THE ANNALS OF “DUNAREA DE JOS” UNIVERSITY OF GALATI
FASCICLE XI – SHIPBUILDING. ISSN 1221-4620, e-ISSN 2668-3156
DOI: https://doi.org/10.35219/AnnUgalShipBuilding/2024.47.11
2024

SECURING INNOVATION AT SEA: CYBER RISK MANAGEMENT FOR SMEs IN SHIP DESIGNE

Ungureanu Mirela-Alexandra
“Dunarea de Jos” University of Galati,
Faculty of Naval Architecture, Galati,
47 Domneasca Street, 800008, Romania,
E-mail: mo222@student.ugal.ro

Gavan Eugen
“Dunarea de Jos” University of Galati,
Faculty of Naval Architecture, Galati,
47 Domneasca Street, 800008, Romania,
E-mail: eugen.gavan@ugal.ro

Gasparotti Carmen
“Dunarea de Jos” University of Galati,
Faculty of Naval Architecture, Galati,
47 Domneasca Street, 800008, Romania,
E-mail: carmen.gasparotti@ugal.ro

ABSTRACT

This paper examines the critical cybersecurity landscape faced by maritime SMEs engaged in Ship Design, analysing their vulnerability to various cyber threats including ransomware, phishing attacks, and supply chain compromises. Through a comprehensive review of recent industry reports, regulatory frameworks, and cybersecurity incidents, we identify key risk factors and assess their potential impact on SMEs' operations, reputation, and competitive advantage. Our analysis reveals that maritime SMEs face disproportionate challenges in cybersecurity due to resource constraints, complex supply chain relationships, and the increasing sophistication of cyber threats targeting intellectual property. The paper presents a structured approach to cyber risk management based on established frameworks, emphasizing the protection of valuable intellectual property while maintaining operational efficiency. We propose practical recommendations for implementing robust cybersecurity measures within the resource constraints typical of SMEs, including strategies for threat detection, incident response, and recovery planning.

Keywords: intellectual property protection; SME risk management; maritime cyber risks; naval design innovation; cybersecurity; supply chain security; operational technology; cyber resilience.

1. INTRODUCTION

The maritime sector plays a vital role in sustaining societies and economies through the movement of people and essential goods, including energy and food. Over 85% of global goods [1], and more than 74% of goods traded between the EU and the rest of the world [2] are shipped by sea.

Within this industry, Small and Medium Enterprises (SMEs) specializing in naval architecture, engineering, and advanced ship technologies are key players, driving innovation in areas like ship design, propulsion systems, digital advancements, and development of complex maritime systems [3]. Their contributions are particularly significant in the European maritime sector, leading to the development of green and autonomous ship technologies [3].

As SMEs increasingly adopt digital tools and technologies in naval design—from Computer-Aided Design (CAD) software to integrated shipbuilding systems— they face significant challenges. The topmost areas are intellectual property (IP) protection and cyber risk management [4]. The stakes are particularly high because a company’s intellectual property often represents its primary competitive advantage and the culmination of years of research and development [5].

Given the international nature of shipbuilding, the complexity of enforcing IP rights across different jurisdictions poses significant challenges [4]. Inadequate IP protection can lead to the loss of valuable innovations, particularly when competing with nations that may not have robust IP enforcement mechanisms.

Moreover, these last few years, SMEs have become prime targets for cyberattacks aimed at disrupting operations, stealing intellectual property, or engaging in industrial espionage [6] but often lack the resources and expertise to fully address the threats.

The truth is that the mix of operational technology (OT) and information technology (IT) in modern ship design further exacerbates the sector's vulnerabilities. As ships become more connected through digital networks, the attack surface expands, making it easier for cybercriminals to infiltrate sensitive systems [7]. Incidents like the NotPetya attack on Maersk in 2017, which resulted in over $300 million in losses, illustrate the devastating impact that cyberattacks can have on the maritime sector [6].

This paper aims to discuss the critical need for enhanced cyber risk management within SMEs in naval design and engineering. It will examine the role of these enterprises in maritime innovation, explore the nature of intellectual property in ship design, analyze key cyber threats for the industry, and provide guidance on mitigating the risks.

2. THE ROLE OF SMES IN NAVAL DESIGN AND ENGINEERING

While a precise count is difficult, it's safe to say that there are thousands of shipyards, well over a hundred thousand marine architecture and engineering companies, and maritime equipment suppliers operating globally. The industry is constantly evolving, with new facilities and existing ones expanding to meet the growing demand for ships and services.

With over 300 shipyards and 22,000 maritime equipment suppliers in Europe alone, SMEs provide a significant portion of the innovative technology used in modern shipbuilding, supporting around 900,000 highly skilled jobs [5]. As such, these businesses can be considered vital players, particularly in naval design and engineering, producing unique prototypes and equipment not found elsewhere. It goes without saying that the intellectual property generated is of immense value.

According to SEA Europe (The Shipyards & Maritime Equipment Association of Europe), European maritime equipment manufacturing companies hold more than 50% of the global market share, while European shipyards hold the most expensive order book. SMEs in naval design specialize in developing cutting-edge technologies, such as propulsion systems, navigation equipment, hull designs, and other vital maritime installations. These companies specialize in building the most intelligent, safe, and efficient vessels on the market, including passenger ships, research vessels, fishing vessels, offshore vessels, naval ships, and submarines [3]. Unlike larger corporations that might focus on mass production, SMEs are often involved in highly personalized projects, delivering solutions tailored to the specific needs of their clients. This is made possible by the significant investment in research, development, and innovation, with many dedicating more than 9% of their turnover to these activities [5]. The complex nature of naval design, where most vessels are built as prototypes, requires special attention to IP protection. Without adequate safeguards, these innovative companies risk losing their competitive edge and technological advancements to competitors through counterfeiting or industrial espionage.

3. INTELLECