rules, each with its unique requirements and penalties for non-compliance. This complexity can lead to increased operational costs and necessitates specialized legal and technical expertise to manage effectively. The TMF Group's Global Business Complexity Index shows that stricter global compliance laws make doing business harder, as companies must adjust to different rules in each country (TMF Group, 2023). Additionally, Neumetric highlights the challenges of following multiple regulations, stressing how businesses struggle to comply with different rules, which adds to operational complexity (Neumetric, 2023).

The absence of uniform global standards complicates the regulatory landscape. While organizations like the International Association of Classification Societies (IACS) and the International Maritime Organization (IMO) have issued guidelines, these are not universally adopted. The lack of standardization makes it difficult for shipbuilders to develop universally compliant cybersecurity measures (Bureau Veritas, 2023).

Regulatory bodies are increasingly adopting stringent enforcement mechanisms. For example, the EU's NIS 2.0 Directive and the UK's updated NIS Regulations include significant new enforcement measures such as random audits, infringement warnings, service suspensions, and fines. Such punitive

measures put additional pressure on shipbuilding companies to comply but also raise concerns about the fairness and effectiveness of these enforcement mechanisms. The regulatory landscape is continuously evolving, making it challenging for companies to stay updated. For instance, the EU is expected to release a proposed Cyber Resilience Act later this year, and the SEC's new regulations are anticipated to be published mid-2023. These forthcoming regulations add another layer of complexity and uncertainty for shipbuilders (Lexology, 2023).

As IACS UR E26 takes effect, Finnish shipbuilders must bridge gaps between existing cybersecurity measures and the new compliance requirements. The challenge for Finnish yards is not only to meet compliance standards but also to integrate cybersecurity as a core component of the shipbuilding process. This reinforces the impact of UR E26 on the industry and answers RQ1 by demonstrating how Finnish shipbuilders are adjusting to regulatory demands.

3.3 Public Policy and Government Support

Government support and public policy play a crucial role in the development and implementation of cybersecurity measures in the maritime sector. In Finland, this is particularly evident in the case of Meyer Turku, because of the involvement with government contracts. Meyer Turku is currently constructing Offshore Patrol Vessels (OPVs) for the Finnish Border Guard (Janes, 2023). The project not only signifies a strong public-private partnership but also highlights the government's commitment to enhancing maritime security and technological innovation. These vessels are not only commercial projects but are closely aligned with national security objectives, emphasizing the crucial role of public policy in maritime cybersecurity.

The Finnish Customs office has expressed the need for balanced resource allocation among security agencies, including the Border Guard. This stance underscores the importance of government backing for projects like the OPV, which are integral to national security (Yle.fi, 2023). Such support could manifest in various forms, including financial backing, policy frameworks, or even the facilitation of international collaborations.

Moreover, the Finnish Border Guard's involvement in a pilot program for digital passports indicates a willingness to adopt new technologies. This openness to innovation could extend to maritime projects, offering an avenue for the integration of advanced cybersecurity measures into the OPVs (Travel and Leisure, 2023).

On a broader scale, the European Union is co-funding a pilot project for digital travel credentials at Helsinki Airport. This project involves a partnership between Finnair, airport operator Finavia, and the Finnish police. The EU's support for such projects in Finland could potentially extend to maritime

initiatives, thereby providing an additional layer of financial and policy support for the implementation of cybersecurity measures in ships like the OPV (Forbes, 2023).

In the United States, the Department of Homeland Security (DHS) has set a precedent for government involvement in maritime cybersecurity. When a major U.S. port was targeted for a cyber-intrusion, the Coast Guard and DHS's Cybersecurity and Infrastructure Security Agency (CISA) collaborated to mitigate the threat. This example illustrates how inter-agency collaboration can be effective in safeguarding maritime infrastructure and could serve as a model for Finnish authorities (DHS News, 2022). Such collaboration brings together different stakeholders, including government agencies and maritime organizations, to pool resources, expertise, and intelligence. This collective effort can effectively mitigate cyber risks and protect maritime ecosystems. Joint training and real-time exchange of threat intelligence are some of the collaborative measures that enhance cyber resilience. By adopting a similar approach, Finnish authorities can benefit from inter-agency collaboration to safeguard their maritime infrastructure (OrbitsHub, 2023).

Moreover, the U.S. government has released a National Maritime Cybersecurity Plan, which outlines priority actions for the next five years. The plan focuses on defining maritime threats, enhancing threat intelligence, and increasing the cybersecurity workforce in the maritime sector. Finland could consider similar plans, especially for projects that involve government contracts like those with Meyer Turku. Such a plan could focus on establishing global standards, enhancing threat intelligence, and fostering a cybersecurity workforce specifically trained for maritime projects involving national security (Security Week, 2022).

Government support and public policy are pivotal in shaping the cybersecurity landscape in Finnish shipbuilding. The OPV project by Meyer Turku serves as a prime example of how such support can help the integration of advanced cybersecurity measures, thereby enhancing the resilience and operational effectiveness of maritime assets.

As part of Finland's strategic response to UR E26, government contracts, such as the Offshore Patrol Vessels (OPVs) project, incorporate enhanced cybersecurity requirements. This directly supports the industry’s transition toward full UR E26 compliance and highlights how Finnish shipbuilders are adapting to the regulation (RQ1).

3.4 International Collaboration and Information Sharing

As cyber threats transcend national borders, international collaboration in cybersecurity has become increasingly vital. The maritime industry, including shipbuilding, operates within a globally interconnected network where cybersecurity threats, such as ransomware attacks and state-sponsored cyber espionage, can emerge from any part of the world. No single nation or organization can

effectively counter these threats alone; instead, collective efforts are required to share intelligence, best practices, and resources to enhance overall cybersecurity resilience (Tagarev & Yanakiev, 2020).

One approach to strengthening global cybersecurity efforts is through Collaborative Networked Organizations, where entities unite to pool their expertise and resources. Unlike isolated cybersecurity initiatives, these networks prioritize cooperation over competition, fostering a more integrated and effective defence against cyber threats (Tagarev & Yanakiev, 2020). Similarly, understanding cybersecurity governance metaphors can provide valuable insights into how different nations conceptualize and address cybersecurity challenges. By recognizing these varied perspectives, stakeholders can develop collaborative frameworks that resonate across jurisdictions, improving the effectiveness of joint security initiatives (Slupska, 2020).

Some countries have already demonstrated the advantages of international collaboration through national cybersecurity programs. Taiwan, for instance, has implemented comprehensive cybersecurity policies that emphasize cross-border cooperation. These initiatives serve as blueprints for other nations looking to enhance their cybersecurity infrastructure by leveraging international expertise and shared knowledge (Jakubczak & Yau, 2021). Another key aspect of global cooperation lies in the financing and market evolution of cybersecurity. In Romania, for example, financial investment has been identified as a crucial factor in strengthening the cybersecurity sector. International partnerships can help allocate resources where they are most needed, ensuring that nations with emerging cybersecurity frameworks receive adequate support to enhance their resilience against cyber threats (Danțiș, 2022).

In addition to financial and technical support, legal frameworks for collaboration play an essential role in structuring global cybersecurity efforts. The United Nations Internet Governance Forum (IGF) has emphasized the importance of adaptable legal mechanisms that facilitate cross-border cooperation. Discussions at the IGF have highlighted the need for dynamic regulations that align cybersecurity policies with international law, ensuring that countries can work together efficiently while respecting national sovereignty (Satola & Judy, 2011). As part of this effort, the IGF serves as a platform where policymakers, private sector leaders, and cybersecurity professionals can collaborate on establishing global cybersecurity norms (IGF, 2023).

For Finnish shipbuilders, international collaboration is particularly significant in ensuring alignment with IACS UR E26 requirements. Since compliance with these cybersecurity standards extends beyond national borders, shipyards like Meyer Turku must actively engage in global cybersecurity initiatives. By joining these collaborations, Finland’s shipbuilding industry can improve regulatory compliance, strengthen cybersecurity, and secure its place in the global maritime sector. As cyber threats evolve, sharing intelligence, aligning regulations, and investing in joint security efforts will be key to protecting shipbuilding operations from new risks (RQ1).

3.5 Ethical Considerations in Maritime Cybersecurity

Ethical considerations in maritime cybersecurity are becoming increasingly important, especially with the growing integration of advanced technologies like AI and machine learning into ship systems. These technologies, while enhancing capabilities, also raise questions about data privacy and consent (VentureBeat, 2023). In the European context, particularly in Finland, the role of compliance officers is crucial. They ensure that ethical considerations are integrated into cybersecurity strategies, especially as AI systems become more prevalent in maritime operations (DarkReading, 2023).

Moreover, the ethical dimensions of cybersecurity extend to the nature and quality of the data used for threat detection and response. Inaccurate or biased data can lead to ethical dilemmas, affecting the effectiveness of cybersecurity measures (Forbes, 2023). Ethical considerations also extend to the workforce, as employees must be trained not only in how to defend against cyber threats but also in the ethical implications of their actions. This is particularly important in an industry where a single mistake can have significant safety and environmental consequences (Oruc, 2022).

One of the primary ethical considerations is data privacy. With the implementation of cybersecurity measures, a significant amount of data is collected and analyzed. The European General Data Protection Regulation (GDPR) sets strict guidelines for data collection and usage. Finnish shipbuilding companies must ensure that they are not only compliant with these regulations but also transparent about how data is used and protected (DLA Piper, 2023) (IT Governance, 2018). Transparency in how cybersecurity measures are implemented and managed is crucial. This is especially important in public-private partnerships, where public funds and resources are involved. There must be clear accountability mechanisms in place to ensure that ethical standards are met (European Parliament, 2019). Cybersecurity measures should not infringe upon basic human rights, such as the right to privacy and freedom of expression. This is relevant given the European Union's focus on human rights and Finland's commitment to these principles (Global Partners Digital, 2015).

Another primary ethical consideration in maritime cybersecurity is the use of ethical hacking and penetration testing. While penetration testing is essential for identifying vulnerabilities, it must be conducted responsibly and transparently to avoid legal and ethical mistakes. In the maritime sector, ethical hacking is increasingly recognized as a necessary security measure, ensuring that shipboard systems can withstand real-world cyberattacks. Many shipbuilders, also Meyer Turku, are beginning to integrate controlled penetration testing into their cybersecurity risk management strategies, ensuring compliance with both UR E26 and broader industry best practices. However, strict oversight is required to ensure that these activities align with legal frameworks such as the GDPR and international maritime cybersecurity standards (DNV, 2024).

Corporate Social Responsibility (CSR) extends to cybersecurity as well. Companies have an ethical obligation to protect not just their assets but also the data and privacy of their clients and the general public. In the context of public-private partnerships, both parties should be committed to ethical practices that extend beyond mere legal compliance (Moody's, 2024).

By considering ethical aspects, Finnish shipbuilding companies can ensure that their cybersecurity measures are effective and ethically sound. It is important and logical for a Finnish shipbuilding company like Meyer Turku to align with both national and European values. Given the complexities involved in maritime cybersecurity, Finnish shipbuilding companies could benefit from establishing an ethics committee focused on cybersecurity. This committee could work in tandem with classification societies to review and approve cybersecurity measures, ensuring they align with ethical guidelines. Additionally, regular ethical audits could be conducted to assess the effectiveness of these measures in real-world scenarios. Such proactive steps would not only enhance cybersecurity effectiveness but also build trust among stakeholders, including the government, clients, and the general public.

3.6 Frameworks and good practices

Frameworks provide a structured approach to managing cybersecurity risks. They offer a set of guidelines and best practices that organizations can adapt to their specific needs. While there are general frameworks for cybersecurity, the maritime industry, given its unique challenges, can benefit from specialized frameworks. The Department of Homeland Security, for example, has been working on frameworks that include maritime cybersecurity (Johnson, 2014). Examples of well-known cybersecurity frameworks include the NIST Cybersecurity Framework (National Institute of Standards and Technology), which focuses on Identify, Protect, Detect, Respond, and Recover, and ISO/IEC 27001, which is an international standard for Information Security Management Systems (ISMS) (IT Governance, 2022).

Good practices in cybersecurity can be guidelines or recommendations aimed at optimizing the security posture of an organization. These can range from simple actions like regular software updates and multi-factor authentication (MFA) to more complex procedures like regular security audits and incident response planning. In the maritime industry, best practices often include secure communications between ships and ports, as well as robust data encryption to protect sensitive information (de Peralta et al., 2021). Conducting regular security audits can help identify vulnerabilities and assess the effectiveness of current security measures. For instance, Meyer Turku could engage third-party auditors to evaluate their cybersecurity infrastructure. Implementing MFA can add an extra layer of security, making it more difficult for unauthorized users to gain access to critical systems. Having an incident response plan ensures that in the event of a cyber-attack, the organization can act swiftly to mitigate damage and recover lost data.

In the complex stakeholder environment of Finnish shipbuilding, particularly in settings like Meyer Turku, cybersecurity is not just a technical issue but a governance challenge that involves multiple layers of stakeholders. This complexity gives a need of a strong framework for best practices in cybersecurity. Given the unique challenges in Finnish shipbuilding, companies like Meyer Turku could develop their own customised cybersecurity frameworks that consider the complex stakeholder environment and specific operational needs.

3.7 Future

The maritime industry, with its vast network of ships, ports, and logistics systems, is a critical component of global trade and commerce. The shipbuilding industry is part of that network. As the industry continues to digitize its operations, it becomes increasingly vulnerable to cyber threats. The future of cybersecurity in shipbuilding hinges on understanding these threats and implementing robust measures to counteract them.

A key driver of change in the industry in 2024 is the introduction of IACS UR E26, which represents a significant step forward in enhancing the cyber resilience of ships. This shift toward a more comprehensive approach to ship safety, including cybersecurity, will redefine regulatory compliance and industry standards. For Finnish shipbuilding companies, the new requirement presents both challenges and opportunities. Companies must invest in new technologies and methodologies to meet compliance expectations. Those that successfully adapt will gain a competitive advantage in an increasingly security-conscious global market. Finnish shipbuilders have the potential not only to comply with new regulations but also to establish themselves as leaders in cybersecurity innovation within the maritime sector.

As maritime operations become more interconnected, so do cybersecurity risks. Ships, ports, shipyards and logistics networks are prime targets for cyberattacks due to their reliance on digital technologies. Recent studies emphasize the modern cybersecurity threat landscape in maritime environments, reinforcing the need for proactive and resilient security measures (Lee & Wogan, 2018). Due to the size and complexity of these threats, industry-wide cooperation is critical for strong cybersecurity preparedness.

The future of maritime cybersecurity will depend not only on the adoption of advanced cybersecurity solutions but also on fostering a culture of continuous learning and innovation. Industry-wide cybersecurity education and training will play a critical role in equipping professionals with the skills needed to combat cyber threats. New virtual maritime logistics cybersecurity training platforms are being developed to offer realistic simulations allowing users to experience and respond to cyberattacks in controlled environments (Pyykkö, Kuusijärvi, Noponen, Toivonen, & Hinkka, 2020). Such simulated environments improve risk awareness and response preparedness across the industry.

One emerging area of innovation is the Internet of Underwater Things (IoUT), which connects underwater devices, sensors, and systems to enable real-time data exchange and monitoring. However, this technological advancement introduces significant cybersecurity challenges related to interoperability and data security. Recent research into semantic modelling and simulation techniques aims to address these issues, ensuring that IoUT systems can operate securely and efficiently (Kotis, Stavrinos, & Kalloniatis, 2022). As Finnish shipbuilders continue to adopt new technologies, securing these systems must be one of the top priorities.

Cybersecurity frameworks are also evolving alongside industry developments. Countries like the United States have already begun implementing comprehensive cybersecurity policies specifically tailored for the maritime transportation system. These policies provide structured frameworks for organizations to assess their cybersecurity posture and implement best practices (Finley & Harkiolakis, 2018). Finnish shipbuilding companies could benefit from similar regulatory developments that establish clear cybersecurity guidelines for shipbuilding operations.

Software systems play an essential role in modern shipbuilding, from design simulations to onboard control systems. A growing focus on software security is shaping the way shipbuilding companies integrate cybersecurity into development practices. Research by Vsevolozhsky & Qu (2022) proposes a process model for ensuring the diffusion and integration of cybersecurity innovations in software development organizations. Their model highlights the importance of continuous learning, adaptation, and best-practice integration to secure shipbuilding software environments (Vsevolozhsky & Qu, 2022).

As the industry continues with its digital transformation, cybersecurity must be an integral part of shipbuilding innovation. Investing in cybersecurity at an early stage, not just as a compliance requirement but as a strategic priority, will determine which companies can maintain operational resilience in the face of evolving cyber threats. By supporting innovation in cybersecurity, Finnish shipbuilders can position themselves as leaders in both shipbuilding and digital security preparedness.

In summary, IACS UR E26 significantly impacts Finnish shipbuilding by introducing new cybersecurity requirements that affect ship design, construction, and operational security. Meyer Turku and other Finnish shipyards must invest in enhanced cybersecurity measures, align with evolving regulatory frameworks, and integrate cybersecurity-by-design principles into ship construction. The regulation not only enforces compliance but also drives technological advancements, industry-wide standardization, and increased collaboration between shipbuilders, regulatory bodies, and government stakeholders. Finnish shipyards need to balance these challenges and opportunities to enhance their cybersecurity posture. The goal always should be long-term competitiveness in the maritime sector. In this chapter, RQ1 is addressed by illustrating how Finnish shipbuilders are to adapt and are adapting to UR E26 through regulatory compliance, technological

innovation, and industry collaboration. Beyond regulatory compliance, early adaptation to UR E26 places Finnish shipbuilders in a leadership position within the global maritime cybersecurity landscape. By proactively implementing these cybersecurity measures Meyer Turku can enhance their reputation as digitally resilient and secure their competitiveness in a rapidly evolving industry.

4 Survey research method

This chapter details the research methods used to assess cybersecurity perceptions, awareness, and priorities among Meyer Turku employees and external stakeholders. A survey-based methodology was chosen as the primary instrument due to its effectiveness in capturing both quantitative and qualitative insights from a diverse group of respondents. The survey was structured to systematically address key cybersecurity concerns, aligning with the study's research questions.

The survey used a mixed-methods approach, combining quantitative data (multiple-choice questions) with qualitative insights (open-ended feedback). This allowed both measurable trends and a deeper understanding of Meyer Turku employees and external stakeholders views on cybersecurity.

A research matrix was used to ensure alignment between the survey questions and the study's research objectives. This ensured that each aspect of cybersecurity awareness, importance, and practices was addressed comprehensively. The survey was structured around five key areas:

1. Demographics – To identify and categorize respondents for comparative analysis.
2. Cybersecurity Awareness – To measure respondents' baseline understanding of cybersecurity.
3. Cybersecurity Importance – To assess how respondents perceive the significance of cybersecurity in shipyard operations.
4. Cybersecurity Practices – To evaluate how respondents apply cybersecurity measures in their daily tasks.
5. Conclusion and Feedback – To capture open-ended responses and suggestions for improvement.

The survey, titled The Cybersecurity Awareness and Importance Survey, was distributed to both internal stakeholders (Meyer Turku employees) and external stakeholders (e.g., subcontractors, turnkey contractors, and owner representatives). The survey design was done to ensure that diverse perspectives were represented and to generate actionable insights for improving cybersecurity strategies.

4.1 Instrument: The cybersecurity awareness and importance survey

A survey was chosen as the primary research instrument because of its flexibility, scalability, and ability to capture both quantitative and qualitative data from a large, diverse population. This method was particularly suited to Meyer Turku's complex stakeholder environment, which includes employees, subcontractors, turnkey contractors, and owner representatives.

Advantages of the Survey Methodology

Scalability: The survey accommodated responses from a large number of stakeholders, enabling a broad representation of perspectives.

- Efficiency: Data collection from geographically dispersed respondents without requiring physical presence.
- Customizability: Questions were tailored to directly address the research objectives, ensuring relevance and focus. (Creswell & Creswell, 2018)

The survey combined quantitative and qualitative elements to provide:

- Quantitative Insights: Scaled and multiple-choice questions captured measurable trends, such as cybersecurity awareness levels.
- Qualitative Insights: Open-ended questions provided nuanced perspectives on challenges, experiences, and suggestions for improvement. (Creswell & Creswell, 2018)

While other methods like interviews, focus groups, and case studies were evaluated, they were deemed less suitable for this research:

- Interviews: Limited scalability and time-intensive for a large respondent base.
- Focus Groups: Logistically challenging.
- Case Studies: Lacked the breadth needed to capture diverse stakeholder perspectives comprehensively. (Creswell & Creswell, 2018)

4.2 Survey matrix design, Alignment of Research and Survey Questions

The survey design was guided by a research matrix (Figure 2), which ensured alignment between the research questions (RQ) and survey questions (Q). This alignment guaranteed that each research objective was addressed.

		Research questions:	RQ2 What type of threats does MT face?	RQ3 How do MT employees and stakeholders perceive the security of digital and physical resources within the shipyard?	RQ4 What is the level of cybersecurity awareness among MT employees and stakeholders, and how do they perceive the importance of cybersecurity in shipyard operations?	RQ5 How do different stakeholder groups (e.g., employees, subcontractors, owner representatives) differ in their perceptions of cybersecurity threats and priorities?
Survey questions		**Demographics**				
	Q1	Are you currently an employee of Meyer Turku shipyard?				
	Q2	If you answered "No" to the previous question, please specify your affiliation with Meyer Turku:				
	Q3	How long have you been associated with shipbuilding and shipyards?				X
	Q4	How long have you been associated with Meyer Turku shipyard?				X
		Cybersecurity Awareness				
	Q5	On a scale of 1 to 5, please rate your understanding of cybersecurity. 1 (Very Low), 2 (Low), 3 (Moderate), 4 (High), 5 (Very High)			X	
	Q6	Have you received any yard information security training or cybersecurity awareness programs at Meyer Turku shipyard?			X	
	Q7	If yes, please rate the effectiveness of the cybersecurity training/awareness programs you have received: 1 (Very Ineffective), 2 (Ineffective), 3 (Neutral), 4 (Effective), 5 (Very Effective).			X	
	Q8	Do you find yourself needing more training in cybersecurity practices?			X	X
		Cybersecurity Importance				
	Q9	How important do you think cybersecurity is for Meyer Turku shipyard's operations? 1 (Not important), 2 (Somewhat important), 3 (Neutral), 4 (Important), 5 (Extremely important)			X	
	Q10	Meyer Turku shipyard's operations involve various resources that require protection. Please select the types of resources you believe should be protected within the scope of cybersecurity efforts. Additionally, indicate their importance to you or your role. Check all that apply and rate their importance on a scale of 1 to 5. Scale: 1 = Not important, 5 = Extremely important.		X	X	X
	Q11	OPTIONAL. Is there anything else, not mentioned above, that you believe is important to consider in the context of cybersecurity at Meyer Turku shipyard? If so, please specify.		X	X	X
	Q12	OPTIONAL. Please rate the importance of your added resource or item in regards of cybersecurity from question 11.		X		
	Q13	In your opinion, what are the main reasons for prioritizing cybersecurity in a shipyard environment? (Please select up to three choices)			X	X
	Q14	OPTIONAL. Do you believe there are additional resources or aspects that should be considered for protection within Meyer Turku shipyard's operations? Please share your thoughts and suggestions:		X		
	Q15	Have you ever encountered a cybersecurity incident or breach at Meyer Turku shipyard or in your role as a stakeholder?	X		X	
	Q16	Optional. If you answered yes to question 15, please briefly describe the incident or breach (optional):	X			
		Cybersecurity Practices				
	Q17	Did you have prior knowledge of CIA best practices before?		X	X	X
	Q18	Do you follow cybersecurity best practices in your day-to-day work at Meyer Turku shipyard or in your role as a stakeholder to ensure the Confidentiality, Integrity, and Accessibility (CIA) of protected resources?		X	X	X
	Q19	Do you think there are specific cybersecurity measures or practices you think should be implemented or improved at Meyer Turku shipyard to better ensure the CIA of the resources you identified in this survey?		X	X	X
		Conclusion and feedback				
	Q20	Please share any additional comments, suggestions, or feedback you have regarding cybersecurity at Meyer Turku shipyard:			X	

Figure 2 Research Matrix with Research Questions RQ2-RQ5 and corresponding Survey questions Q1-Q20

In the matrix the research questions align with survey questions as follows:

- RQ2: Q15, Q16
- RQ3: Q10, Q11, Q14, Q17, Q18, Q19
- RQ4: Q5, Q6, Q7, Q8, Q11, Q13, Q15, Q17, Q18, Q19, Q20
- RQ5: Q3, Q4, Q8, Q10, Q11, Q13, Q17, Q18, Q19

The research questions are displayed separately with their focus and purpose in Table 1 below.

Research Question (RQ)	Focus	Purpose
RQ2: What types of cybersecurity threats does Meyer Turku face?	Identification of Threats	To analyse the specific types of cyber risks affecting the shipbuilding process, including both digital and physical vulnerabilities.
RQ3: How do Meyer Turku employees and stakeholders perceive the security of digital and physical resources within the shipyard?	Perception of Security	To explore how respondents evaluate the current state of cybersecurity for critical resources and identify any perceived weaknesses or strengths.
RQ4: What level of cybersecurity awareness exists among Meyer Turku employees and stakeholders, and how do they perceive the importance of cybersecurity in shipyard operations?	Awareness and Importance	To assess respondents' baseline knowledge, training exposure, and their perspectives on the significance of cybersecurity measures for operational safety and resilience.
RQ5: How do different stakeholder groups (e.g., employees, subcontractors, owner representatives) differ in their perceptions of cybersecurity threats and priorities?	Group-Specific Insights	To compare the cybersecurity priorities and risk perceptions of various stakeholder groups, revealing different needs and concerns.

Table 1 The Research Questions used in the design of the survey, RQ2-RQ5

The survey was designed with five key focus areas displayed in 4.1, each addressing a distinct aspect of the research objectives. These focus areas aim to provide a comprehensive understanding of stakeholder perspectives on cybersecurity at Meyer Turku shipyard. By structuring the survey in this way, the collected data allows for both comparative and in-depth analysis of stakeholder views and practices.

The Demographics section aims to identify and categorize respondents based on their roles, affiliations, and experience levels. This categorization allows for comparative analysis across different stakeholder groups. Understanding the composition of respondents was helped analysing group-specific perceptions and priorities. Tables 2-6 below provide an overview of the survey questions related to demographics, their focus, and how they align with the research objectives.

Demographics		
Question	**Focus**	**Reasoning**
Q1. "Are you currently an employee of Meyer Turku shipyard?"	Identifies whether respondents are internal employees or external stakeholders.	For segmenting data and comparing perceptions of different groups (e.g., employees vs. subcontractors). Supports RQ4 and RQ5.
Q2. "If you answered 'No' to the previous question, please specify your affiliation with Meyer Turku:"	Captures detailed affiliations of external stakeholders (e.g., subcontractors, turnkey contractors).	Enhances ability to compare subgroup perspectives. Aligns with RQ4 and RQ5.
Q3. "How long have you been associated with shipbuilding and shipyards?"	Measures respondents' industry experience.	Helps identify how professional experience influences perceptions of cybersecurity. Supports RQ5 by uncovering differences in priorities and awareness levels.
Q4. "How long have you been associated with Meyer Turku shipyard?"	Captures respondents' familiarity with Meyer Turku.	Highlights how length of association affects cybersecurity awareness and perceptions. Contributes to RQ5.

Table 2 Demographics section of the survey, Q1-Q4.

The Cybersecurity Awareness section measures the respondent baseline understanding of cybersecurity concepts and their exposure to training programs. This area examines awareness gaps and evaluates whether current training effectively prepares respondents to handle cybersecurity risks. Table 3 presents the survey questions related to cybersecurity awareness, along with their intended focus and alignment with the research objectives.

Cybersecurity Awareness		
Question	**Focus**	**Reasoning**
Q5. "On a scale of 1 to 5, please rate your understanding of cybersecurity."	Measures respondents' baseline knowledge of cybersecurity.	Supports RQ4 by identifying variations in awareness among different groups and providing a foundation for analysing training needs.
Q6. "Have you received any yard information security training or cybersecurity awareness programs at Meyer Turku shipyard?"	Evaluates exposure to formal cybersecurity training.	Helps to assess the availability and accessibility of training programs, directly contributing to RQ4 by identifying disparities in awareness-building efforts.
Q7. "If yes, please rate the effectiveness of the cybersecurity training/awareness programs you have received."	Gauges how useful respondents perceive existing training programs to be.	Provides actionable insights into the quality of training and its impact on awareness. Addresses RQ4.
Q8. "Do you find yourself needing more training in cybersecurity practices?"	Identifies gaps in respondents' confidence or preparedness.	Highlights unmet needs and areas for improvement in training. Contributes to RQ4 and RQ5.

Table 3 Cyber security awareness section of the survey, Q5-Q8.

The Cybersecurity Awareness section measures the respondents' baseline understanding of cybersecurity concepts and their exposure to training programs. This area focuses on identifying gaps in awareness and determining whether current training efforts effectively equip respondents with the knowledge needed to address cybersecurity risks.

The Cybersecurity Importance section explores how respondents perceive the significance of cybersecurity in shipyard operations. It delves into the prioritization of critical resources, motivations for emphasizing cybersecurity, and the perceived importance of specific measures. This section provides insight into stakeholder priorities and motivations, helping to identify areas where awareness or investment might be improved. Table 4 outlines the survey questions in this area, highlighting their focus and relevance to the research objectives.

Cybersecurity Importance		
Question	**Focus**	**Reasoning**
Q9. "How important do you think cybersecurity is for Meyer Turku shipyard's operations? 1 (Not important), 2 (Somewhat important), 3 (Neutral), 4 (Important), 5 (Extremely important)"	Measures perceptions of cybersecurity's relevance.	Directly addresses RQ4 by assessing the perceived importance of cybersecurity across groups.
Q10. "Meyer Turku shipyard's operations involve various resources that require protection. Please rate their importance on a scale of 1 to 5. Scale: 1 = Not important, 5 = Extremely important."	Identifies critical resources respondents prioritize for cybersecurity protection.	Aligns with RQ3 by showing which resources are viewed as essential and with RQ5 by revealing differences in priorities across stakeholder groups.
Q11. "OPTIONAL. Is there anything else, not mentioned above, that you believe is important to consider in the context of cybersecurity at Meyer Turku shipyard? If so, please specify."	Captures qualitative insights into overlooked concerns or priorities.	Complements RQ3 and RQ5 by allowing respondents to highlight specific, nuanced cybersecurity issues.
Q12. "OPTIONAL. Please rate the importance of your added resource or item in regards to cybersecurity from question 11."	Quantifies the perceived importance of resources identified in Q11.	Provides measurable data to supplement qualitative feedback, supporting RQ3 and RQ5.
Q13. "In your opinion, what are the main reasons for prioritizing cybersecurity in a shipyard environment? (Please select up to three choices)"	Identifies motivations for prioritizing cybersecurity (e.g., compliance, operational continuity).	Aligns with RQ4 and RQ5 by revealing stakeholder-specific priorities and motivations.
Q14. "OPTIONAL. Do you believe there are additional resources or aspects that should be considered for protection within Meyer Turku shipyard's operations? Please share your thoughts and suggestions:"	Invites respondents to suggest additional cybersecurity priorities.	Expands on Q11 and aligns with RQ3 and RQ4 by capturing nuanced stakeholder perspectives.
Q15. "Have you ever encountered a cybersecurity incident or breach at Meyer Turku shipyard or in your role as a stakeholder?"	Explores respondents' direct experience with cybersecurity incidents.	Addresses RQ2 by identifying vulnerabilities and risks faced by respondents.
Q16. "OPTIONAL. If you answered yes to question 15, please briefly describe the incident or breach:"	Collects qualitative data about the nature and impact of incidents.	Provides deeper insights into specific cybersecurity threats, supporting RQ2.

Table 4 Cybersecurity Importance section of the survey, Q9-Q16.

The Cybersecurity Practices section evaluates how respondents apply cybersecurity measures in their daily tasks. It investigates the practical implementation of cybersecurity knowledge and best practices, including the use of Confidentiality, Integrity, and Availability (CIA) principles. This area bridges the gap between theoretical knowledge and actionable practices, highlighting opportunities for improvement. Table 5 summarizes the survey questions under this focus area, emphasizing their role in addressing the research questions.

Cybersecurity Practices		
Question	**Focus**	**Reasoning**
Q17. "Did you have prior knowledge of CIA best practices before?"	Assesses familiarity with the principles of confidentiality, integrity, and availability.	Supports RQ3 and RQ4 by identifying knowledge gaps in cybersecurity concepts.
Q18. "Do you follow cybersecurity best practices in your day-to-day work at Meyer Turku shipyard?"	Evaluates how well respondents implement cybersecurity knowledge in practice.	Links awareness to action, supporting RQ3 and RQ4.
Q19. "Do you think there are specific cybersecurity measures or practices you think should be implemented or improved at Meyer Turku shipyard?"	Collects actionable suggestions for improving cybersecurity measures.	Supports RQ3, RQ4, and RQ5 by revealing perceived gaps and priorities.

Table 5 Cybersecurity Practices section of the survey, Q17-Q19.

The Conclusion and Feedback section captures open-ended responses from respondents, offering an opportunity to identify overlooked issues or gather innovative suggestions for enhancing cybersecurity measures. This section provides qualitative insights that complement the quantitative data collected in other areas, enriching the overall analysis. Table 6 provides an overview of the open-ended survey questions and their contributions to the research objectives.

Conclusion and Feedback		
Question	**Focus**	**Reasoning**
Q20. "Please share any additional comments, suggestions, or feedback you have regarding cybersecurity at Meyer Turku shipyard."	Provides an open platform for unstructured feedback.	Complements all research questions by capturing broad stakeholder perspectives, uncovering potential blind spots, and generating ideas for future improvements.

Table 6 Conclusion and Feedback section of the survey, Q20

4.3 Challenges and Limitations

The process of designing and conducting the survey for this research presented a range of challenges, each with distinct implications for the quality and scope of the data collected. These challenges spanned multiple stages, including survey design, data collection, and data analysis. To ensure transparency and provide a deeper understanding of the methodology, the following table outlines the key challenges encountered, their corresponding impacts, and how these factors shaped the overall research process. The Table 7 below provides a comprehensive overview of the challenges and impacts involved.

Survey Design Challenges	**Challenge**	**Impact**
Balancing Depth and Simplicity	The survey needed to cover cybersecurity awareness, perceptions, practices, and priorities, while remaining concise and easy to complete.	Some survey questions were broad in scope, limiting depth of insights. Open-ended questions were included to mitigate this, but their qualitative nature complicated analysis.
Question Alignment with Research Objectives	Ensuring that all survey questions aligned directly with the research questions required significant effort during the design phase.	While the research matrix ensured alignment, there was a risk of oversimplifying complex issues to fit into predefined question formats.
Data Collection Challenges	**Challenge**	**Impact**
Response Rate Variability	The survey relied on voluntary participation, leading to variations in response rates across different stakeholder groups (e.g., employees vs. subcontractors).	Certain groups, such as some external stakeholders' groups, had lower participation rates, potentially affecting the representativeness of the data.
Language and Terminology	Respondents came from diverse professional and linguistic backgrounds, creating potential barriers to understanding technical cybersecurity terminology.	Simplified language and explanations were provided, but misunderstandings may have influenced responses, particularly for non-native speakers or those unfamiliar with cybersecurity.
Anonymity Concerns	While the survey was anonymous, some respondents might have hesitated to share honest feedback, particularly about negative incidents, due to concerns about confidentiality.	This may have resulted in underreporting of cybersecurity incidents or other critical issues.
Analysis Challenges	**Challenge**	**Impact**
Interpreting Qualitative Data	Open-ended questions generated a wealth of qualitative data, which provided valuable insights but required extensive coding and interpretation to identify themes.	The process was time-consuming and required careful consideration to avoid researcher bias when categorizing responses.
Comparative Analysis	Comparing responses across different stakeholder groups (e.g., employees, subcontractors, owner representatives) was complex due to varying levels of familiarity with cybersecurity and differing priorities.	This complexity made it challenging to draw definitive conclusions about group-specific trends without further context.

Table 7 Challenges and impacts of the research design

4.4 Why This Approach Was Chosen

The decision to adopt a survey-based methodology was rooted in its ability to effectively address the research objectives within the context of Meyer Turku's shipbuilding operations. This approach was particularly well-suited to the unique challenges posed by the environment of the industry. It allowed the collection of a wide range of data while ensuring inclusivity and adaptability.

Surveys offered a flexible means of capturing both quantitative and qualitative data, making it possible to balance breadth and depth. By incorporating multiple-choice, scaled, and open-ended questions, the survey captured measurable trends in cybersecurity awareness levels and nuanced perspectives. It captured also personal experiences and recommendations for improvement. This mixed-methods design ensured the research could provide a comprehensive understanding of cybersecurity-related issues.

The survey's accessibility was another critical factor in its selection. Given the diverse stakeholder environment at Meyer Turku, including employees, subcontractors, turnkey contractors, and owner representatives, the survey provided a practical way to gather input across these groups. Employees and stakeholders at Meyer Turku operate across various locations, and a digital survey format allowed for participation without the need for in-person meetings. This made it an efficient method for reaching a broad audience while accommodating different work schedules and time constraints. The anonymity of the survey also encouraged honest responses, reducing the likelihood of social desirability bias that might have influenced feedback in other research settings.

Beyond its logistical advantages, the survey method was particularly suited for measuring subjective factors such as cybersecurity awareness, risk perception, and stakeholder priorities. Since cybersecurity concerns often vary based on professional experience, role-specific responsibilities, and exposure to digital systems, it was essential to gather direct insights from participants in a way that allowed comparisons across different groups. The survey was designed to facilitate comparative analyses, segmenting responses based on job roles, years of experience, and organizational affiliations. These comparisons helped uncover differences in cybersecurity awareness, priorities, and vulnerabilities across various stakeholder groups, ultimately leading to more targeted and actionable insights.

Cybersecurity is a rapidly evolving field, where new threats and best practices emerge continuously. A survey-based approach provided flexibility to explore real-time concerns specific to Meyer Turku's operations while remaining adaptable to the latest cybersecurity challenges in the shipbuilding industry. By structuring the questions to address both current industry standards and anticipated future risks, the study ensured that its findings remained relevant and applicable within the rapidly changing digital landscape of maritime operations.

While alternative research methods such as interviews, focus groups, and case studies were considered, they presented limitations that made them less suitable for this study. Conducting interviews with a large and diverse pool of stakeholders would have been time-consuming and resource-intensive, ultimately limiting the scope and representativeness of the research. Focus groups, though valuable in exploring group dynamics, posed logistical challenges and the risk of dominant participants skewing discussions, which could have led to biased conclusions (Smithson, 2000). Additionally, focus groups shared the same downsides as interviews in terms of cost and time efficiency. Case studies were not broad enough to fully address the research questions, especially when comparing different stakeholder perspectives (Yin, 2018).

The survey-based approach proved to be effective and practical method for gathering comprehensive, representative, and actionable data on cybersecurity awareness, practices, and perceptions at Meyer Turku. By balancing inclusivity, flexibility, and depth, it enabled the study to meet its objectives within the constraints of time, resources, and respondent availability.

5 Cybersecurity Awareness and Importance Survey

This chapter presents the results of the survey conducted to evaluate cybersecurity awareness, perceptions, and practices among Meyer Turku shipyard employees and external stakeholders. The survey was created to match the research goals, making sure cybersecurity in shipbuilding was carefully examined. Since the shipyard has many different stakeholders, the survey helps to understand how various groups view, prioritize, and handle cybersecurity.

The chapter is structured around five key areas: Demographics, Cybersecurity Awareness, Cybersecurity Importance, Cybersecurity Practices, and Conclusion & Feedback. Each section presents the survey questions, analyses the responses, and discusses their relevance to the research questions. The findings help to identify security gaps, training needs, and stakeholder-specific concerns regarding cybersecurity at Meyer Turku. With this structured approach, the survey findings provide an overview of cybersecurity awareness at Meyer Turku, highlighting key areas for improvement and informing future cybersecurity strategies.

To conduct the survey, official permissions were granted by Meyer Turku's Project Management, Outfitting Department, Procurement Department, and IT Department that is responsible for network security and digital infrastructure. The approvals ensured that the survey aligned with Meyer Turku's operational policies and data protection guidelines. The approvals allowed an industry-relevant research of cybersecurity awareness across internal and external stakeholder groups.

The survey was conducted using Microsoft Forms (forms.office) as the digital platform for collecting responses. The survey invitation and access link were distributed on March 6, 2024, through two main channels: Meyer Turku Employees and External Stakeholders. The survey link was shared via the company's internal intranet, ensuring accessibility to all Meyer Turku employees. Meyer Turku procurement department distributed the survey invitation via direct email to Meyer Turku's entire stakeholder network.

To ensure a broad and inclusive response, the survey was open for one month, closing on April 6, 2024. It was designed to be fully anonymous, with an estimated completion time of 5 to 10 minutes. Respondents had the option to complete the survey in either Finnish or English, ensuring accessibility across different language groups.

Once the response period ended, all collected data was compiled and structured into an analysable format using Microsoft Excel. Open-ended responses were carefully reviewed to prevent the disclosure of company-specific or personally identifiable information before being included in the final analysis.

The data interpretation phase was conducted in collaboration with Meyer Turku's project management department and the University of Turku through control meetings. This ensured that the analysis was well-grounded in both industrial and academic perspectives, enhancing the reliability and applicability of the findings.

Meyer Turku's external stakeholders play a critical role in shipbuilding operations, making their cybersecurity practices a key concern. The survey included participation from the following external stakeholder groups:

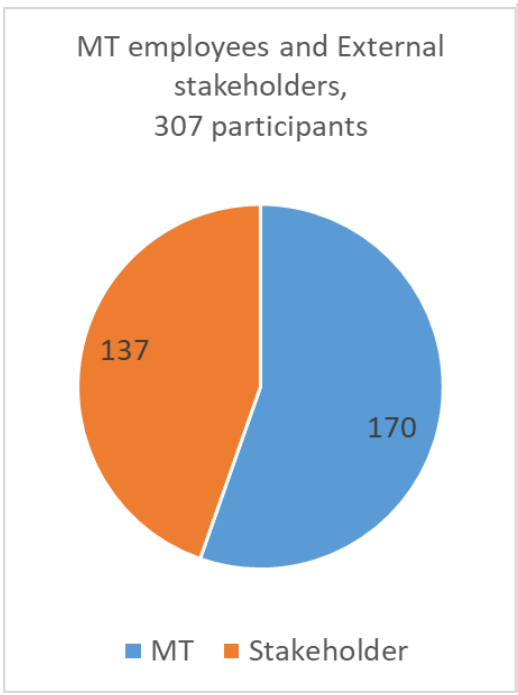
- Turnkey Contractors: Companies responsible for delivering fully operational areas, systems or solutions, such as complex modules or subsystems, under a single contract.
- Subcontractors: Specialized companies performing specific tasks or services within the shipyard, such as component installations or technical implementations.
- Material or System Suppliers: Providers of raw materials, machinery, or systems necessary for ship construction and outfitting, ensuring compliance with design and operational requirements.
- Owner: Refers to the shipowners, such as entities like Royal Caribbean Cruise Line or TUI Cruises. Shipowners commission the construction of the vessel.
- Class Societies: Regulatory bodies ensuring the vessel's design, construction, and outfitting comply with international safety and quality standards.

By engaging both internal employees and external stakeholders, the survey results provide a comprehensive view of cybersecurity awareness and preparedness across the entire Meyer Turku shipbuilding "ecosystem". The following sections will present and analyse the findings in detail, beginning with respondent demographics.

5.1 Demographics, Q1-Q4

Understanding the demographics of the respondents is crucial for contextualizing the survey results. By categorizing participants based on their roles, experience, and affiliation with Meyer Turku, the survey enables a comparative analysis of cybersecurity awareness and priorities across different stakeholder groups. This section examines respondent employment status, years of experience in the shipbuilding industry, and their specific affiliation with Meyer Turku. These factors influence perceptions of cybersecurity and help identify potential disparities in awareness and training needs among internal employees, subcontractors, and other stakeholders.

External stakeholder demographics pie chart shows that all possible stakeholders inside Meyer Turku shipyard that were able to participate in the survey. The main pie chart (Figure 3) shows the split between Meyer Turku employees (170 participants) and external stakeholders (137 participants) among the survey respondents. The external stakeholders represent almost half of the survey population, which is accurate in also considering that also almost half of the Meyer Turku population are external stakeholders. Therefore, the consideration of cybersecurity policies and practices in the midst of external stakeholders carry equal weight to internal Meyer Turku cybersecurity policies and practices. Given that external stakeholders make up a significant portion of the survey respondents, it highlights the importance of including these groups in cybersecurity strategies. Ensuring that external stakeholders adhere to the same cybersecurity standards as Meyer Turku employees.



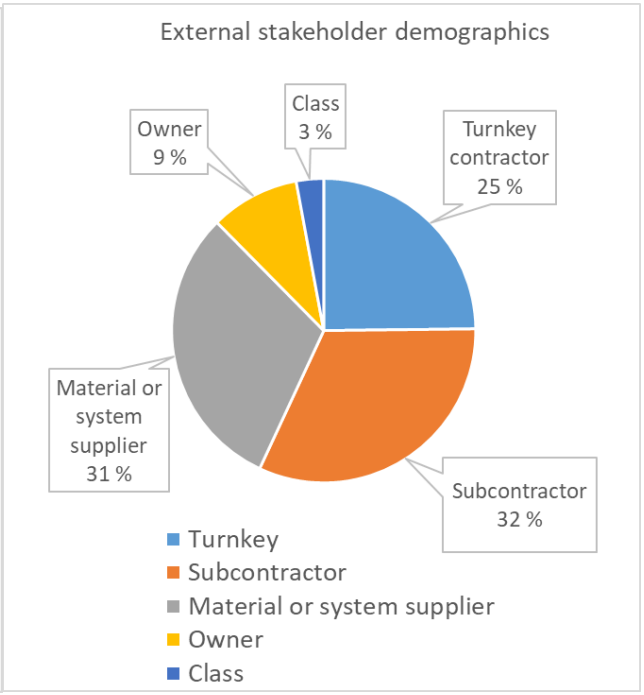


Figure 3 Q1 MT and external stakeholders. Figure 4 Q2 307 participants.

The two bar charts (Figure 5 and 6) reveal the distribution of tenure among respondents, both in the shipbuilding industry in general and specifically at Meyer Turku. There is a considerable number of respondents with long-term association in both charts, suggesting that a significant portion of the workforce has extensive experience and potentially deep expertise in the field. A workforce with a rich knowledge base can be advantageous for maintaining high standards in shipbuilding. However, this also implies that cybersecurity training and policies may need to be adjusted or reinforced to cater to a workforce that might be set in traditional ways of working. For example, newer employees or external stakeholders might need introductory training, while more seasoned professionals might benefit from advanced, scenario-based training focusing on emerging threats.

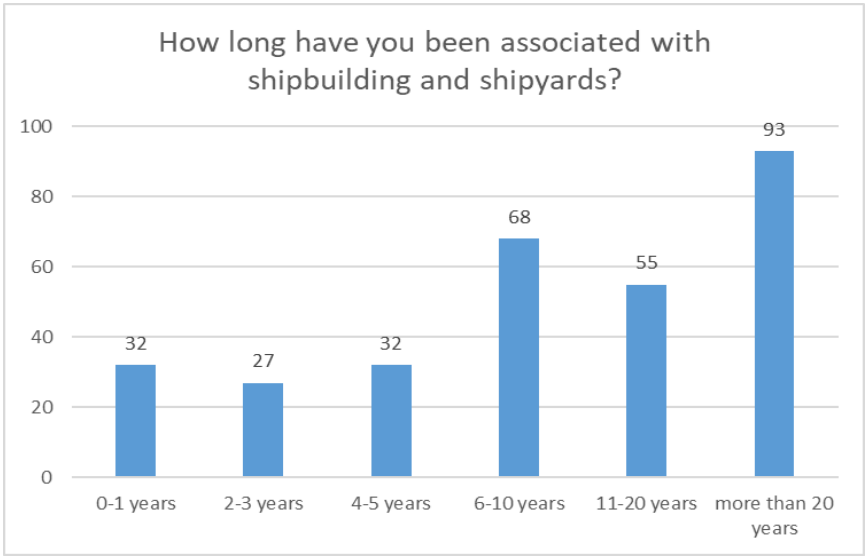


Figure 5 Q3 Association with shipbuilding

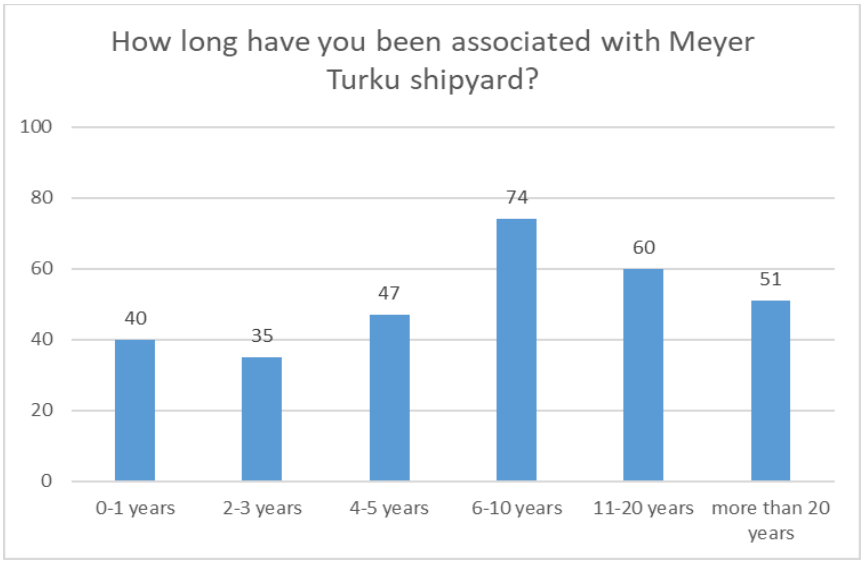


Figure 6 Q4 Association with Meyer Turku

5.2 Cybersecurity Awareness, Q5-Q8

Cybersecurity awareness is a fundamental component of effective security management. Without a strong understanding of cyber threats, employees and external stakeholders may inadvertently expose critical systems to risks. This section evaluates how well respondents understand cybersecurity concepts and whether they have received any formal training at Meyer Turku.

The analysis highlights the level of familiarity with cybersecurity principles such as the CIA Triad (Confidentiality, Integrity, and Availability) and explores the perceived effectiveness of training programs. By assessing knowledge gaps, this section informs recommendations on improving cybersecurity education and awareness at the shipyard.

Q5: "On a scale of 1 to 5, please rate your understanding of cybersecurity. 1 (Very Low), 2 (Low), 3 (Moderate), 4 (High), 5 (Very High)"

The responses to Q5 reflect how confident different respondent groups feel about their self-perceived cybersecurity knowledge. The results highlight strong similarities between Meyer Turku employees and external stakeholders.

The majority (63%) of respondents believe they have a High (49%) or Very High (14%) understanding of cybersecurity. However, a significant portion (29%) rate their knowledge as only Moderate (3) (Figure 7). Additionally, 8% of respondents reported Low (2) cybersecurity knowledge, suggesting a potential need for further training. No respondents rated their knowledge as Very Low (1).

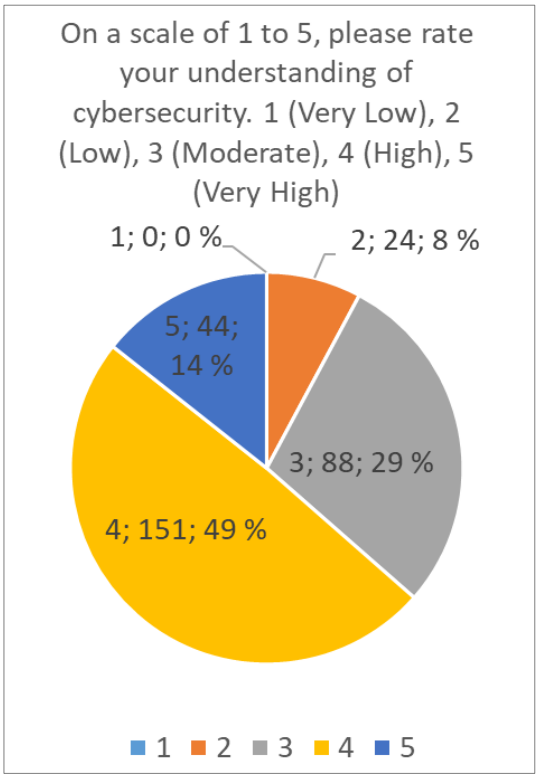


Figure 7 Q5 All respondents

The difference between Meyer Turku employees and external stakeholders (Figure 8) is minimal. However, MT employees exhibit slightly lower confidence levels in the "Very High" (5) category compared to external stakeholders. This may indicate that external stakeholders, such as IT contractors or system suppliers, have received more cybersecurity training in their respective organizations or work directly in security-sensitive environments. Due to the small variance between the groups, the "all respondents" chart was deemed to provide a sufficiently accurate representation of the results.

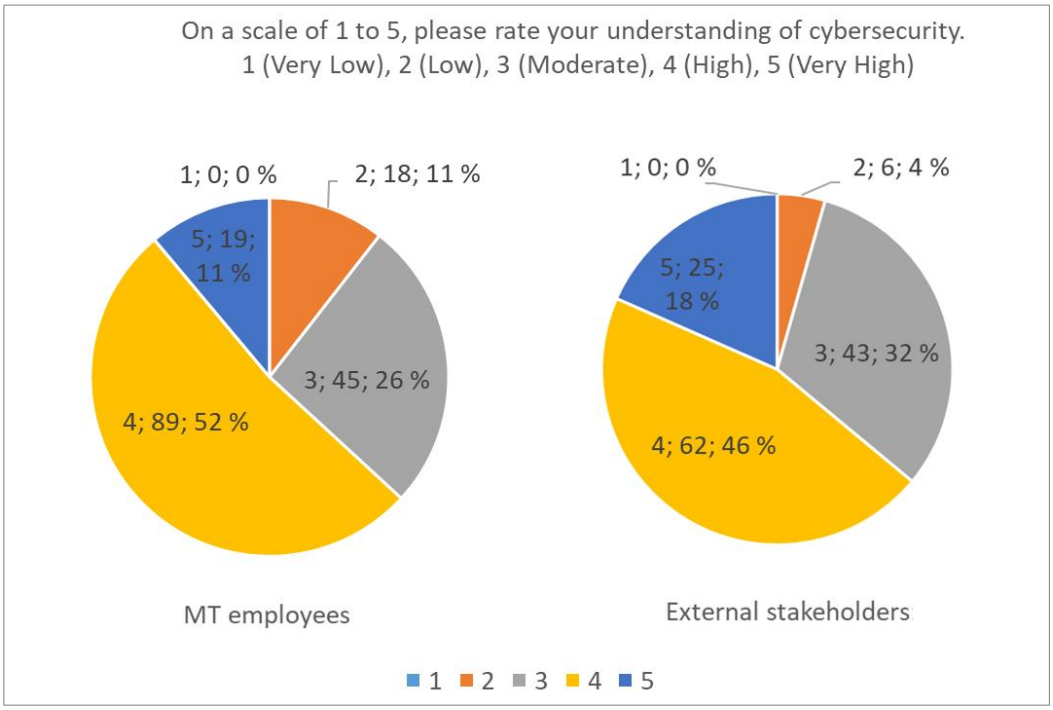


Figure 8 Q5 MT employees vs. External stakeholders

Overall, while most respondents demonstrate a solid understanding of cybersecurity, notable gaps remain. Since the differences between groups are minimal, targeted cybersecurity training and awareness initiatives should be reinforced for both internal and external stakeholders to ensure they remain well-informed and prepared to mitigate cyber threats effectively.

Q6. ”Have you received any yard information security training or cybersecurity awareness programs at Meyer Turku shipyard?”

The training participation pie chart (Figure 9) reveals a concerning statistic: 116 respondents reported having received cybersecurity training or awareness programs at Meyer Turku shipyard, while 191 respondents stated that they had not. This means that approximately 62% of the respondents has not participated in any formal cybersecurity training provided by the shipyard. Given the increasing digitization of shipbuilding operations and the associated cyber risks, this figure raises serious concerns regarding the overall cybersecurity resilience of the shipyard.

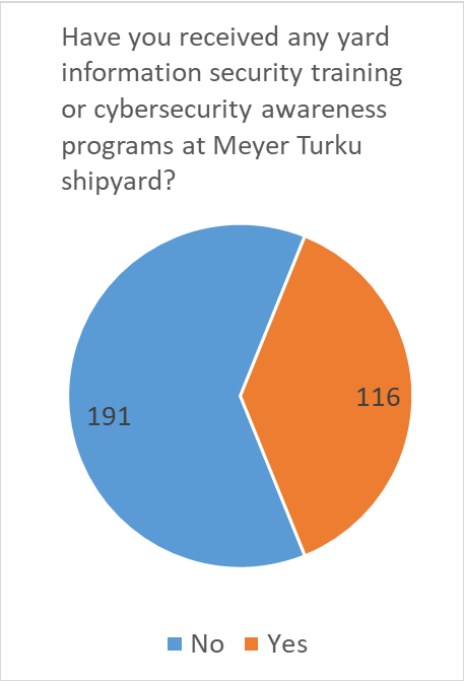


Figure 9 Q6 All respondents

The lack of cybersecurity training among such a large proportion of the workforce could be indicative of multiple underlying issues. One possibility is that Meyer Turku's orientation program for new employees and external stakeholders lacks a strong cybersecurity component or, if it does include such training, it might not be sufficiently emphasized. Another explanation could be that existing training programs do not effectively engage workers, leading to either low participation rates or a lack of awareness about the importance of cybersecurity. Additionally, it is possible that employees and external stakeholders do not perceive cybersecurity as a high-priority concern, resulting in negligence or a lack of motivation to undergo training.

The issue becomes even more pressing when examining the training participation rate among external stakeholders. The pie chart (Figure 11) shows that only 21% (28 out of 136 participants) of external stakeholders have received cybersecurity training, while a staggering 79% (108 respondents) have not. This stark disparity suggests that cybersecurity training efforts are primarily focused on internal employees, leaving external contractors, suppliers, and subcontractors significantly underprepared in terms of cybersecurity awareness.

This is particularly alarming because many external stakeholders have access to Meyer Turku's digital infrastructure, communication networks, and shipbuilding designs. Without proper training, these individuals could unknowingly expose the shipyard to cyber threats such as phishing attacks, malware infections, or unauthorized access to sensitive systems. The situation raises critical questions: Is cybersecurity training a mandatory requirement for subcontractors and third-party vendors? If so, why do so many claim to have not received any training?

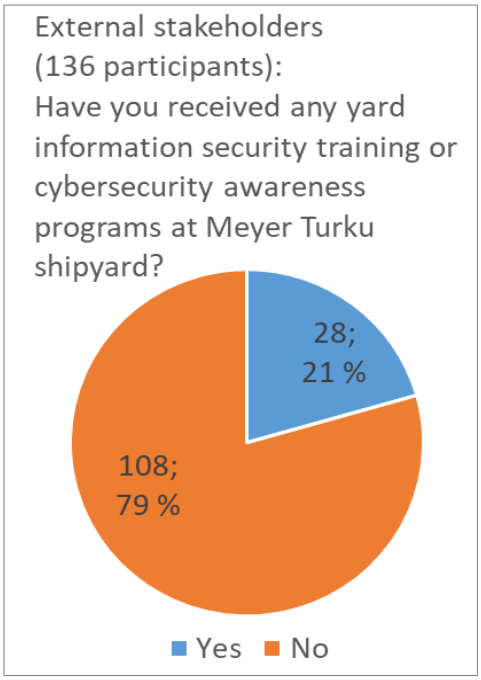


Figure 10 Q6 External stakeholders

One potential explanation is that Meyer Turku does not have a strict enforcement mechanism for ensuring third-party compliance with cybersecurity training. If cybersecurity awareness is merely an optional recommendation rather than a contractual obligation, it is possible that many external workers simply choose to bypass it. Another contributing factor could be language barriers or logistical constraints, where external partners are not adequately informed about available training programs or do not have easy access to them. Additionally, some subcontractors operate on short-term contracts, meaning that if cybersecurity training sessions are conducted infrequently, they may never receive training before their work is completed.

The fact that the majority of external stakeholders lack cybersecurity training exposes Meyer Turku to severe security risks, particularly in supply chain vulnerabilities, operational security, and regulatory compliance. Cyber threats often originate from third-party suppliers and contractors, making them an easy entry point for cybercriminals targeting the shipyard's infrastructure. Furthermore, physical security risks could emerge, as workers unfamiliar with cybersecurity protocols may inadvertently allow unauthorized access to restricted areas.

From a compliance standpoint, failing to ensure that all employees and external partners receive cybersecurity training could put Meyer Turku at risk of non-compliance with industry regulations. Many cybersecurity frameworks, including the IACS UR E26 and EU cybersecurity directives, emphasize the need for robust security training across all personnel handling sensitive data and systems. If Meyer Turku's cybersecurity strategy does not extend to external stakeholders, it may struggle to meet these regulatory standards.

To mitigate these risks, Meyer Turku should consider implementing mandatory cybersecurity training for all external suppliers, ensuring that participation is enforced through contractual agreements and compliance monitoring. One possible solution is to introduce a certification system, requiring all external personnel to complete basic cybersecurity awareness training before being granted access to the shipyard's infrastructure.

Additionally, cybersecurity awareness could be better integrated into existing onboarding and safety training programs, making it an integral part of Meyer Turku's overall security culture. Training materials should be made accessible in multiple languages to accommodate international stakeholders, and frequent refresher courses should be conducted to keep personnel updated on evolving threats.

The current low participation rate in cybersecurity training, especially among external stakeholders, represents a critical vulnerability for Meyer Turku. If left unaddressed, this gap could significantly increase the shipyard's exposure to cyber threats, operational disruptions, and compliance risks. Strengthening cybersecurity training programs and ensuring inclusive participation across all levels of the workforce and supply chain is essential for maintaining a resilient and secure shipbuilding environment.

Q7. "If yes, please rate the effectiveness of the cybersecurity training/awareness programs you have received: 1 (Very Ineffective), 2 (Ineffective), 3 (Neutral), 4 (Effective), 5 (Very Effective)."

The bar chart (Figure 11) illustrates how respondents rated the effectiveness of cybersecurity training at Meyer Turku shipyard. Among the 116 respondents who had received training, the majority (63) rated it as neutral (3), while 44 considered it effective (4), and only 5 found it very effective (5). Additionally, a small number (4) rated it as ineffective (2), and no respondents rated it as very ineffective (1).

While it is positive that many respondents found the training at least somewhat useful, the high proportion of neutral responses suggests that the training might not be engaging or in-depth enough to leave a strong impact. A training program that does not actively engage employees and external stakeholders or fails to address their specific cybersecurity challenges may result in participants feeling indifferent about its effectiveness. The presence of neutral responses indicates an opportunity to improve the content and delivery of these training programs to ensure they are more interactive, relevant, and aligned with the cybersecurity risks faced in the shipyard environment.

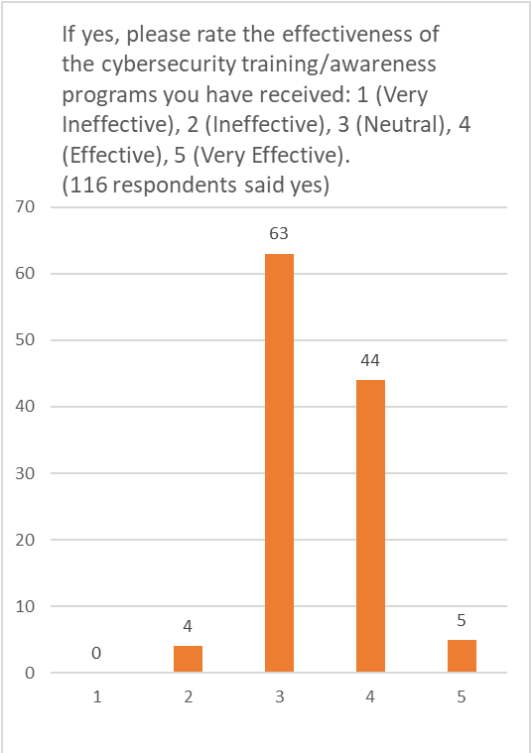


Figure 11 Q7 Rating of "Yes" answers from Q6

When focusing on external stakeholders, the results in Figure 12 show a similar trend, but with an even greater share of neutral responses. Among external stakeholders who participated in training, 14 rated it as neutral, 10 found it effective, and 4 considered it very effective. This reinforces the concern that cybersecurity training may not be tailored to the specific needs of different stakeholder groups, particularly external partners who play a crucial role in shipyard operations. Since external stakeholders interact with Meyer Turku's systems and data, ensuring that they receive impactful and comprehensive training is essential for overall cybersecurity resilience.

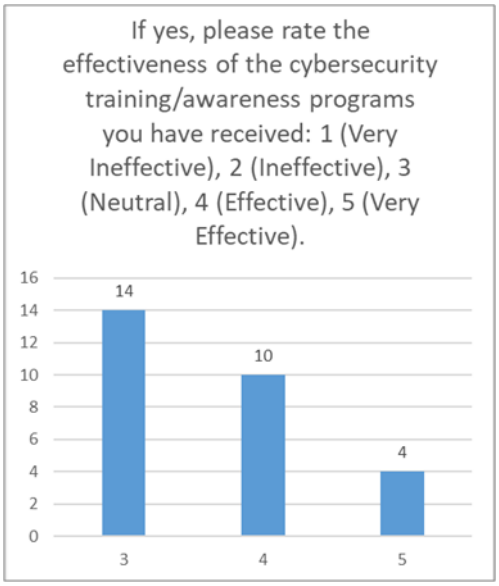


Figure 12 Q7 External stakeholders

The data from both internal and external respondents suggests that while cybersecurity training is available, there is room for improvement in both content and delivery. Future training initiatives could benefit from incorporating real-world case studies, hands-on exercises, and stakeholder-specific cybersecurity scenarios to increase engagement and practical understanding. The goal should be to shift participants from a neutral stance toward finding the training actively beneficial in their day-to-day roles.

Q8 Do you find yourself needing more training in cybersecurity practices?

The responses to this question reveal a divided perception among the participants regarding their cybersecurity preparedness. Out of all respondents, 47% (143 respondents) answered "Yes," indicating that they see a need for additional training in cybersecurity practices, while 53% (164 respondents) responded "No," suggesting confidence in their existing knowledge (Figure 13). This near-even split highlights a significant portion of the workforce recognizing room for improvement in their cybersecurity awareness and skills.

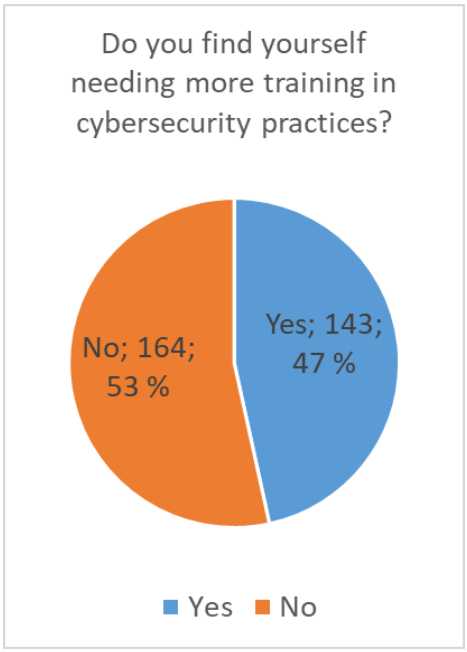


Figure 13 Q8 All respondents

Among those who answered "Yes," 35% (107 respondents) are Meyer Turku (MT) employees, while 65% (200 respondents) belong to external stakeholder groups (Figure 14). This distribution suggests that the majority of those seeking more training come from the external stakeholder group, reinforcing concerns regarding cybersecurity engagement and preparedness beyond Meyer Turku's internal workforce.

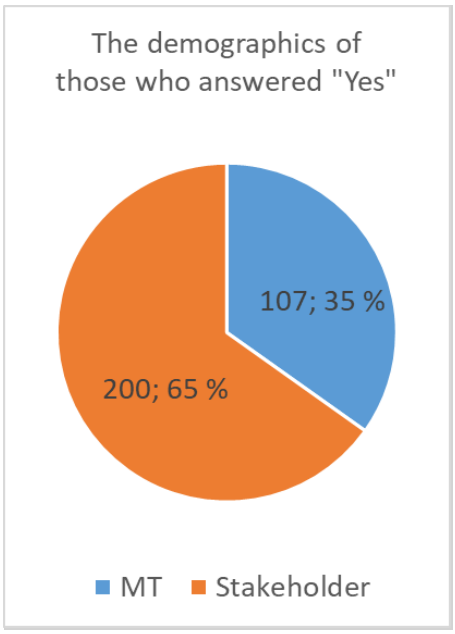


Figure 14 Q8 "Yes" answers MT employees vs. External stakeholders

A more focused look at external stakeholders (136 participants) reveals that only 26% (36 respondents) expressed the need for more training, while 74% (100 respondents) felt additional training was unnecessary (Figure 15). This finding suggests that most external stakeholders perceive their current cybersecurity knowledge as sufficient. However, a quarter of them still acknowledge a need for further training, which is a considerable proportion.

Figure 15 Q8 External stakeholders

When analysing these responses in conjunction with previous questions on cybersecurity training (Q6) and its effectiveness (Q7), an important trend emerges. As shown before in Figure 11, the majority (79%) of external stakeholders reported that they had not received any cybersecurity awareness

training at Meyer Turku shipyard. This raises concerns about whether the mandatory onboarding procedures at Meyer Turku adequately cover information security and whether training programs sufficiently engage external contractors, suppliers, and other third-party stakeholders. The results suggest a mismatch between the perceived need for training and the availability or quality of the training currently provided.

The lack of cybersecurity training for most external stakeholders, who include subcontractors, turnkey contractors, and suppliers, increases the risk of cyber vulnerabilities. Without adequate training, external stakeholder practices may not align with Meyer Turku's cybersecurity standards, leading to gaps in the overall security framework. Moreover, insufficient engagement with external stakeholders on cybersecurity best practices could result in data breaches or system disruptions, exposing Meyer Turku to compliance risks with maritime cybersecurity regulations such as IMO's Cyber Risk Management guidelines.

This segment of the survey analysis underscores an urgent need for Meyer Turku to enhance cybersecurity engagement with external stakeholders, ensuring that all actors within the shipyard ecosystem are equipped to handle the evolving challenges of a digitalized maritime industry.

Development suggestions:

- Targeted Training Programs: Meyer Turku could develop specialized cybersecurity training programs catering to both internal employees and external stakeholders. These programs should be tailored to the varying levels of cybersecurity exposure that different stakeholder groups encounter in their daily operations.
- Increased Focus on External Stakeholder Collaboration: A structured collaboration approach could help align external partners with Meyer Turku's cybersecurity policies, ensuring a unified security posture across all operations. Regular workshops and awareness sessions would be valuable in reinforcing best practices and compliance requirements.
- Ongoing Assessment and Adaptation: Regular evaluation of training effectiveness should be conducted to track improvements and identify emerging gaps. This approach would ensure that both internal and external stakeholders stay updated on cybersecurity threats and best practices in an ever-evolving landscape.

5.3 Cybersecurity Importance, Q9-Q16

The perception of cybersecurity's importance varies among different stakeholder groups, affecting how they prioritize security measures in their daily tasks. This section examines how respondents perceive the significance of cybersecurity within Meyer Turku's operations.

Survey questions in this section focus on identifying the digital and physical resources that external stakeholders consider critical for protection. Additionally, respondents provide insights into the reasons why cybersecurity should be prioritized, such as preventing cyberattacks, ensuring safety, maintaining trust, and complying with industry regulations. These responses help in understanding which aspects of cybersecurity are most valued by employees and external stakeholders.

Q9. "How important do you think cybersecurity is for Meyer Turku shipyard's operations? 1(Not important), 2 (Somewhat important), 3 (Neutral), 4 (Important), 5 (Extremely important)"

The pie chart (Figure 16) shows responses to the question Q9. 61% (186 respondents) rated cybersecurity as "5," indicating they view it as extremely important. 35% (107 respondents) rated it as "4," showing that a significant portion also considers cybersecurity to be very important. Combined, 96% of respondents (293 out of 307) recognize cybersecurity as critical to Meyer Turku shipyard's operations.

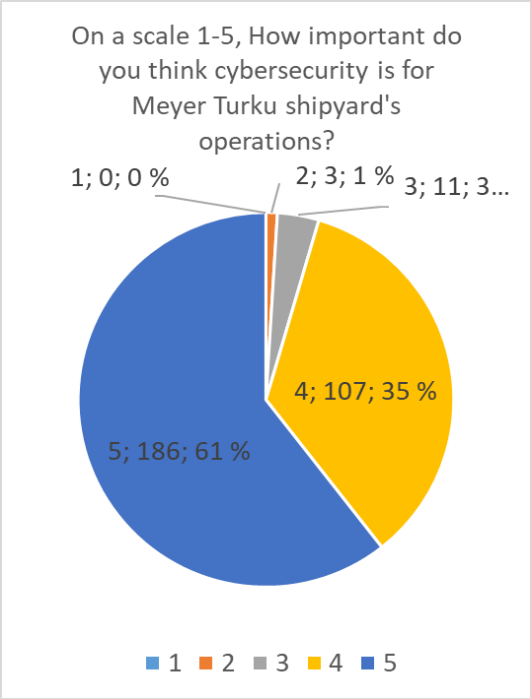


Figure 16 Q5 All respondents

3% (11 respondents) rated it as "3." moderate importance. Only 1% (3 respondents) rated it as "2.". 0% (0 respondents) rated it as "1,". This shows a very small minority who view cybersecurity as somewhat important or to be unimportant.

The data strongly suggests that cybersecurity is viewed as a critical aspect of Meyer Turku shipyard's operations. The majority of respondents (96%) believe it holds high to extremely high importance. This can be likely due to the increasing digitization of shipbuilding processes and cyberattacks that

become more known to the general population through media. This chart shows that cybersecurity is not necessarily just an operational priority but a bigger concern among Meyer Turku's employees and external stakeholders.

The responses from both MT employees and external stakeholders show results (Figure 17) that demonstrate a strong consensus across both groups. MT Employees: 63% rated cybersecurity as "5" (extremely important), and 33% rated it as "4," with negligible responses below this level. External Stakeholders: 58% rated cybersecurity as "5," and 37% rated it as "4," with similarly minimal responses for lower importance ratings.

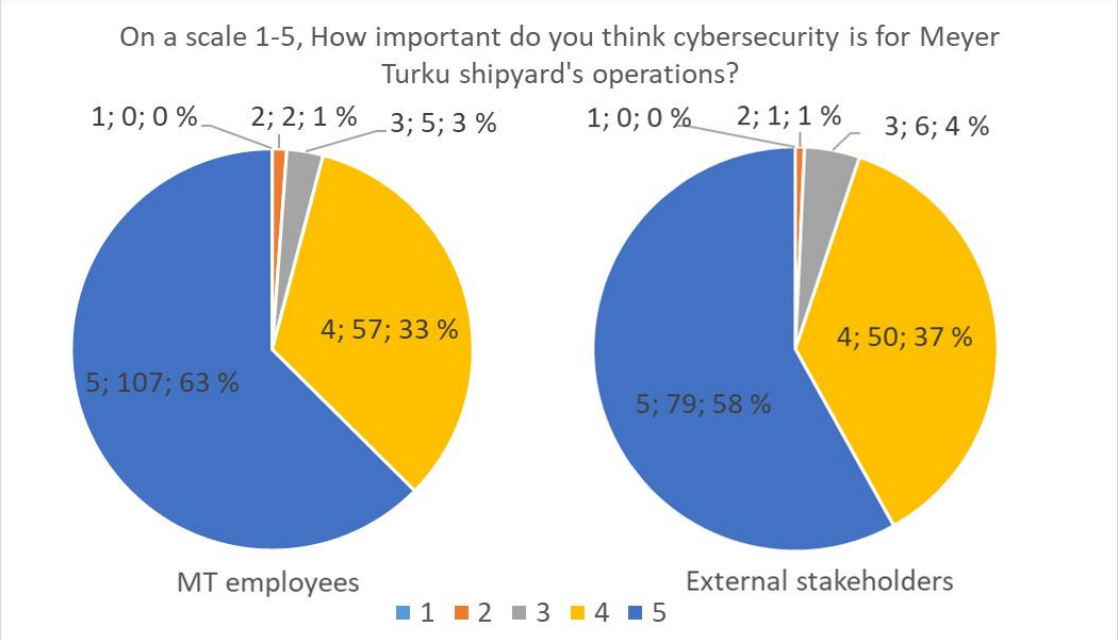


Figure 17 Q6 MT employee comparison to external stakeholders

The similarity between the two groups' responses confirms that both internal and external perspectives to be almost identical in recognizing the high importance of cybersecurity for Meyer Turku shipyard's operations.

Q10. Meyer Turku shipyard's operations involve various resources that require protection. Please select the types of resources you believe should be protected within the scope of cybersecurity efforts. Additionally, indicate their importance to you or your role. Check all that apply and rate their importance on a scale of 1 to 5. Scale: 1 = Not important, 5 = Extremely important.

The survey responses indicate a strong awareness among Meyer Turku's employees and external stakeholders regarding the importance of cybersecurity in protecting various resources. Both digital and physical assets received high importance ratings, underlining a broad recognition of potential vulnerabilities and the operational disruptions that could result from security breaches.

Kronodoc and Jira:

Kronodoc and Jira were among the most highly rated digital management tools (Figure 18 and Figure 19). These systems are crucial for project management, documentation, and quality control at Meyer Turku. A large proportion of respondents assigned them high importance ratings (4 and 5), demonstrating a shared understanding of their role in maintaining project efficiency and safeguarding sensitive data.

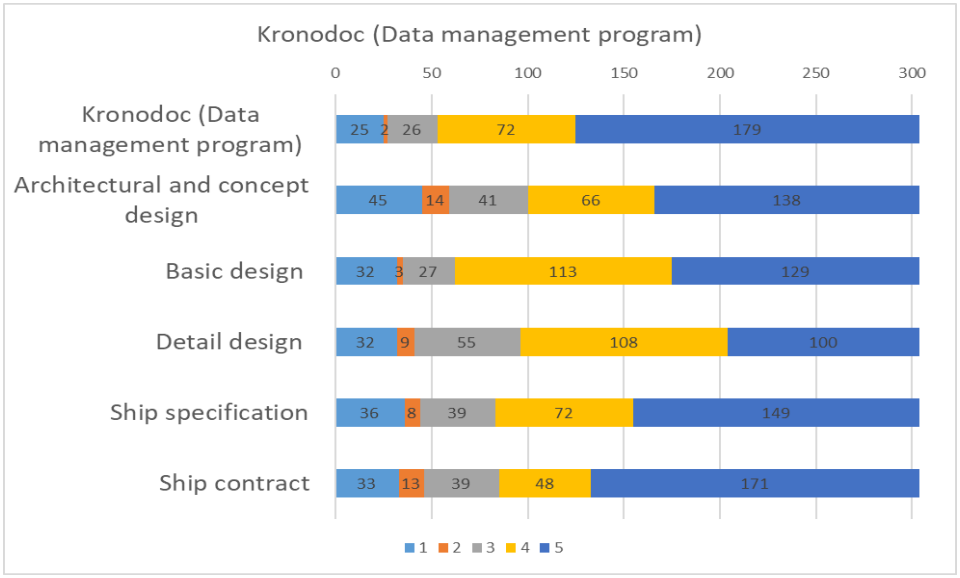


Figure 18 Q10 Data management section

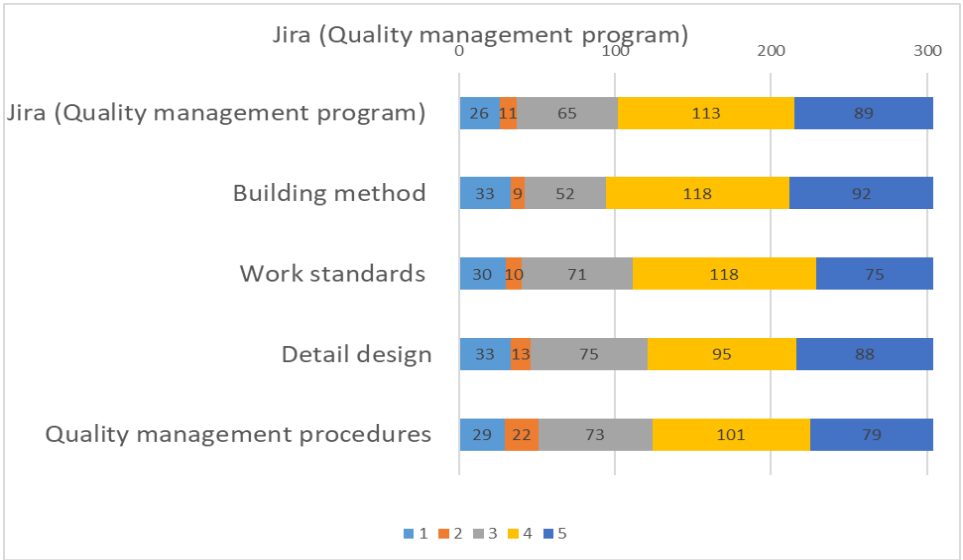


Figure 19 Q10 Quality management section

Given the centrality of these systems in managing documentation, work standards, and project tracking, any security breach could lead to delays, unauthorized data access, or financial loss. Employees and external stakeholders' dependent on these platforms recognize the risks, emphasizing the need for enhanced security measures.

Mars and SAP:

The Mars and SAP systems, which handle material procurement, production management, and planning schedules, also received strong ratings (Figure 20 and Figure 21). Their critical role in coordinating shipyard logistics and ensuring timely project execution makes them vital to cybersecurity considerations.

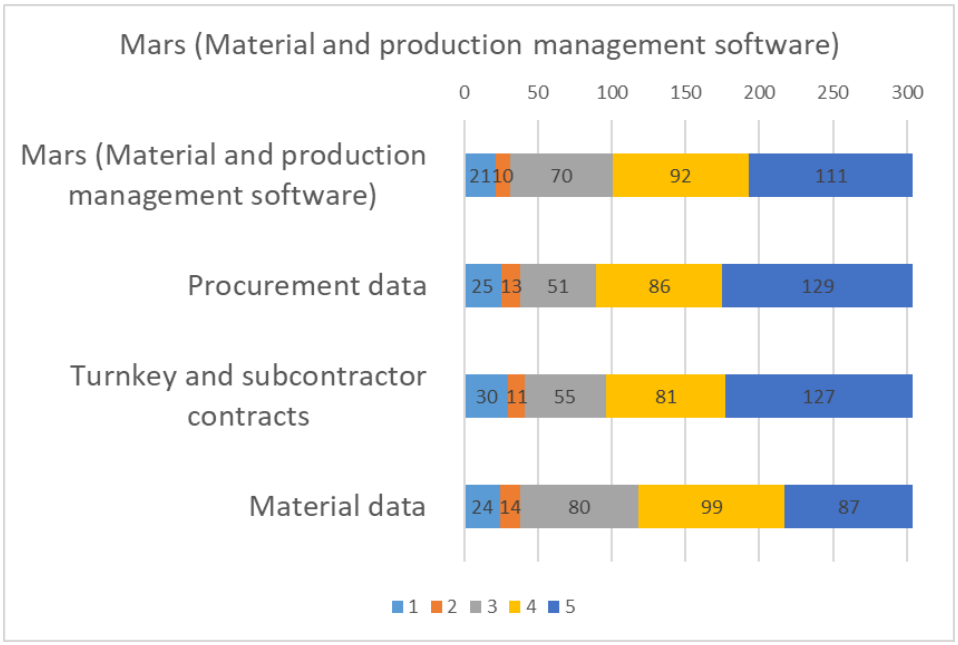


Figure 20 Q10 Material and production management section

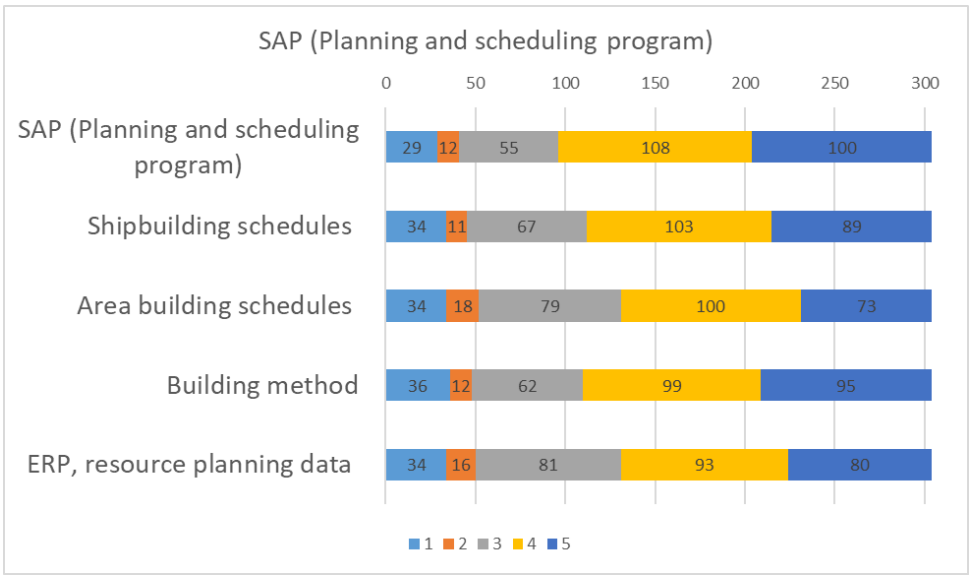


Figure 21 Q10 Planning and scheduling section

Compromising these systems could lead to disruptions in material deliveries, incorrect procurement data, or scheduling failures, all of which would significantly impact project costs and efficiency. The strong importance ratings indicate that respondents recognize the potential cybersecurity risks and the need for protection.

The importance of securing operational data was also highlighted in the survey responses. Data related to ship contracts, specifications, and design information (Figures 18 and 20) received consistently high ratings. These data sets contain sensitive intellectual property, contract details, and regulatory compliance information, making them valuable targets for cyber threats.

The results reinforce the necessity of strict access controls, encryption, and regular audits to prevent unauthorized access, industrial espionage, or data manipulation.

Critical Infrastructure and Physical Assets:

The importance of securing physical assets was reflected in the responses concerning critical infrastructure, docks, power generation, transport vehicles, and industrial control systems (Figure 22). High importance ratings across these categories indicate a broad awareness of the risks associated with physical breaches, including theft, sabotage, or disruptions caused by compromised operational technology.

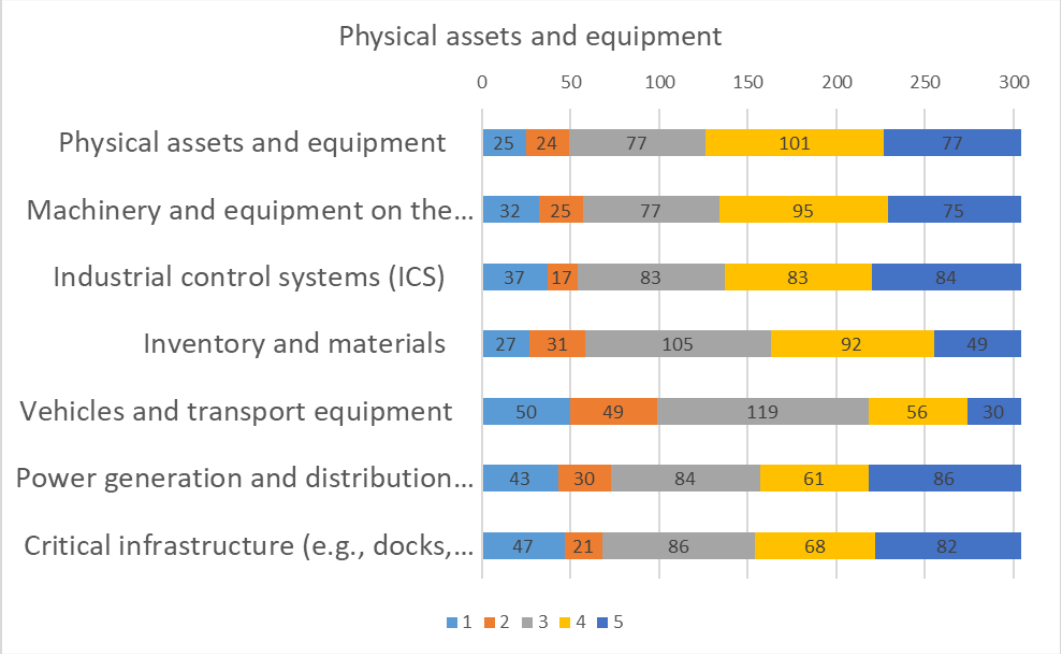


Figure 22 Q10 Physical assets

The fact that respondents rated power generation, machinery, and transport vehicles as critical security concerns suggests an understanding that cybersecurity measures must extend beyond digital networks to include physical access controls and surveillance mechanisms.

The physical nature of these assets, especially Vehicles and Transport Equipment, Inventory and Materials, makes them vulnerable to sabotage, theft, misplacement or accidental damage, all of which would have direct and immediate effects on operational capacity. Ensuring the security of these resources is crucial not only for the continuity of operations but also for preventing financial losses associated with asset replacement or repair.

Other Items:

Intellectual property, internal communication networks, and employee records were also identified as high-priority areas (Figure 23). These items received some of the highest importance ratings, emphasizing concerns related to data privacy, proprietary technology, and secure communications.

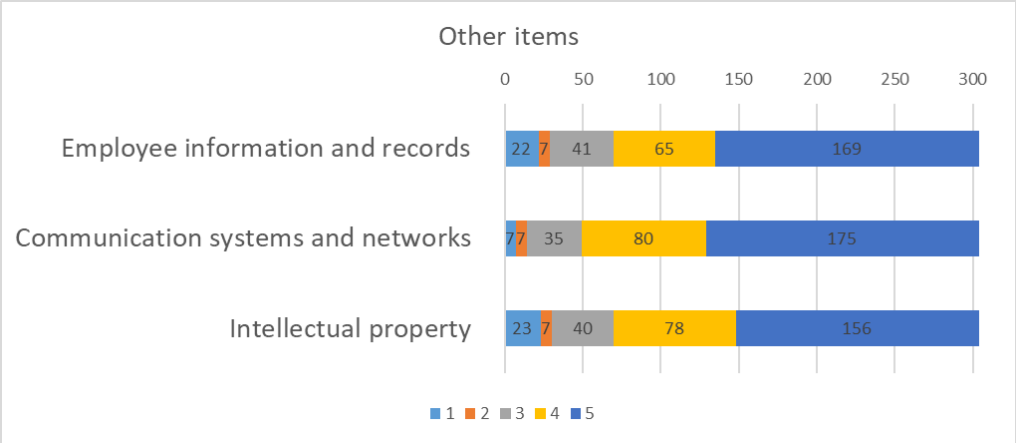


Figure 23 Q10 Other items

A breach in any of these areas could have severe consequences, including reputational damage, legal repercussions, or financial losses. The strong recognition of these cybersecurity concerns highlights the need for comprehensive protective measures that cover both digital information security and physical access management.

The protection of these items is critical as breaches could lead to loss of proprietary technology, violation of employee privacy, and disruption of internal and external communications. The high ratings suggest a mature understanding of the broad scope of cybersecurity, which includes all forms of data and communication, not just the operational tools.

The ratings reflect a well-rounded concern for both digital and physical assets, indicating that employees and external stakeholders are aware of the wide range of resources that need protection. The high ratings for different resources indicate that people recognize how cyber and physical security are connected in today's shipbuilding industry.

Development Suggestions:

- Enhanced Protection across All Rated Resources: Given the high importance ratings across various categories, Meyer Turku should ensure robust protection strategies that cover both digital management systems and physical resources.
- Regular Security Assessments and Upgrades: Conduct regular security assessments to identify vulnerabilities in both IT infrastructure and physical assets. Upgrading security measures where necessary will help protect against evolving threats.

- Training and Awareness Programs: Continued education and awareness programs focusing on the specific types of resources identified by employees and external stakeholders will help maintain a high level of vigilance and proactive security practices.
- Stakeholder Collaboration: Since both employees and external stakeholders interact with these resources, fostering a collaborative approach to security practices can help ensure comprehensive protection.

The survey findings confirm that Meyer Turku's workforce and external stakeholders understand the importance of cybersecurity in protecting both digital and physical assets. This awareness is a strong foundation for improving cybersecurity practices. However, continuous investment in training, technology, and security protocols is necessary to adapt to evolving threats. Strengthening these areas will protect the shipyard's assets and protect its competitive position in the maritime industry.

Q11 OPTIONAL. Is there anything else, not mentioned above, that you believe is important to consider in the context of cybersecurity at Meyer Turku shipyard? If so, please specify.

Given that only 36 out of 307 respondents chose to answer these optional questions, the data suggests that while a minority, these participants are notably engaged and possibly more aware or concerned about specific cybersecurity aspects not covered by general policies or not widely recognized within the shipyard. This subset of responses offers valuable insights into nuanced areas of cybersecurity that may not be on the radar of the broader workforce but are critical to the overall security posture of the shipyard. The responses ranged widely from technical aspects like AI system use and 3D model protection to organizational measures like clearer access rights management and enhanced physical security controls.

Those who responded are likely in positions where the gaps in cybersecurity measures are most evident or have potentially experienced or understood the ramifications of these gaps, prompting them to highlight these specific concerns.

Some issues like the management of supplier bank information, the physical access controls within the shipyard, and the role-based access rights to critical systems were highlighted by respondents, pointing to potential oversight areas.

"Alihankijoiden tietoturvallisuus" - "Subcontractors' data security"

"Verkoston sidonnaisuudet. Esimerkiksi kiinariippuvuudet yms. KT toimittajilla, systeemitoimittajilla ja suunnittelutoimistoilla." - "Network affiliations. For example, interdependencies, etc. KT suppliers, system suppliers and design offices."

“Toimittajien pankkitietojen hallinta ja siihen liittyvien dokumenttien hallinta ja välitys toimittajan ja Meyer Turku Oy:n / tytäryhtiöiden kanssa” - "Management of suppliers' bank details and related documents and communication with the supplier and Meyer Turku Ltd/subsidiaries."

There may be a broader under-recognition or underestimation of certain cybersecurity risks among the general workforce, which could leave Meyer Turku vulnerable to specific threats that these engaged respondents have identified.

“Suurin osa noista arvoitavista ohjelmista ovat minulle tuntemattomia” - "Most of the programmes being evaluated are unknown to me"

Several respondents focused on the technical aspects of cybersecurity, such as the protection of 3D models and the implications of AI system usage. These concerns are indicative of the evolving technological landscape within the shipyard, where advanced tools and systems are integral to design and production processes.

“3D-mallin suojaaminen (Cadmatic)” - "3D model protection (Cadmatic)"

“AI system use and policy”

The mention of AI and CAD systems like Cadmatic reflects an understanding that these technologies, while enhancing capabilities, also introduce specific vulnerabilities that could be exploited to access proprietary designs or manipulate data.

Another major theme that emerged involves the organizational aspects of cybersecurity. For instance, the management of access controls, both digital (ID and system access) and physical (entry points and visitor management), was frequently cited. Respondents expressed concerns about the current processes being insufficiently rigorous or lacking in enforcement, such as the ongoing access rights of former employees or subcontractors, which could lead to unauthorized access to sensitive information or critical systems.

“ID and ACCESS control cards/ system”

“Fyysinen pääsynhallinta telakan sisällä” - "Physical access control within the yard”

“Parakkitoimistojen päätyovien lukitus on täysin valvomaton. Vierailijoille pitäisi olla oma vieralutila; heitä ei tulisi päästää perussuunnittelun tilohin.” - "The main doors of the barrack offices are completely unlocked. Visitors should have their own guest room; they should not be allowed into the basic design spaces."

The physical security measures currently in place may be insufficient or outdated, failing to keep pace with evolving security needs and technological advancements in shipyard operations.

Some respondents demanded for more extensive and regular cybersecurity training. This suggests a perceived gap in the current educational measures provided to the shipyard's workforce. Respondents pointed out the absence of widespread cybersecurity training that addresses both general awareness and specific operational risks associated with various job roles. This indicates a recognition that while some employees may be well-versed in cybersecurity protocols, a uniform level of knowledge and vigilance across all employees is crucial to effectively safeguarding the shipyard against cyber threats.

“Vaikka kaikki tietojärjestelmät olisi teknisillä välineillä (ohjelmistot, fyysinen suoja) suojattu viimisen päälle, ihmisten tietoisuus asiasta ja oikea tapa toimia on kaiken perusta.”- "Even if all information systems are protected by technical means (software, physical protection), people's awareness and the right way of doing things is the basis"

”Ihmisten ohjaus kyseenalaistamaan tietopyyntöjä.” - "Guiding people to question requests for information"

”Parempi perehdytys, tiedän monta työntekijää jotka eivät ole käyneet tietoturvakoulutusta ja ovat melkoinen riski.” - "Better training, I know many employees who have not undergone security training and are quite a risk."

Interestingly, some responses reflected external stakeholder-specific insights, emphasizing the need for cybersecurity practices that extend beyond the internal workforce to include contractors, suppliers, and other external parties involved in the shipyard's operations. The mention of external groups having potentially excessive access to internal systems or retaining access post-contract illustrates a critical awareness of the risks posed by extended enterprise security.

“Verkoston sidonnaisuudet. Esimerkiksi kiinariippuvuudet yms. KT toimittajilla, systeemitoimittajilla ja suunnittelutoimistoilla.” - "Network ties. For example, interdependencies, etc. KT suppliers, systems suppliers and design agencies"

”Alihankijoiden tietoturvallisuus” - "Subcontractor cybersecurity"

“ymmärrys alihankkijoiden käytön vaikutuksesta kyberturvallisuuteen” - “Understanding the impact of using subcontractors on cybersecurity"

“Due to SUBCONTRACTOR being a supplier to MT we do not use MT systems or infrastructure"

Q12. OPTIONAL. Please rate the importance of your added resource or item in regards of cybersecurity from the previous question.

The replies had consistently high importance ratings (4-5) given to all of these concerns. It suggests that these specific respondents are not only aware of but are also significantly concerned about these

specific vulnerabilities. Overall, the variety of responses gathered from the optional questions paints a picture of a workforce that is not only aware of the general need for cybersecurity but is also acutely aware of the specific vulnerabilities and risks associated with various aspects of their work environment. This detailed feedback is invaluable for developing a more comprehensive and effective cybersecurity strategy that addresses both broad and specific concerns, ensuring protection across all sides of the shipyard's operations.

Development Suggestions:

- Targeted Cybersecurity Awareness and Engagement using these responses to pilot specific cybersecurity enhancements in departments or areas directly affected by these issues.
- Conduct focused group discussions or workshops to delve deeper into the concerns raised by these respondents to understand their perspective better and to disseminate their insights across the broader employee base.
- Comprehensive Review of Cybersecurity Policies. Integrating the insights from these optional responses into the broader cybersecurity strategy to address niche but significant risks.
- Enhance Physical Security Protocols. Upgrading and expanding physical security systems to include more stringent access controls, monitored entry points, and visitor segregation to safeguard sensitive operational areas.
- Regularly audit physical security measures to ensure they meet current security standards and address any new vulnerabilities that emerge.

The engagement and concerns of this informed minority (36 respondents) are crucial for pre-empting potential cybersecurity issues that might not yet be widely acknowledged across Meyer Turku. By addressing these specific points raised in the optional responses, Meyer Turku can enhance its cybersecurity framework to be more inclusive and comprehensive, ensuring protection against both recognized and emerging threats. This approach not only strengthens the shipyard's defences but also fosters a more security-aware culture among all employees and external stakeholders.

Q14. OPTIONAL. Do you believe there are additional resources or aspects that should be considered for protection within Meyer Turku shipyard's operations? Please share your thoughts and suggestions:

The survey question Q14 had only 24 responses out of 307 participants providing their thoughts and suggestions. The questions aim was to receive responses that address potential areas for improvement in cybersecurity practices at Meyer Turku Shipyard. Even though the number of replies were small, the replies showed perceived vulnerabilities and suggestions for enhanced security measures.

The diversity of responses suggests a varying degree of concern and awareness among respondents regarding cybersecurity's scope and its integration within operational protocols. The focus extends beyond traditional IT security to operational technology, physical security, and protection of proprietary and sensitive information.

A recurring theme is the call for increased awareness and training among employees. This implies that current efforts might not be comprehensive or penetrating enough to address all employee levels or departments effectively.

“Tietoisuuden lisääminen on avain myös tietoturvallisuuden parantamiseksi.” - "Raising awareness is also key to improving data security."

There are multiple calls for improving access control systems and identity management, suggesting current measures may not adequately restrict access to sensitive systems and information, potentially leaving gaps for internal misuse or external breaches.

”Kyllä, identiteetin ja pääsynhallinta on yhtä tärkeää kuin aidat ja portit, ellei jopa tärkeämpää.” - "Yes, identity and access management is as important as, if not more important than, fences and gates."

”Identiteetti- ja pääsynhallinta on retuperällä” - "Identity and access management is backward"

Concerns about vendor management, particularly with respect to how external contractors and suppliers handle sensitive information, indicate possible deficiencies in vendor security policies or their enforcement.

”Toimittajien pankkitietojen hallinta ja siihen liittyvien dokumenttien hallinta ja välitys toimittajan ja Meyer Turku Oy:n / tytäryhtiöiden kanssa.” - "Management of suppliers' bank details and related documents and communication with the supplier and Meyer Turku Ltd/subsidiaries."

”tarkkuuttaa alihankintaverkostolle jaettavaan tietoon” - "accurate information to be shared with the subcontractor network"

Some responses highlight concerns about physical security measures and the need for better surveillance and locking systems for both digital assets and physical premises.

”Tietokoneita EI jätettäisi lukitsematta työpisteeltä poistuttaessa” - "Computers should NOT be left unlocked when leaving the workplace"

”Kyllä, laivan rakennusaikaiseen valvontaan pitäisi asettaa enemmän paukkuja.” - "Yes, more effort should be put into monitoring the ship during construction."

Suggestions for more robust planning for crisis situations indicate a perceived need for better preparedness against potential cyber-attacks or other disruptions.

”Onko tehty poikkeusoloja varten suunnitelmia ja jos niin mitä?” - "Have there been any contingency plans, and if so, what?"

Development Suggestions:

- Enhanced Cybersecurity Training: Implement regular, mandatory training sessions tailored to different employee roles to increase cybersecurity awareness and skill across the organization.
- Robust Access Management: Strengthen identity and access management protocols, ensuring that access rights are closely aligned with job requirements and promptly revoked when no longer needed.
- Vendor Security Assessments: Conduct thorough security assessments of vendors and third-party service providers to ensure compliance with the shipyard’s cybersecurity standards.
- Physical Security Upgrades: Improve surveillance and access control systems at physical locations to prevent unauthorized access to sensitive areas.
- Crisis Management Planning: Develop and regularly update comprehensive response plans for various cybersecurity incidents, ensuring readiness for quick and effective action.

The qualitative insights from the survey responses underscore a notable concern among respondents about various aspects of cybersecurity at Meyer Turku Shipyard. There is a clear indication that while there may be a solid foundation for cybersecurity, there are significant areas for improvement, particularly in employee training, access control, third-party management, and crisis preparedness. Addressing these concerns through targeted strategies could substantially enhance the overall security posture of the shipyard, safeguarding against both current and emerging cyber threats.

Q15. Have you ever encountered a cybersecurity incident or breach at Meyer Turku shipyard or in your role as a stakeholder?

The replies in Figure 24 indicated that 258 stated “No” and 49 “Yes”. The number of "Yes" responses suggests that while cybersecurity incidents are not exceedingly common, they are not rare either. Almost 16% of respondents have encountered an incident, which is significant enough to warrant attention and action.

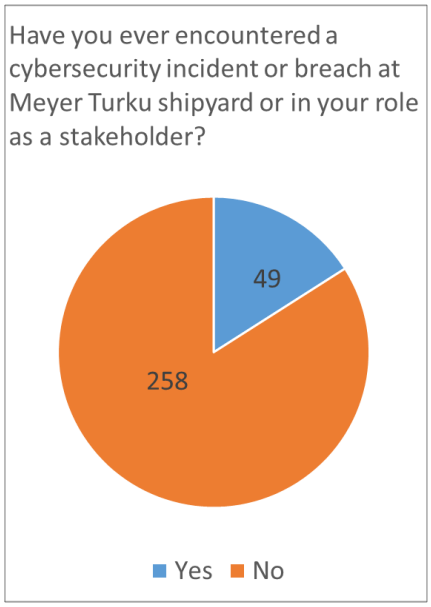


Figure 24 Q15 All respondents

In Figure 25 from the 49 “Yes” replies, 40 replies were from Meyer Turku employees and 9 from external stakeholders, mainly Turnkey contractors and Subcontractors.

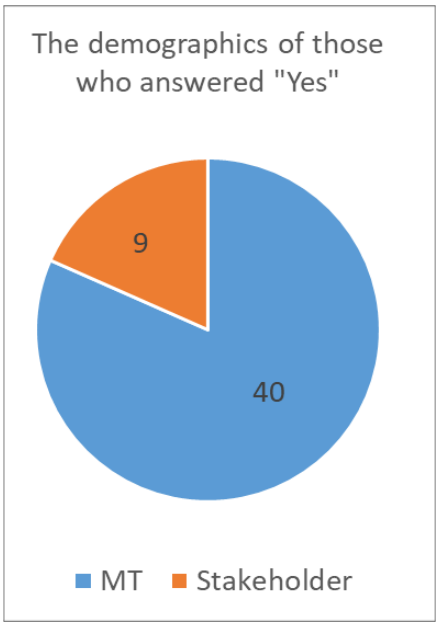


Figure 25 Q15 "Yes" answers, MT employees and external stakeholders

Experience Level and Risk Exposure:

The data In Figures 26 and 27 show an even spread across different experience levels with both the shipbuilding industry and Meyer Turku specifically. This indicates that cybersecurity incidents affect employees and external stakeholders regardless of their tenure. More seasoned employees (those with more than 20 years) might have different types of exposure to cybersecurity risks due to potentially broader access to information and systems over time. A notable number of incidents involve

individuals with fewer years of association, which may imply that newer employees and external stakeholders might not be fully aware of existing threats or the best practices to mitigate them. It's also possible that the likelihood of reporting an incident may vary with the level of experience, where long-tenured individuals may be more aware of what constitutes an incident and thus more likely to report.

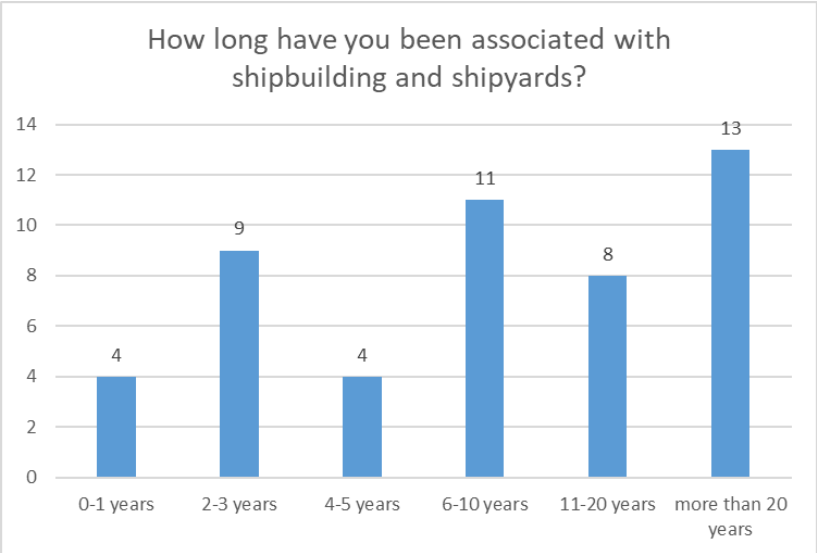


Figure 26 Association with shipbuilding (Q3) for the demographic that replied “Yes” in Q15

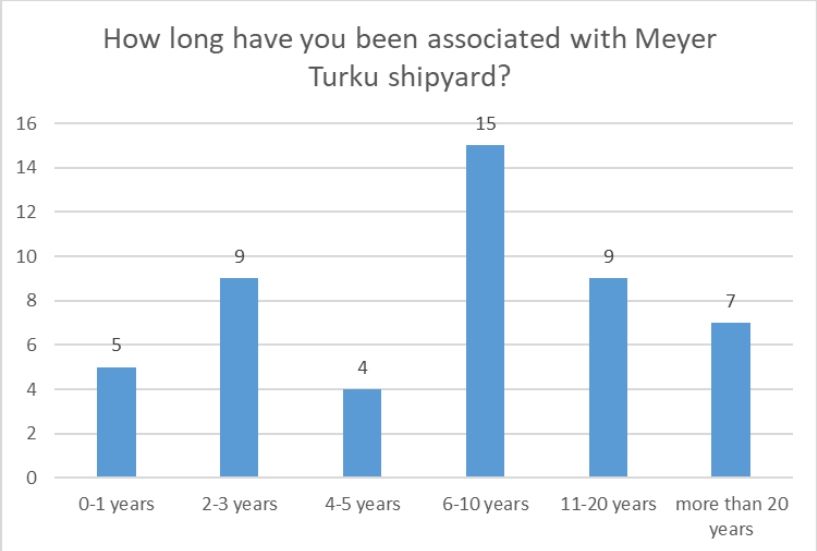


Figure 27 Association with Meyer Turku (Q4) for the demographic that replied “Yes” in Q15

Q16 Optional. If you answered yes to question 15, please briefly describe the incident or breach (optional)

The responses to this question provide detailed insights into the various cybersecurity incidents encountered at Meyer Turku. The sheer variety and severity of incidents reported indicate systemic vulnerabilities across multiple areas, including financial fraud, unauthorized access, data leaks, corporate espionage, phishing, and physical security breaches.

A notable trend in the responses is that most incidents were reported by Meyer Turku employees rather than external stakeholders. This could indicate two key concerns: either employees face a higher volume of cybersecurity threats due to their direct access to critical systems, or they are more aware of security policies and feel more obligated to report incidents. The low reporting rate from subcontractors, turnkey contractors, and other external suppliers raises significant concerns regarding their level of cybersecurity awareness and their willingness or ability to recognize and report security breaches. This lack of reporting suggests gaps in cybersecurity training and policies for external stakeholders, making it imperative to extend awareness programs, access control measures, and security reporting mechanisms beyond Meyer Turku's direct workforce.

The severity of incidents reported highlights serious security risks that, if left unaddressed, could lead to financial losses, operational disruptions, reputational damage, and regulatory consequences. The responses confirm that Meyer Turku faces a rapidly evolving cybersecurity landscape, requiring continuous adaptation and proactive defence measures.

Social Media Leakage and Press Leaks

A recurring issue mentioned in the responses is the unauthorized sharing of sensitive images and information on social media platforms. Employees admitted to witnessing confidential shipbuilding-related content being shared publicly. One respondent noted:

"Eräs kollega jakoi telakan sisäisiä kuvia sosiaalisessa mediassa. Hän ei varmaan ymmärtänyt, että ne olivat luottamuksellisia."

"A colleague shared internal shipyard images on social media. He probably didn't realize they were confidential."

Another respondent described a case where Meyer Turku's confidential information appeared in public maritime news:

"Löysin erään julkaisun, jossa esiteltiin telakan projektidokumentteja, joita ei olisi pitänyt olla kenenkään ulkopuolisen saatavilla."

"I found a publication showcasing the shipyard's project documents, which should not have been accessible to outsiders."

These incidents indicate insufficient awareness about the sensitivity of company information and the lack of clear internal policies regarding external communication. Public leaks can damage the company's reputation, provide competitors with strategic insights, and pose security risks.

Banking Information Fraud, Email Compromise, and Access Control Issues

Another major cybersecurity concern raised in responses involves fraudulent banking information, email hijacking, and unauthorized access to key systems. Several employees shared experiences related to phishing attacks targeting suppliers and financial fraud attempts. One response highlighted a real-world financial fraud attempt:

"Saatiin sähköposti, jossa esiintyi tuntemamme toimittaja ja ilmoitti pankkitietojen muuttumisesta. Kävi ilmi, että se oli huijausviesti."

"We received an email impersonating a supplier we work with, informing us of a change in banking details. It turned out to be a fraud attempt."

Access control issues were also widely reported, with employees highlighting cases of former employees retaining system access long after their departure:

"Huomasin, että entisellä työntekijällä oli vielä pääsy Kronodociin kuukausia sen jälkeen, kun hän oli lähtenyt yrityksestä."

"I realized that a former employee still had access to Kronodoc months after leaving the company."

This suggests inadequate enforcement of post-employment access revocation policies, leaving potential vulnerabilities that could be exploited for data breaches.

Data Exfiltration and Corporate Espionage:

A particularly serious concern raised by multiple respondents was data exfiltration by former employees and external actors. One alarming response described a former employee transferring sensitive shipyard data abroad:

"Eräs työntekijä vei mukanaan laivan suunnitteludokumentteja ja tietoja Kiinaan. Tämä huomattiin vasta myöhemmin."

"A former employee took ship design documents and information to China. This was only discovered later."

Other respondents mentioned unauthorized file downloads and corporate espionage investigations, reinforcing the idea that intellectual property protection is a major cybersecurity challenge.

"Yritysvakoilua tutkitaan parhaillaan. Meillä on syytä uskoa, että jokin ulkopuolinen taho on saanut käsiinsä luottamuksellisia tietoja."

"Corporate espionage is currently under investigation. We have reason to believe that an external party has accessed confidential information."

These incidents highlight the need for strict data monitoring policies and legal frameworks to address data exfiltration.

Phishing, Social Engineering, Physical Security, and Malware Intrusions:

Phishing attacks and social engineering tactics were frequently mentioned, with employees falling victim to email scams and malicious links. One respondent described an incident where an employee unknowingly compromised their credentials:

"Työkaveri avasi linkin sähköpostista, joka näytti tulevan IT-osastolta. Hän antoi tunnuksensa ja joutui huijauksen uhriksi."

"A colleague opened a link from an email that appeared to be from IT. He entered his credentials and became a victim of a scam."

Concerns about physical security breaches were also raised. Employees observed workstations left unlocked and unauthorized access to sensitive areas:

"Monet jättävät työasemansa lukitsematta tauoilla. Kuka tahansa voisi päästä käsiksi tietoihin."

"Many employees leave their workstations unlocked during breaks. Anyone could access sensitive information."

Malware intrusions and near cyberattack incidents that threatened shipbuilding operations were also noted:

"Järjestelmään havaittiin tunkeutumisyritys, joka olisi voinut pysäyttää tuotannon. Onneksi se huomattiin ajoissa."

"An intrusion attempt was detected in the system that could have halted production. Fortunately, it was caught in time."

Based on the earlier data on cybersecurity training, it appears that even though some employees have received training, security incidents are still happening. Additionally, a large part of the workforce has not been trained. This might suggest either a gap in the training coverage or content. High number of “No” responses might indicate that cybersecurity measures are effective for a majority of employees or external stakeholders. However, it could also suggest varying levels of awareness and reporting. Some individuals might not recognize what constitutes a cybersecurity incident, or they might not report minor incidents they deem inconsequential. It is also possible that some incidents go unreported

due to the lack of awareness or fear of repercussions, meaning the actual number of incidents could be higher.

The diversity and severity of incidents reported confirm that Meyer Turku faces an extensive range of cybersecurity threats, from email fraud and unauthorized access to industrial espionage and physical security lapses. The responses paint a picture of a cybersecurity landscape under continuous attack, where adversaries are exploiting human error, weak policies, and unprotected digital and physical assets.

The variety of cyber threats targeting Meyer Turku demands an equally comprehensive and adaptive defence strategy. Attackers are constantly evolving their tactics, and Meyer Turku must proactively strengthen its security posture to prevent significant financial losses, operational disruptions, and reputational damage.

Meyer Turku's dependency on external stakeholders clearly introduces an additional layer of risk, as external stakeholders may have weaker security postures than the company itself. A compromised vendor or contractor could serve as a weak entry point for an attack. It is, therefore, critical to extend security policies, training, and enforcement beyond Meyer Turku's immediate workforce.

Given the severity of these challenges, immediate action is required to strengthen cybersecurity awareness, implement stricter access controls, and enhance reporting mechanisms across all respondents.

Development suggestions:

- Extend Training to All Stakeholders: Implement mandatory cybersecurity awareness and training programs for all stakeholders involved in operations at the shipyard. This should include tailored content relevant to the risks and interfaces they handle.
- Monitor and Enforce Compliance: Regularly audit stakeholder compliance with cybersecurity training and practices and include cybersecurity requirements in contractual agreements.
- Awareness Campaigns: Launch cybersecurity awareness campaigns specifically designed for external stakeholders, emphasizing the importance of recognizing and reporting security incidents.
- Easy Reporting Mechanisms: Establish clear, simple, and accessible incident reporting mechanisms for all stakeholders to encourage prompt reporting of potential threats or breaches.

- Comprehensive Security Culture: Developing a comprehensive security culture that encompasses not just employees but also external stakeholders is essential. This culture should promote continuous education, vigilance, and shared responsibility for cybersecurity.
- Insider Threat Program: Establish a formal insider threat program that includes employee monitoring, behavioural analysis, and clear consequences for violations of company policy.
- Promote a Security Culture: Foster a culture of security within the organization where employees feel responsible for maintaining cybersecurity and are encouraged to report suspicious activities.
- Third-Party Risk Management: Develop a comprehensive third-party risk management program that includes risk assessments, periodic audits, and the enforcement of cybersecurity standards through contractual agreements.
- Stakeholder Engagement: Conduct cybersecurity awareness sessions for all stakeholders, including contractors and suppliers, to ensure they understand and comply with Meyer Turku's cybersecurity policies.
- Strengthen Physical Security: Enhance physical security measures, such as securing workstations, using biometric access controls, and implementing strict policies for securing devices when not in use.
- Enhance Network Security: Invest in advanced network security solutions, including firewalls, intrusion detection systems, and regular security audits to identify and mitigate vulnerabilities.

5.4 Cybersecurity Practices: Q17, Q18, Q19

Understanding cybersecurity awareness and its importance is only part of the picture—actual implementation of security practices is what ultimately determines the resilience of an organization. This section evaluates whether respondents actively apply cybersecurity measures in their daily work at Meyer Turku.

The analysis includes self-reported adherence to best practices, such as following the CIA Triad principles, using strong authentication methods, and complying with organizational cybersecurity policies. Additionally, respondents were asked to suggest improvements for enhancing security measures at the shipyard, offering valuable insights into practical challenges and potential areas for development.

Q17. Did you have prior knowledge of CIA best practices before?

Among the total respondents, 121 out of 306 (about 40%) indicated they had prior knowledge of Confidentiality, Integrity, and Accessibility (CIA) best practices in Figure 28. This highlights a moderate level of baseline cybersecurity knowledge within the respondents but points out that a significant portion, nearly 60%, may lack fundamental understanding, increasing vulnerability to cyber threats.

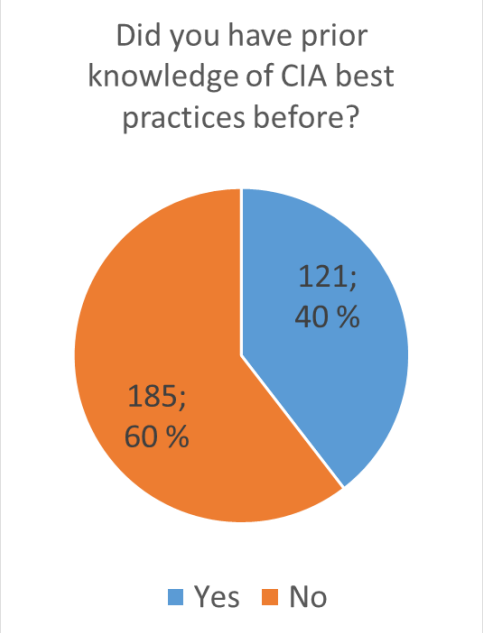


Figure 28 Q17 All respondents

The level of cybersecurity awareness and its perceived importance within Meyer Turku shipyard is likely to vary widely among different external stakeholder groups due to their diverse roles and degrees of access to sensitive information. Differences in awareness levels may stem from variations in training, exposure to cybersecurity protocols, and the nature of the stakeholders' interaction with digital and physical assets.

Q18. Do you follow cybersecurity best practices in your day-to-day work at Meyer Turku shipyard or in your role as a stakeholder to ensure the Confidentiality, Integrity, and Accessibility (CIA) of protected resources?

The data in Figure 29 reveals that 178 out of 306 respondents (approximately 58%) always follow cybersecurity best practices, indicating strong compliance and an active commitment to cybersecurity by a majority of the participants.

However, 98 out of 306 respondents (about 32%) only often adhere to these practices, and a smaller number sometimes or rarely follow, suggesting gaps in consistent application across all operations.

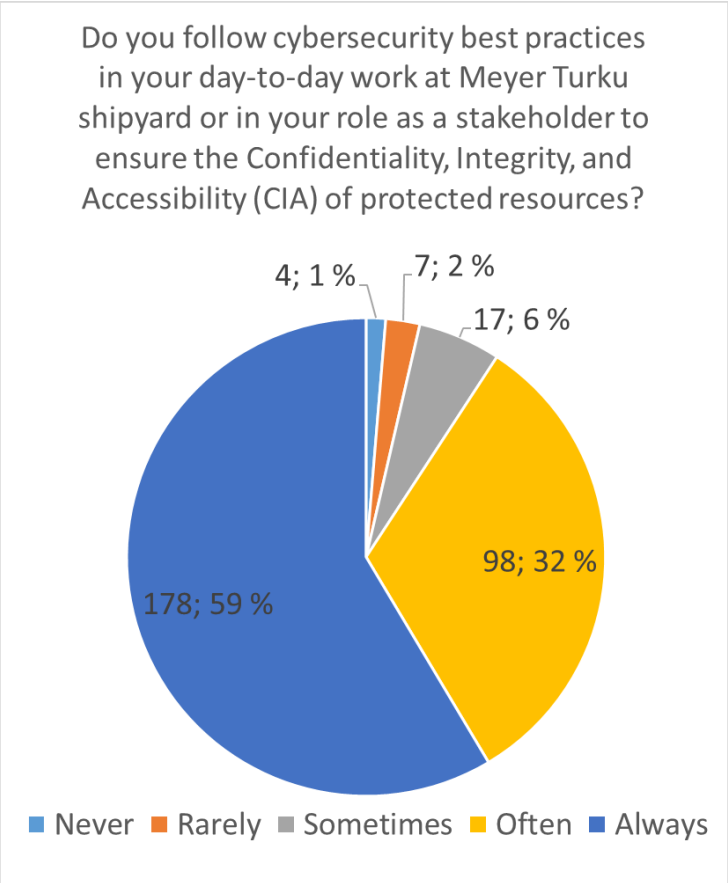


Figure 29 Q18 All respondents

The gap in prior knowledge and the fluctuating adherence rates may reflect a need for more robust, consistent training and communication about the importance and implementation of cybersecurity measures. Respondents directly involved with critical systems or sensitive data might exhibit higher adherence due to the direct risks associated with their roles.

Among external stakeholders (Figure 30), 56 out of 136 (41%) indicated having prior knowledge of CIA best practices. This suggests a moderate level of baseline cybersecurity awareness within this group, which is lower compared to internal employees. This could be attributed to less frequent cybersecurity training or varying levels of engagement with the shipyard's internal cybersecurity policies.

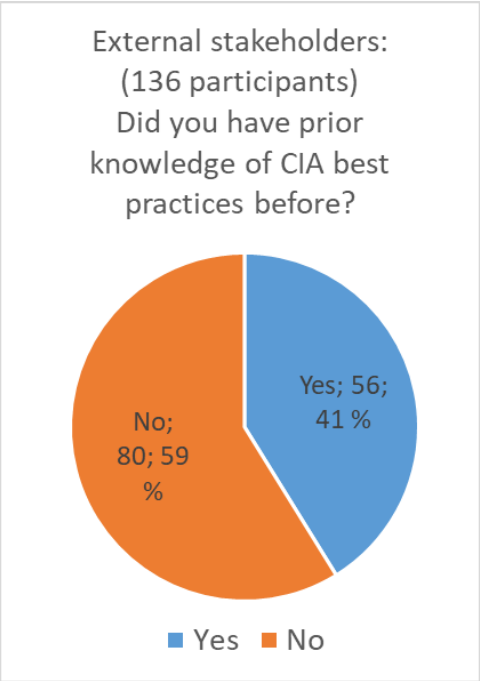


Figure 30 Q17 External stakeholders

In Figure 31 a significant 60% (82 out of 136) of external stakeholders reported that they 'Always' follow cybersecurity best practices, which is commendably high and crucial for maintaining secure operations. However, 29% (39 out of 136) only 'Often' follow the practices, and a smaller percentage sometimes, rarely, or never adhere, indicating potential vulnerabilities.

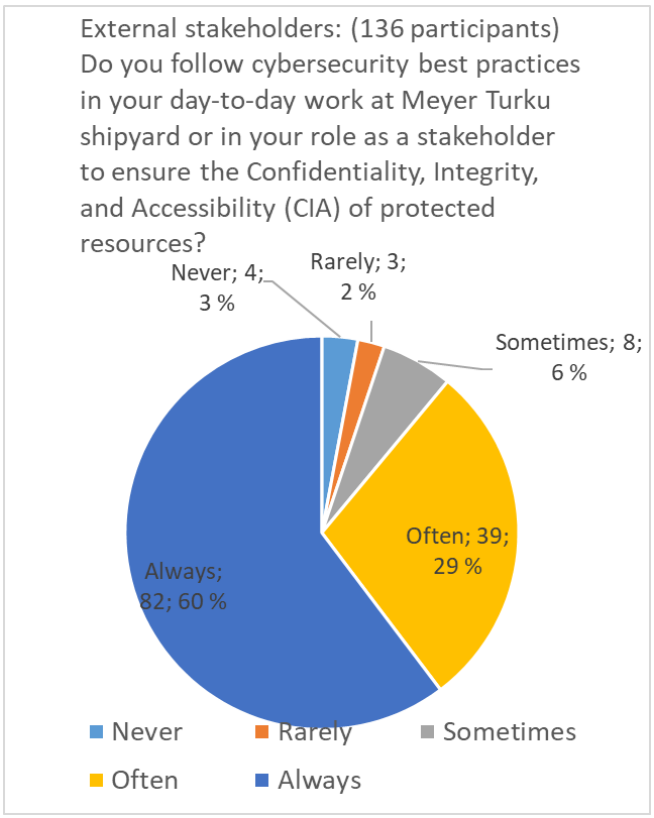


Figure 31 Q18 External stakeholders

The strong adherence rate could be influenced by the operational requirements and contractual obligations imposed by Meyer Turku as part of their risk management strategy.

External stakeholders who frequently interact with sensitive data or systems may be more likely to adhere to cybersecurity best practices due to the higher perceived risk and the direct consequences of a breach. The variance in adherence among external stakeholders might be impacted by the degree of cybersecurity training provided by Meyer Turku or the external stakeholders' own organizations. Those with less exposure to formal training or less stringent internal policies might not adhere as strongly.

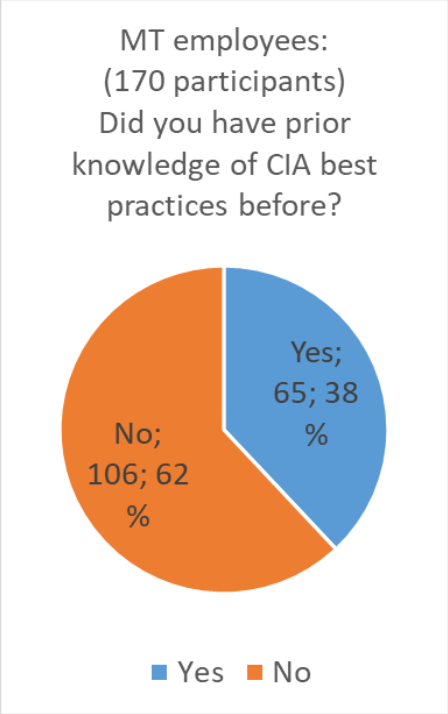


Figure 32 Q17 MT employees

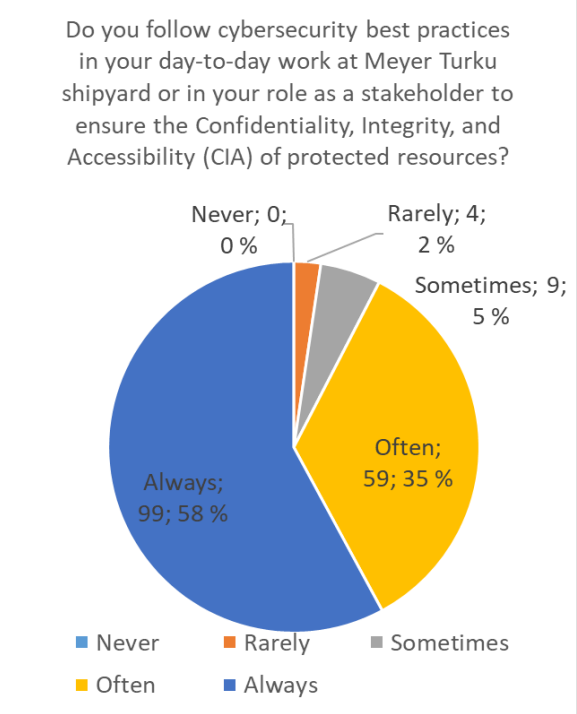


Figure 33 Q18 MT employees

Among MT employees (Figure 32), 38% (65 out of 170) reported having prior knowledge of CIA best practices. This suggests a similar situation of the awareness of the internal workforce to external stakeholders. The high rate of adherence to cybersecurity best practices among both MT employees and external stakeholders is encouraging and suggests cybersecurity culture is being considered at Meyer Turku.

However, the knowledge gap in nearly 40-60% of the respondents highlight an area for improvement. By addressing this through comprehensive training and clear policies, Meyer Turku can further enhance its overall cybersecurity resilience, protecting both its operations and its collaborative ventures.

Q19: Do you think there are specific cybersecurity measures or practices you think should be implemented or improved at Meyer Turku shipyard to better ensure the CIA of the resources you identified in this survey?

The responses to Q19 highlight a mix of confirmation, uncertainty and recommendations regarding the implementation and improvement of cybersecurity measures to ensure the Confidentiality, Integrity, and Availability (CIA) of resources at Meyer Turku shipyard.

A significant number of respondents explicitly stated that cybersecurity measures should be implemented or improved:

"Kyllä." – ”Yes”

"Toimintaa pitää kokoajan kehittää, koska hyökkääjät kehittyvät myös." - "You have to improve all the time, because the attackers are also improving."

"Aina on varaa parantaa." - "There is always room for improvement."

"Zero trust -periaate tulisi ottaa joka paikassa ja asiassa käyttöön." - "The zero trust principle should be adopted everywhere and in everything."

A notable portion of respondents expressed uncertainty or lack of knowledge regarding specific improvements:

"En osaa sanoa." - "I don't know."

"En tiedä tarpeeksi pystyäkseni arvioimaan tätä." - "I don't know enough to be able to judge."

"Minulla ei ole suoraa näkyvyyttä asiaan." - "I don't have direct visibility."

These responses suggest a need for better awareness and understanding of cybersecurity measures at the shipyard.

Recommendations emphasized clearer roles and responsibilities, stricter access control and better monitoring of permissions:

"Oikeuksien jako paremmin valvotuksi." - "Better control of the distribution of rights."

"Roolien ja vastuiden kautta varmistetaan resurssien suojaus." - "Roles and responsibilities ensure protection of resources."

"Alihankkijoiden ja kumppanien pääsy IT-järjestelmiin." - "Access to IT systems by subcontractors and partners."

Many respondents recommended regular and practical cybersecurity training:

"Alihankkijoiden koulutus." - "Training of subcontractors."

"Selkeät säännöt/ohjeistukset." - "Clear rules/guidelines."

"Tietoisuuden lisääminen antamalla selkeitä esimerkkejä." - "Raising awareness by providing clear examples."

Password policies were a common theme, with suggestions for two-factor authentication and modern alternatives:

"2 vaiheinen tunnistautuminen." - "2-step authentication."

"Salasananvaihtamista pidetään tehottomana keinona." - "Password change is considered an ineffective method."

Concerns about outdated systems and inefficient processes:

"Stop using legacy systems like Mars and Kronodoc."

Several suggestions were made to enhance document control and tracking:

"Tiettyjen dokumentaatioiden vesileimaus voisi olla parannus." - "Watermarking of certain documents could be an improvement."

"Tietojen saanti on liian löyhällä pohjalla." - "Access to information is too loose."

Some respondents raised concerns about overly restrictive cybersecurity measures impacting productivity:

"Työn ulkopuolella vanhempi väki uskoo huijauksia helpommin mitä nuoremmat." - "Outside of work, older people are more likely to believe scams than younger people."

"Turha kankeus saattaa johtaa käyttäjätunnusten jakamiseen yms." - "Unnecessary rigidity may lead to sharing of usernames, etc."

"Pitää tasapainottaa suojauksen taso ja käytön helppous." - "Need to balance level of protection with ease of use."

Many responses emphasized the need for ongoing improvement in cybersecurity to adapt to evolving threats:

"Toimintaa pitää kehittää jatkuvasti, koska hyökkääjät kehittyvät myös." - "There is a need for continuous improvement because the attackers are evolving too."

"AI tuo uusia uhkatekijöitä, jotka vaativat jatkuvaa koulutusta." - "AI introduces new threats that require continuous training."

The responses to Q19 reveal a strong recognition of cybersecurity's importance at Meyer Turku shipyard, coupled with specific recommendations for improvement. Although some respondents feel that current measures are sufficient, there is a clear need for better training, improved access control, and the use of modern technology to handle new challenges and strengthen resource protection.

5.5 Conclusion and feedback: Q20

To complement the structured survey responses, this section captures open-ended feedback from respondents. Open feedback provides qualitative insights into aspects of cybersecurity that may not have been fully addressed in the multiple-choice and scaled questions.

Respondents were invited to share additional concerns, recommendations, and observations about cybersecurity at Meyer Turku. These insights help contextualize the quantitative findings and highlight specific areas where improvements are needed. The feedback also reflects respondents, external or internal, engagement and their willingness to contribute to strengthening cybersecurity practices at the shipyard.

Q20. “Please share any additional comments, suggestions, or feedback you have regarding cybersecurity at Meyer Turku shipyard:”

Multiple respondents emphasized the importance of dedicated cybersecurity training tailored to the shipyard's environment rather than general processes:

"Telakalle suunnittelun puolelle tultaessa voisi olla hyvä olla tarkempi tietoturvaperehdytys erillään yleisestä perehdytyksestä." - "When entering the design side of a shipyard, it could be a good idea to have a more detailed security briefing separate from the general briefing."

"Cybersecurity awareness should be included in our daily routine."

"Kunnolliset luennot asiasta, joissa kuvataan meille tärkeitä uhkakuvaa ja sen torjuntaa." - "Good lectures on the subject, describing the threats we face and how to combat them."

Suggestions also included improving employee awareness about specific threats and appropriate responses, particularly in areas like phishing and password management.

Some respondents highlighted inefficiencies and frustrations with current practices and tools:

"Salasanan vaihto tuntuu tulevan turhan usein, ja siitä seuraa välillä ongelmia esim. mobiililaitteiden suhteen." - "Password changes seem to come too often, and sometimes cause problems, for example with mobile devices."

"MT lacks clear structure of what information is and where. Duplicates are a lot which adds the risk."

"Ois kiva jos tulostimet ja muistitikut toimisi edes jollain tavalla." - "It would be nice if printers and notebooks worked at least in some way."

There was feedback about balancing security with usability, suggesting that overly strict measures may hinder operations, while insufficient controls lead to vulnerabilities.

Several comments pointed to a lack of clarity in cybersecurity policies and structure:

"MT lacks clear structure of what information is and where."

"Global IT tekee Turun Telakan tietoturvatyöstä haastavaa." - "Global IT makes Turku Shipyards security work challenging."

"M-asema on villi länsi ja siellä on paljon meidän tavaraa. En pidä sitä kovin turvallisena." - "M drive (VPN) is the Wild West and there's a lot of our stuff there. I don't think it's very safe."

There is a call for more defined and straightforward protocols for document storage, information management, and secure collaboration.

Respondents highlighted a growing awareness of sophisticated cyber threats, citing the geopolitical context and increasing phishing attempts:

"Very important point, regarding the political situation in Europe and worldwide."

"Ajoittain tulee paljon tietojenkalastelupuheluita ulkomailta." - "From time to time there are a lot of phishing calls from abroad."

Suggestions were made to introduce modern cybersecurity practices, such as advanced authentication methods and reducing reliance on passwords.

There were calls for greater involvement from top-level management to prioritize cybersecurity:

"Kunhan vaan se muistetaan ottaa riittävän vakavasti myös ylätasolla." - "As long as we remember to take it seriously enough at the top."

"The involvement of all parties to keep our guard up against Cyber attacks active and constant."

Respondents provided several actionable suggestions, including improving password policies and introducing alternatives like biometric authentication, training on digital signatures and document reliability, providing guidelines for handling specific scenarios, such as phishing attempts or suspicious calls, and making security tools and protocols more accessible and user-friendly. These comments reflect both an acknowledgment of cybersecurity's importance and a desire for more practical, reliable, and user-friendly measures to better the shipyard's security status.

5.6 Development suggestions grouped and listed

This section consolidates and categorizes the key development suggestions derived from survey responses, reflecting respondents concerns and areas for improvement. The recommendations focus on strengthening cybersecurity awareness, compliance, technical measures, and incident response at Meyer Turku. Grouping these suggestions into key themes allows for a more structured approach to addressing cybersecurity challenges and ensuring practical implementation.

Training and Awareness

D1. Implement mandatory cybersecurity awareness and training programs for all stakeholders, tailored to the specific risks and interfaces they handle.

D2. Launch targeted cybersecurity awareness campaigns emphasizing the importance of recognizing and reporting security incidents.

D3. Conduct focused group discussions or workshops to delve into different stakeholder concerns and share insights across the organization.

D4. Foster a culture of security within the organization, promoting continuous education, vigilance, and shared responsibility for cybersecurity among employees and external stakeholders.

D5. Ensure regular, role-specific cybersecurity training sessions to increase awareness and skills across the organization.

Security Culture and Compliance

D6. Develop a comprehensive security culture that includes all employees and external stakeholders, emphasizing continuous education and proactive security practices.

D7. Regularly audit all stakeholders’ compliance with cybersecurity training and practices, including cybersecurity requirements in contracts with third parties.

D8. Establish a formal insider threat program, incorporating employee monitoring, behavioural analysis, and clear consequences for policy violations.

D9. Foster stakeholder collaboration by engaging employees, contractors, and suppliers in discussions on cybersecurity practices and compliance with policies.

Physical Security Enhancements

D10. Enhance physical security measures, such as implementing biometric access controls, securing workstations, and establishing strict device security policies.

D11. Upgrade and expand physical security protocols, including monitored entry points, visitor segregation, and stringent access controls to safeguard sensitive areas.

D12. Conduct regular audits of physical security measures to ensure they meet current standards and address emerging vulnerabilities.

Cybersecurity and Technical Measures

D13. Invest in advanced network security solutions, including firewalls, intrusion detection systems, and regular security audits to identify and mitigate vulnerabilities.

D14. Conduct regular security assessments to identify and address vulnerabilities in IT infrastructure and physical assets.

D15. Strengthen identity and access management protocols, ensuring access rights align with job requirements and are revoked when no longer needed.

D16. Ensure robust protection strategies that cover both digital management systems and physical resources, reflecting the high importance ratings across these categories.

Third-Party and Vendor Management

D17. Develop a comprehensive third-party risk management program, including risk assessments, periodic audits, and enforcement of cybersecurity standards through contractual agreements.

D18. Conduct thorough security assessments of vendors and third-party service providers to ensure compliance with the organization’s cybersecurity policies.

Incident and Risk Management

D19. Establish clear, simple, and accessible mechanisms for reporting cybersecurity incidents to encourage prompt reporting and resolution.

D20. Develop and regularly update comprehensive crisis management plans for various cybersecurity incidents to ensure quick and effective responses.

D21. Integrate insights from respondent's feedback into the broader cybersecurity strategy to address niche but significant risks.

Collaborative Development Initiatives

D22. Use targeted responses to pilot specific cybersecurity enhancements in departments or areas directly affected by identified issues.

D23. Conduct workshops and engagement sessions to share best practices and improve collective understanding of cybersecurity risks and measures.

These seven key themes presented here are directed towards the development at Meyer Turku. Target was here to create a package that can be reviewed and help systematically implementing targeted improvements, enhancing both digital and physical security across the shipyard operations.

5.7 Constraints and Considerations of the Survey

While the survey-based methodology provided valuable insights into cybersecurity awareness, perceptions, and practices at Meyer Turku, it is important to acknowledge its limitations. These factors influenced the scope and interpretation of the findings and should be considered when applying the results to broader contexts.

One key limitation of the study is the reliance on self-reported data. Respondents may have overestimated their cybersecurity knowledge or underreported past security incidents due to concerns about anonymity or perceived repercussions. Self-reporting bias is a well-recognized challenge in survey research and can affect the accuracy of the collected data.

To mitigate this limitation, the survey included multiple-choice questions and scaled ratings to introduce some level of objectivity. While these measures helped in standardizing responses, the potential for bias could not be entirely eliminated. Therefore, the findings should be interpreted as reflecting respondent perceptions rather than absolute measures of cybersecurity proficiency.

Another limitation of this methodology is its emphasis on cybersecurity awareness and perceptions rather than directly measuring security practices and vulnerabilities. While self-reported perceptions provide valuable insights into respondent priorities and concerns, they do not necessarily align with the actual state of cybersecurity implementation at Meyer Turku.

Recognizing this limitation, the study treated the findings as indicative of awareness levels and respondent priorities rather than an empirical assessment of cybersecurity effectiveness. Future research could complement this approach with direct observational methods, technical audits, or penetration testing to provide a more comprehensive picture of cybersecurity practices.

The research findings are specific to Meyer Turku and its external stakeholders and may not be directly transferable to other organizations, industries, or shipbuilding operations in different geographic regions. The cybersecurity challenges, awareness levels, and practices identified in this study are influenced by the shipyard's unique operational environment, regulatory landscape, and stakeholder composition.

While the results provide valuable insights into shipbuilding cybersecurity, they should be extrapolated cautiously when applied to other settings. Future research could expand the scope by conducting comparative studies across multiple shipyards or maritime organizations to identify broader trends and variations in cybersecurity awareness and implementation.

Despite these limitations, the survey methodology proved to be the most suitable approach for capturing a broad range of internal and external stakeholder perspectives on cybersecurity at Meyer Turku. The findings provided actionable insights into gaps in awareness, training needs, and opportunities for improvement.

Main lessons learned points:

1. Simplifying survey language to improve accessibility for respondents with diverse technical backgrounds.
2. Using targeted outreach and incentives to increase participation among external stakeholders.
3. Combining survey data with qualitative methods such as interviews or focus groups to gain deeper insights into complex cybersecurity issues.

These lessons can guide future research efforts and help refine methodologies for studying cybersecurity awareness and practices in shipbuilding and shipyard applications.

6 Conclusion and Discussion

This thesis has examined cybersecurity in Finnish shipbuilding, with a particular focus on Meyer Turku and the implementation of IACS UR E26. As shipbuilding becomes increasingly digitized, cybersecurity risks grow, necessitating a shift in how shipyards approach security. Unlike previous regulations, IACS UR E26 requires cybersecurity to be integrated from the earliest stages of construction, addressing vulnerabilities that could persist throughout a vessel's lifecycle. This regulatory shift affects not only ship design and construction but also employee training, stakeholder engagement, and supply chain security. Although compliance comes with financial and operational challenges, it also provides a competitive edge. Shipbuilders that adopt strong cybersecurity measures can stand out in an industry where cyber resilience is essential.

This research aimed to understand how cybersecurity threats are identified, managed, and addressed in the shipbuilding sector. This was guided by the five research questions: (RQ1) How does the IACS UR E26 impact Finnish shipbuilding? (RQ2) What types of cybersecurity threats does Meyer Turku face? (RQ3) How do Meyer Turku employees and stakeholders perceive the security of digital and physical resources within the shipyard? (RQ4) What level of cybersecurity awareness exists among Meyer Turku employees and stakeholders, and how do they perceive the importance of cybersecurity in shipyard operations? (RQ5) How do different stakeholder groups differ in their perceptions of cybersecurity threats and priorities? These questions scoped the study's investigation into how Finnish shipbuilders are adapting to regulatory changes, identifying vulnerabilities, and implementing stronger cybersecurity practices.

The first research question, concerning the impact of IACS UR E26 on Finnish shipbuilding, was investigated through an analysis of regulatory changes, compliance requirements, and industry adaptation. IACS UR E26 introduces new cybersecurity requirements that affect ship design, production processes, and supply chain management. Finnish shipyards, including Meyer Turku, must enhance cybersecurity governance, implement stronger risk assessments, and improve access controls to comply with these regulations. The regulatory shift requires increased training for MT employees and external stakeholders, along with technical investments in network security and system monitoring. While compliance increases operational complexity, it also strengthens shipyards' resilience against cyber threats and enhances their competitiveness in global markets.

To address these challenges, this study recommends establishing a shipyard-wide cybersecurity policy framework (D1), conducting regular third-party security audits (D2), and ensuring external stakeholder compliance through contractual security standards (D3). Additionally, role-specific cybersecurity training programs (D4) should be integrated into Meyer Turku's onboarding and continuous education initiatives to ensure that all MT employees and external stakeholders are

equipped with the necessary cybersecurity competence. While these development suggestions were directly linked to survey findings, they also reinforce Meyer Turku's UR E26 compliance strategy. This makes them essential for regulatory adaptation.

The second research question examined the cybersecurity threats faced by Meyer Turku, identifying key risks affecting IT and OT systems, intellectual property, and supply chain security. Meyer Turku is exposed to both digital and physical cybersecurity threats. Digital threats include phishing attacks, ransomware, data breaches, and unauthorized access to ship design files, which could compromise intellectual property or disrupt operations. Physical threats, such as unauthorized access to restricted areas and hardware tampering, pose additional risks, especially with a large number of external contractors working within the shipyard. The survey found that 16% of respondents had encountered a cybersecurity incident, highlighting ongoing security gaps. A major concern is supply chain security, as 79% of external stakeholders reported not receiving cybersecurity training. This makes third-party vendors a major risk.

To address these threats, Meyer Turku should strengthen security assessments by conducting regular third-party audits (D2) to identify weaknesses in external stakeholder security. Enforcing stricter cybersecurity compliance (D3) and setting higher security standards (D7) will ensure all external stakeholders follow necessary protocols. Improving oversight by closely monitoring external stakeholder security practices (D9) will further enhance supply chain security and minimize risks. Investing in advanced network security solutions (D13) will help detect and block unauthorized access, while strengthening identity and access management systems (D15) will ensure only authorized personnel can access critical systems. To complement these technical measures, comprehensive cybersecurity training for external stakeholders (D4, D6) is critical for aligning external stakeholders with the same security standards as internal employees.

The third research question explored how Meyer Turku employees and external stakeholders perceive the security of digital and physical resources within the shipyard. Survey responses showed disparities between MT employees and external stakeholders, with MT employees expressing higher trust in existing cybersecurity measures while external stakeholders raised concerns about unclear security protocols. Although 63% of respondents rated their cybersecurity knowledge as high or very high, only 38% believed that Meyer Turku's cybersecurity policies were consistently enforced across all stakeholders. The lack of clear security policies and inconsistent enforcement adds to weaknesses in access management, system security, and external stakeholder risk exposure.

To improve security perceptions, Meyer Turku must enhance security governance and enforcement. Conducting routine security audits (D2) will help assess current practices and ensure compliance with established cybersecurity protocols. Improving oversight by enhancing compliance monitoring for external contractors (D9) will strengthen accountability and reduce risks associated with third-party

access. Strengthening access management policies and implementing stricter identity verification systems (D15) will further prevent unauthorized access to critical systems. Establishing clear reporting mechanisms for cybersecurity concerns (D19) will improve communication between internal employees and external partners, ensuring that security threats are identified and resolved in a timely manner. Externally expanding cybersecurity training programs (D4, D6) will help unify security practices and close awareness gaps across all stakeholder groups. While primarily linked to the survey, these development suggestions also support compliance with UR E26.

The fourth research question assessed the level of cybersecurity awareness among MT employees and external stakeholders, as well as their perception of cybersecurity's importance in shipyard operations. The study found gaps in cybersecurity awareness, particularly among external stakeholders. While general awareness is relatively high, formal training is inconsistent. Only 21% of external stakeholders had received cybersecurity training, despite many having direct access to shipyard networks and critical systems. This highlights a major gap in supply chain security that must be addressed. Cybersecurity was widely recognized as important, with 96% of respondents rating it as highly or extremely important to shipyard operations. However, this awareness does not always translate into action, as many respondents were unfamiliar with best practices or did not consistently follow security protocols.

To improve cybersecurity awareness and engagement, Meyer Turku must expand cybersecurity training initiatives (D4, D5) to ensure that all internal employees and external stakeholders receive the necessary knowledge to follow best practices. Strengthening internal communication on cybersecurity policies (D6) and integrating cybersecurity awareness into onboarding processes will help foster a culture of security. Establishing an insider threat awareness program (D8) will further educate internal employees on potential security risks and how to recognize suspicious activity. Improving crisis management exercises (D20) will also help internal employees and external stakeholder understand how to respond effectively to security threats.

The fifth research question examined how different stakeholder groups, including MT employees, turnkey companies, subcontractors, and owner representatives, differ in their perceptions of cybersecurity threats and priorities. While MT employees prioritized data security, system integrity, and access controls, owner representatives emphasized operational continuity and regulatory compliance. External stakeholders like turnkey contractors and subcontractors raised concerns about supply chain security vulnerabilities, whereas internal employees focused more on network security and phishing risks. These findings highlight the need for a more coordinated approach to cybersecurity that aligns stakeholder priorities.

To address these differences, Meyer Turku should strengthen third-party risk management (D17) by enforcing cybersecurity requirements for all external stakeholders. Conducting vendor security

assessments (D18) and implementing clear compliance measures will ensure stakeholders follow industry best practices. Expanding cybersecurity training programs (D4, D5) will improve awareness, while facilitating knowledge-sharing initiatives (D23) between internal employees and external partners will help align security practices across all stakeholders involved in shipyard operations.

While this study provides a detailed assessment of cybersecurity adaptation at Meyer Turku, this study might not be applicable to other shipyard environments. The scale and environment of stakeholder collaboration varies broadly in the shipbuilding industry. For Meyer Turku, further research is needed to address long-term cybersecurity evolution in shipbuilding. A useful approach would be a long-term study tracking how UR E26 is implemented over time, analysing how compliance strategies change and whether initial challenges improve with industry experience. Future research could also compare how different shipyards in Europe and globally adapt to cybersecurity regulations, identifying best practices that could benefit the Finnish maritime sector.

Future research should also explore AI-driven cybersecurity tools, secure databases and information-sharing systems. AI-tools are becoming more common and digital supply chains continue to expand in heavy industries like shipbuilding. It is important to understand how AI can affect shipyard security policies, automated decision-making and threat detection errors. Similarly studying authentication and verification methods in shipyard environments could help prevent unauthorized access to sensitive information and ensure that suppliers follow cybersecurity rules.

As cyber threats evolve, this thesis provides insights to help Finnish shipbuilders enhance cybersecurity throughout the shipbuilding process. However, true cyber resilience is not a one-time compliance task or just a simple checklist for meeting regulations. It requires continuous improvement, investment, and commitment at every stage of shipbuilding. To achieve a strong security environment, shipbuilders must work closely with shipowners, regulatory authorities, and international partners. Cybersecurity must also be integrated into supplier contracts to ensure all stakeholders uphold strict security measures. By promoting a strong security culture and strengthening industry-wide collaboration, Finnish shipbuilders can raise cybersecurity standards and build a more resilient industry. Like other safety and security challenges, lack of awareness remains the greatest risk. Even the best cybersecurity systems will fail if people do not recognize threats or follow protocols.

References

WAGO. (2024). Cybersecurity in the shipbuilding industry: An expert interview on increasing security threats. https://www.wago.com/us/open-automation/cybersecurity/interview-cyber-security-shipbuilding-industry

Aeromarine Cybersecurity. (2024). Cybersecurity by design: A new approach in maritime security. https://cybersecurity.aeromarine.es/cybersecurity-by-design

DNV. (2024). Tackling a growing cybersecurity threat in an increasingly connected industry. https://www.dnv.com/expert-story/maritime-impact/tackling-a-growing-cybersecurity-threat

Maritime Executive. (2024). New Trends in Maritime Cybersecurity in 2024. The Maritime Executive. https://maritime-executive.com/features/new-trends-in-maritime-cybersecurity-in-2024

NCCoE (National Cybersecurity Center of Excellence). (2019). Cybersecurity Framework: NIST Special Publication 1800-26. https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html

Bureau Veritas. (2023). Ensuring cyber resilience to meet new IACS requirements. https://marine-offshore.bureauveritas.com/magazine/ensuring-cyber-resilience-meet-new-iacs-requirements

USNI News. (2016, November 24). Navy: Personal Data of 134K Sailors Compromised. https://news.usni.org/2016/11/24/navy-personal-data-134k-sailors-compromised

ClearanceJobs. (2023, April 25). Defense Contractors in the Cyber Crosshairs – U.S. Shipbuilders Hit in Cyberattacks. https://news.clearancejobs.com/2023/04/25/defense-contractors-in-the-cyber-cross-hairs-two-u-s-shipbuilders-hit-in-cyberattacks/

IBM. (2024). What is Role-Based Access Control (RBAC)? https://www.ibm.com/think/topics/rbac

Digital WarRoom. (2024). Bill Gallivan (2024) What is hashing? https://www.digitalwarroom.com/blog/what-is-hashing

NCCoE (National Cybersecurity Center of Excellence). (2020). Executive Summary — NIST SP 1800-26 documentation. https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html

Security Week. (2022). U.S. Releases Cybersecurity Plan for Maritime Sector. https://www.securityweek.com/cybersecurity-plan-released-us-maritime-sector/

Unitrends. (2023). Failover: What it is and its importance in business continuity. https://www.unitrends.com/blog/failover/

Darktrace. (n.d.). Cybersecurity for Maritime: Definition & Examples. https://darktrace.com/cyber-ai-glossary/cybersecurity-in-maritime

Financial Times. (2024, August). Cyber attacks on shipping rise amid geopolitical tensions. https://www.ft.com/content/c05c9b21-77bd-4ddf-82e1-02356acf0899

Fortinet. (n.d.). IoT Device Vulnerabilities. https://www.fortinet.com/resources/cyberglossary/iot-device-vulnerabilities

Fortinet. (n.d.). What is the CIA Triad and Why is it important? https://www.fortinet.com/resources/cyberglossary/cia-triad

Cyber Consultancy. (n.d.). IoT Security in Maritime. https://thecyberconsultancy.com/iot.html

Ruan, J., Liang, G., Zhao, J., Zhao, H., Qiu, J., Wen, F., & Dong, Z. (2023). Deep learning for cybersecurity in smart grids: Review and perspectives. https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/enc2.12091

Melnyk, O., Shcherbina, O., Mykhailova, I., Obnyavko, T., & Korobko, T. O. (2023). Focused research on technological innovations in shipping industry: Review and prospects, https://journals.onmu.in.ua/index.php/journal/article/view/211

Dunlevie, T. (2023, April 27). Defending our shipbuilding critical infrastructure. Center for Maritime Strategy. https://centerformaritimestrategy.org/publications/defending-our-shipbuilding-critical-infrastructure/

Yamout, Y., Yeasar, T. S., Iqbal, S., & Zulkernine, M. (2023). Beyond Smart Homes: An In-Depth Analysis of Smart Aging Care System Security. https://dl.acm.org/doi/10.1145/3610225

Safitra, M. F., Lubis, M., & Kurniawan, M. T. (2023). Cyber Resilience: Research Opportunities. https://dl.acm.org/doi/10.1145/3592307.3592323

ABS Group. (2023). Improving Safety Onboard Ships: IACS Puts Cybersecurity on the Roadmap. https://www.abs-group.com/Knowledge-Center/Insights/Improving-Safety-Onboard-Ships-IACS-Puts-Cybersecurity-on-the-Roadmap/#:~:text=IACS%20identified%20that%2C%20for%20ships,a%20practical%20risk%2Dbased%20approach.

Trusted Docks. (n.d.). Shipbuilding in Finland. https://www.trusteddocks.com/catalog/country/75-finland

Forum Marinum. (n.d.). Finnish Shipbuilding. https://www.forum-marinum.fi/en/exhibitions/finnish-shipbuilding/

IACS (International Association of Classification Societies). (2024). IACS UR E26 and E27 Press Release. https://iacs.org.uk/news/iacs-ur-e26-and-e27-press-release

DNV GL. (2022). Yards and vendors must act promptly to comply with upcoming IACS cyber security requirements. https://www.dnv.com/expert-story/maritime-impact/Yards-and-vendors-must-act-promptly-to-comply-with-upcoming-IACS-cyber-security-requirements/#:~:text=Industry%20Insights-,Yards%20and%20vendors%20must%20act%20promptly%20to%20comply%20with%20upcoming,up%20for%20the%20supply%20industry

Lexology. (2023). Cyber security regulations applicable to the maritime transport sector. https://www.lexology.com/library/detail.aspx?g=d9bbcb6e-5540-477e-b419-6e320d129439

Atlantic Council. (2022). Cooperation on maritime cybersecurity: A system of systems. https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-a-system-of-systems/

TMF Group. (2023). Global compliance legislation and business complexity. https://www.tmf-group.com/en/news-insights/articles/global-business-complexity/global-compliance-challenges-business-complexity/

Neumetric. (2023). Challenges of multi-regulatory compliance. https://www.neumetric.com/multi-regulatory-compliance-challenges/

Offshore Energy. (2023). Korean Register Grants AiP for SHI's Ship Cyber Resilience Tech. https://www.offshore-energy.biz/korean-register-grants-aip-for-shis-ship-cyber-resilience-tech/

MarineLink. (2024). Cybersecurity in Maritime: Navigating the Digital Seas Safely. https://www.marinelink.com/articles/maritime/cybersecurity-in-maritime-navigating-the-digital-seas-safely-101609

Trend Micro. (2013). Threats at Sea: A Security Evaluation of AIS. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-security-evaluation-of-ais

Mission Secure. (n.d.). A Comprehensive Guide to Maritime Cybersecurity. https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach

Janes. (2023). Finnish Border Guard orders two OPVs from Meyer Turku. https://www.janes.com/osint-insights/defence-news/sea/finnish-border-guard-orders-two-opvs-from-meyer-turku

Yle.fi. (2023). Finnish Customs calls for balanced resource allocation among security agencies. https://yle.fi/a/74-20049566

Travel and Leisure. (2023). Finnish Border Guard involved in digital passport pilot program. https://www.travelandleisureasia.com/in/news/finland-is-testing-a-digital-passport-system/

Forbes. (2023). EU co-funds digital travel credentials pilot project at Helsinki Airport. https://www.forbes.com/sites/suzannerowankelleher/2023/09/06/europe-testing-digital-passport-finland/

DHS News. (2022). Secretary Mayorkas Delivers Remarks at the Maritime and Control Systems Cybersecurity Conference. https://www.dhs.gov/archive/news/2022/03/21/secretary-mayorkas-delivers-remarks-maritime-and-control-systems-cybersecurity

OrbitsHub. (2023). How Do Maritime Organizations Collaborate to Enhance Cybersecurity Resilience? https://orbitshub.com/how-do-maritime-organizations-collaborate-to-enhance-cybersecurity-resilience/

Tagarev, T., & Yanakiev, Y. (2020). Business Models of Collaborative Networked Organisations: Implications for Cybersecurity Collaboration. https://ieeexplore.ieee.org/document/9125011

Slupska, J. (2020). War, Health and Ecosystem: Generative Metaphors in Cybersecurity Governance. https://link.springer.com/article/10.1007/s13347-020-00397-5

Jakubczak, W., & Yau, H. (2021). TRENDS IN CYBERSECURITY REGULATIONS OF TAIWAN (REPUBLIC OF CHINA) – Phases of Promotion of major cyber security plans and programs in the National Cyber Security Program of Taiwan (2021–2024). https://www.researchgate.net/publication/357230565_TRENDS_IN_CYBERSECURITY_REGULATIONS_OF_TAIWAN_REPUBLIC_OF_CHINA_-_Phases_of_Pro_motion_of_major_cyber_security_plans_and_programs_in_the_National_Cyber_Security_Program_of_Taiwan_2021-2024

Danțiș, D. (2022). Latest developments in cybersecurity management in Romania. Financing a condition for market evolution. https://www.researchgate.net/publication/362560779_Latest_developments_in_cybersecurity_management_in_Romania_Financing_a_condition_for_market_evolution

Satola, D., & Judy, H. (2011). Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum. William Mitchell Law Review, 37(4), 1745. https://open.mitchellhamline.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1427&context=wmlr

United Nations Department of Economic and Social Affairs. (2023). Internet Governance Forum (IGF). https://publicadministration.desa.un.org/capacity-development/igf

Oruc, A. (2022). Ethical Considerations in Maritime Cybersecurity Research. https://www.researchgate.net/publication/362372469_Ethical_Considerations_in_Maritime_Cybersecurity_Research

DLA Piper. (2023). Data protection laws of the world: Finland. https://www.dlapiperdataprotection.com/?c=FI&t=law

IT Governance. (2018). EU General Data Protection Regulation (GDPR). https://www.itgovernance.eu/fi-fi/eu-general-data-protection-regulation-gdpr-fi

European Parliament. (2019). Public-private partnerships for cybersecurity. https://www.europarl.europa.eu/legislative-train/package-better-business-environment-for-digital-networks-services/file-public-private-partnerships-for-cybersecurity

Global Partners Digital. (2015). Human rights and cybersecurity policy making. https://www.gp-digital.org/wp-content/uploads/2015/06/GCCS2015-Webinar-Series-Introductory-Text.pdf

DNV. (2024). Ethical hacking for maritime cyber security. DNV. https://www.dnv.com/cyber/insights/articles/ethical-hacking-for-maritime-cyber-security/

Moody's. (2024). Enhancing national security with public-private partnerships. https://www.moodys.com/web/en/us/insights/public-sector/enhancing-national-security-with-public-private-partnerships.html

VentureBeat. (2023). AI-assisted cybersecurity: 3 key components you can't ignore. https://venturebeat.com/ai/ai-assisted-cybersecurity-3-key-components-you-cant-ignore/

Forbes. (2023). Artificial Intelligence In Cybersecurity: Unlocking Benefits And Confronting Challenges. https://www.forbes.com/councils/forbestechcouncil/2023/08/25/artificial-intelligence-in-cybersecurity-unlocking-benefits-and-confronting-challenges/

DarkReading. (2023). Cybersecurity and Compliance in the Age of AI. https://www.darkreading.com/cyber-risk/cybersecurity-and-compliance-in-the-age-of-ai

de Peralta, F. A., Watson, M., Bays, R. M., Boles, J. R., & Powers, F. (2021). Cybersecurity Resiliency of Marine Renewable Energy Systems Part 2: Cybersecurity Best Practices and Risk Management. Marine Technology Society Journal, 55, 104-116. https://www.semanticscholar.org/paper/Cybersecurity-Resiliency-of-Marine-Renewable-Energy-Peralta-Watson/1cf84cde8935595b6196413f7f16396484562712

Johnson, M. D. (2014). Department of Homeland Security Efforts. Engineering. https://www.semanticscholar.org/paper/Department-of-Homeland-Security-Efforts-Johnson/57f92868e64a4b08e9b9a0a41571e7c0314d5f6e

IT Governance. (2022). What is ISO/IEC 27001? https://www.itgovernance.co.uk/iso27001

Lee, A., & Wogan, H. P. (2018). All at Sea: The Modern Seascape of Cybersecurity Threats of the Maritime Industry. https://www.semanticscholar.org/paper/a4df8799b4adc72bf287037adbfaf8625744005c

Pyykkö, H., Kuusijärvi, J., Noponen, S., Toivonen, S., & Hinkka, V. (2020). Building a Virtual Maritime Logistics Cybersecurity Training Platform. https://www.semanticscholar.org/paper/46129d80d50976048391dc5ba741e336ed8526ab

Kotis, K. I., Stavrinos, S., & Kalloniatis, C. (2022). Review on Semantic Modeling and Simulation of Cybersecurity and Interoperability on the Internet of Underwater Things. https://ideas.repec.org/a/gam/jftint/v15y2022i1p11-d1015688.html

Finley, I., & Harkiolakis, N. (2018). Cybersecurity policies and supporting regulations for maritime transportation system in the USA. https://www.researchgate.net/publication/324233871_Cybersecurity_policies_and_supporting_regulations_for_maritime_transportation_system_in_the_USA

Vsevolozhsky, G., & Qu, Y. (2022). A Process Model for Ensuring Diffusion and Adhesion of Cybersecurity Innovations in Software Development Organizations. https://american-cse.org/csci2022-ieee/pdfs/CSCI2022-2lPzsUSRQukMlxf8K2x89I/202800b880/202800b880.pdf

Creswell, J. W., & Creswell, J. D. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th ed.). https://spada.uns.ac.id/pluginfile.php/510378/mod_resource/content/1/creswell.pdf

Yin, R. K. (2018). Case Study Research and Applications: Design and Methods (6th ed.). https://www.academia.edu/download/106905310/Artikel_Yustinus_Calvin_Gai_Mali.pdf

Smithson, J. (2000). Using and analysing focus groups: limitations and possibilities. International Journal of Social Research Methodology, 3(2), 103–119. https://www.sfu.ca/~palys/Smithson-2000-Using%26AnalysingFocusGroups.pdf

Federal Trade Commission. (n.d.). Understanding the NIST cybersecurity framework. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework

Appendices

Appendix 1 Cybersecurity Awareness and Importance Survey for MT employees and external stakeholders (English)

Introduction: Thank you for participating in this survey. Your feedback is important in helping us understand the level of cybersecurity awareness and its importance among Meyer Turku shipyard employees and external stakeholders. This survey will take approximately [5-10] minutes to complete. Your responses will remain confidential.

Introduction to Cybersecurity:

Cybersecurity protects digital systems, networks, and data from unauthorized access and cyber threats. It includes practices, processes, and technologies aimed at safeguarding sensitive information, ensuring data integrity, and maintaining system availability.

Cyber threats, such as malware and hacking attempts, pose risks to organizations and individuals worldwide. Effective cybersecurity involves implementing robust security measures, including encryption, regular updates, and awareness training, to mitigate risks and prevent data breaches.

1. Demographics

Q1. Are you currently an employee of Meyer Turku shipyard?

Yes

No

Q2. If you answered "No" to the previous question, please specify your affiliation with Meyer Turku:

| Turnkey Contractor | Subcontractor | Material or system supplier | Owner representative |

| Class representative | Other: free |

Q3. How long have you been associated with shipbuilding and shipyards?

| 0-1 years | 2-3 years | 4-5 years | 6-10 years | 11-20 years | more than 20 years |

Q4. How long have you been associated with Meyer Turku shipyard?

| 0-1 years | 2-3 years | 4-5 years | 6-10 years | 11-20 years | more than 20 years |

2. Cybersecurity Awareness

Q5. On a scale of 1 to 5, please rate your understanding of cybersecurity.

1 (Very Low)

2 (Low)

3 (Moderate)

4 (High)

5 (Very High)

Q6. Have you received any yard information security training or cybersecurity awareness programs at Meyer Turku shipyard?

Yes

No

Q7. If yes, please rate the effectiveness of the cybersecurity training/awareness programs you have received:

1 (Very Ineffective)

2 (Ineffective)

3 (Neutral)

4 (Effective)

5 (Very Effective)

Q8. Do you find yourself needing more training in cybersecurity practices?

Yes

No

3. Cybersecurity Importance

Q9. How important do you think cybersecurity is for Meyer Turku shipyard's operations?

1 (Not Important)

2 (Somewhat Important)

3 (Neutral)

4 (Important)

5 (Very Important)

Q10. Meyer Turku shipyard's operations involve various resources that require protection. The following list includes the systems/programs and resource types. Please indicate their importance in regards of cybersecurity on your role.

Please rate their importance on a scale of 1 to 5. Scale: 1 = Not important, 5 = Extremely important.

Kronodoc (Data management program)

Architectural and concept design

Basic design

Detail design

Outfitting

Ship specification

Ship contract

Jira (Quality management program)

Building method

Work standards

Detail design

Quality management procedures

Mars (Material and production management software)

Procurement data

Turnkey and subcontractor contracts

Material data

SAP (Planning and scheduling program)

Shipbuilding schedules

Area building schedules

Building method

ERP, resource planning data

Physical assets and equipment

Machinery and equipment on the shipyard floor

Industrial control systems (ICS)

Inventory and materials

Vehicles and transport equipment

Power generation and distribution systems

Critical infrastructure (e.g., docks, cranes)

Other items:

Employee information and records

Communication systems and networks

Intellectual property

Q11. OPTIONAL. Is there anything else, not mentioned above, that you believe is important to consider in the context of cybersecurity at Meyer Turku shipyard? If so, please specify.

Resource: _____

Q12. OPTIONAL. Please rate the importance of your added resource or item in regards to cybersecurity from question 11.

Importance: 1 2 3 4 5

Q13. In your opinion, what are the main reasons for prioritizing cybersecurity in a shipyard environment? (Please select up to three choices)

Preventing cyberattacks and data breaches

Ensuring the safety of employees and assets

Maintaining customer trust and reputation

Compliance with industry regulations

Enabling subcontractors to act responsibly

Other (please specify):

Q14. OPTIONAL. Do you believe there are additional resources or aspects that should be considered for protection within Meyer Turku shipyard's operations? Please share your thoughts and suggestions:

_____

Q15. Have you ever encountered a cybersecurity incident or breach at Meyer Turku shipyard or in your role as a stakeholder?

Yes

No

Q16. OPTIONAL. If you answered yes to question 15, please briefly describe the incident or breach:

_____

4. Cybersecurity Practices

Before we proceed with questions related to your cybersecurity practices, let's briefly define some key concepts:

Cybersecurity Best Practices: These are a set of guidelines and actions that individuals and organizations can take to protect their digital systems, data, and resources from cyber threats. Cybersecurity best practices help ensure the confidentiality, integrity, and accessibility of sensitive information and resources/assets.

CIA Triad:

Confidentiality: Ensuring that information is accessible only to those who are authorized to access it. It involves safeguarding sensitive data from unauthorized disclosure.

Integrity: Maintaining the accuracy and reliability of data and resources. It involves protecting information from unauthorized modification or tampering.

Accessibility: Ensuring that authorized users have timely and reliable access to information and resources when needed.

The above described CIA triad should be fulfilled in the cyber security of all protected resources.

Q17. Did you have prior knowledge of CIA best practices before?

Yes

No

Q18. Do you follow cybersecurity best practices in your day-to-day work at Meyer Turku shipyard?

Always | Often | Sometimes | Rarely | Never

Q19. Do you think there are specific cybersecurity measures or practices you think should be implemented or improved at Meyer Turku shipyard?

_____

5. Conclusion and feedback

Thank you for completing this survey. Your input is valuable in helping us assess and improve cybersecurity awareness and practices within Meyer Turku shipyard and among its stakeholders. Your responses will contribute to our ongoing efforts to enhance cybersecurity

Q20. Please share any additional comments, suggestions, or feedback you have regarding cybersecurity at Meyer Turku shipyard:

_____

Appendix 2 Kyberturvallisuustietoisuus- ja tärkeyskysely Meyer Turku Oy:n ja sidosryhmien työntekijöille (Suomeksi)

Johdanto: Kiitos osallistumisestasi tähän kyselyyn. Palautteesi on tärkeää auttaaksemme ymmärtämään kyberturvallisuustietoisuuden tasoa ja sen merkitystä Meyer Turun telakan työntekijöiden ja ulkoisten sidosryhmien keskuudessa. Tämä kysely kestää noin [5-10] minuuttia. Vastauksesi pysyvät luottamuksellisina.

Johdatus kyberturvallisuuteen:

Kyberturvallisuus suojaa digitaalisia järjestelmiä, verkkoja ja informaatiota luvattomalta pääsyltä ja kyberuhilta. Se sisältää käytäntöjä, prosesseja ja teknologioita, joiden tavoitteena on suojata arkaluontoisia tietoja, varmistaa tietojen eheys ja ylläpitää järjestelmien käytettävyyttä.

Kyberuhkat, kuten haittaohjelmat ja hakkerointiyritykset, aiheuttavat riskejä organisaatioille ja yksilöille maailmanlaajuisesti. Tehokas kyberturvallisuus edellyttää vahvojen turvatoimien toteuttamista, kuten salausta, säännöllisiä päivityksiä ja tietoisuuskoulutusta, riskien pienentämiseksi ja tietomurtojen estämiseksi.

1. Demografiset tiedot

Q1. Oletko tällä hetkellä Meyer Turun telakan työntekijä?

Kyllä

Ei

Q2 Jos vastasit "Ei" edelliseen kysymykseen, ilmoita suhteesi Meyer Turun telakkaan:

| Kokonaistoimittaja | Alihankkija | Materiaali- tai järjestelmätoimittaja | Omistajan edustaja |Luokituslaitoksen edustaja | Muu: _____ |

Q3. Kuinka kauan olet ollut tekemisissä laivanrakennuksen ja telakoiden kanssa?

| 0-1 vuotta | 2-3 vuotta | 4-5 vuotta | 6-10 vuotta | 11-20 vuotta | yli 20 vuotta |

Q4. Kuinka kauan olet ollut tekemisissä Meyer Turun telakan kanssa?

| 0-1 vuotta | 2-3 vuotta | 4-5 vuotta | 6-10 vuotta | 11-20 vuotta | yli 20 vuotta |

2. Kyberturvallisuustietoisuus

Q5. Arvioi kyberturvallisuuden ymmärryksesi asteikolla 1-5.

1 (Erittäin matala)

2 (Matala)

3 (Kohtalainen)

4 (Korkea)

5 (Erittäin korkea)

Q6. Oletko saanut tietoturvakoulutusta tai kyberturvallisuustietoisuuskoulutusta Meyer Turun telakalla?

Kyllä

Ei

Q7. Jos vastasit kyllä, arvioi saamasi kyberturvallisuuskoulutuksen/ tietoisuuskoulutuksen tehokkuus:

1 (Erittäin tehoton)

2 (Tehoton)

3 (Neutraali)

4 (Tehokas)

5 (Erittäin tehokas)

Q8. Koetko tarvitsevasi lisäkoulutusta kyberturvallisuuskäytännöistä?

Kyllä

Ei

3. Kyberturvallisuuden tärkeys

Q9. Kuinka tärkeänä pidät kyberturvallisuutta Meyer Turun telakan toiminnalle?

1 (Ei tärkeä)

2 (Jossain määrin tärkeä)

3 (Neutraali)

4 (Tärkeä)

5 (Erittäin tärkeä)

Q10. Meyer Turun telakan toiminnanohjaukseen liittyy monia resursseja, jotka vaativat suojaamista. Arvioi seuraavien järjestelmien, ohjelmien ja resurssityyppien tärkeys kyberturvallisuuden kannalta omassa roolissasi.

Arvioi asteikolla 1-5 (1 = Ei tärkeä, 5 = Erittäin tärkeä).

Kronodoc (Tiedonhallintaohjelma)

Arkkitehti- ja konseptisuunnittelu

Perussuunnittelu

Valmissuunnittelu

Varustelu

Laivaspesifikaatio

Laivasopimukset

Jira (Laadunhallintaohjelma)

Rakennustapa

Työstandardit

Valmissuunnittelu

Laadunhallintamenettelyt

Mars (Materiaali- ja tuotannonhallintaohjelma)

Hankintatiedot

Kokonaistoimitus- ja alihankintasopimukset

Materiaalitiedot

SAP (suunnittelu- ja aikataulutusohjelma)

Laivanrakennusaikataulut

Alueiden rakennusaikataulut

Rakennustapa

ERP, resurssienhallintatiedot

Fyysiset toiminnot ja laitteet

Telakalla olevat koneet ja laitteet

Teolliset ohjausjärjestelmät (ICS)

Varastot ja materiaalit

Ajoneuvot ja kuljetuskalusto

Sähköntuotanto- ja jakelujärjestelmät

Kriittinen infrastruktuuri (esim. laiturit, nosturit)

Muut:

Työntekijätiedot ja -asiakirjat

Viestintäjärjestelmät ja verkot

Immateriaalioikeudet / Teollis- ja tekijänoikeudet

Q11. VALINNAINEN. Onko jotain muuta, mikä olisi tärkeää huomioida Meyer Turku Oy:n kyberturvallisuustoimenpiteissä? Jos on, tarkenna.

Resurssi: _____

Q12. Arvioi lisäämäsi resurssin tärkeys kyberturvallisuuden kannalta (1-5).

Tärkeys: 1 2 3 4 5

Q13. Mitkä ovat mielestäsi keskeisimmät syyt kyberturvallisuuden priorisoinnille telakkaympäristössä? (Valitse enintään kolme vaihtoehtoa)

Kyberhyökkäysten ja tietomurtojen estäminen

Työntekijätietojen ja asiakirjojen turvallisuuden varmistaminen

Asiakasturvallisuuden ja maineen ylläpitäminen

Alan säännösten noudattaminen

MT:n ja ulkoisten sidosryhmien vastuullinen toiminta

Muu (Tarkenna): _____

Q14. VALINNAINEN. Oletko sitä mieltä, että Meyer Turku Oy:n toiminnoissa tulisi suojata lisää resursseja tai näkökohtia? Jaa ajatuksesi ja ehdotuksesi:

_____

Q15. Oletko koskaan kohdannut kyberturvallisuusvahinkoa tai tietomurtoa Meyer Turun telakalla tai roolissasi sidosryhmässä?

Kyllä

Ei

Q16. VALINNAINEN. Jos vastasit kyllä, kuvaile lyhyesti tapahtunutta kyberturvallisuusvahinkoa tai tietovuota:

_____

4. Kyberturvallisuuskäytännöt

Koskien kyberturvallisuuskäytäntöjä, alla on lyhyesti muutama määritelmä keskeisistä käsitteistä:

Kyberturvallisuuden käytännöt (”best practices”): Nämä ovat ohjeita ja toimenpiteitä, joita yksilöt ja organisaatiot voivat toteuttaa suojatakseen digitaalisia järjestelmiä, tietoja ja resursseja kyberuhkilta. Kyberturvallisuuden parhaat käytännöt varmistavat suojattavien tietojen ja resurssien luottamuksellisuuden, eheyden ja saatavuuden (CIA:n).

CIA:

Confidentiality / Luottamuksellisuus: Tietojen saanti vain niille, joilla on siihen oikeus. Arkaluontoisten tietojen suojaamisen luvattomalta julkistamiselta sisältyy tähän.

Integrity / Eheys: Tietojen ja resurssien tarkkuuden ja luotettavuuden ylläpitäminen. Tämä sisältää tietojen suojaamisen luvattomalta muokkaukselta tai väärentämiseltä.

Availability / Saatavuus: Varmistetaan, että valtuutetuilla käyttäjillä on oikeaan aikaan ja luotettavasti pääsy tietoihin ja resursseihin tarvittaessa.

Yllä mainittu CIA-kolmikko tulisi täyttyä kaikkien suojattujen resurssien kyberturvaamisessa.

Q17. Oliko sinulla aiempaa tietoa CIA:n kyberturvakäytännöistä?

Kyllä

Ei

Q18. Noudatatko yllä mainittuja kyberturvallisuuden käytäntöjä päivittäisessä työssäsi Meyer Turku Oy:ssä tai sidosryhmässäsi niin, että suojattujen resurssien luottamuksellisuus, eheys ja saatavuus toteutuvat?

| Aina | Usein | Joskus | Harvoin | En koskaan |

Q19. Mielestäsi, tulisiko Meyer Turku Oy:ssä toteuttaa tai parantaa tiettyjä kyberturvallisuustoimenpiteitä tai käytäntöjä, jotka paremmin varmistaisivat suojattujen resurssien CIA:n?

_____

5. Päätelmä ja palaute

Kiitos kyselyyn vastaamisesta! Osallistumisesi auttaa meitä arvioimaan ja parantamaan kyberturvallisuustietoisuutta ja -käytäntöjä Meyer Turku Oy:ssä ja sen sidosryhmissä.

Vastauksilla pyrimme parantamaan kyberturvallisuutta telakkaympäristössä.

Q20. Jaa halutessasi lisäkommentteja, ehdotuksia tai anna palautetta liittyen kyberturvallisuuteen Meyer Turku Oy:n työympäristössä:

_____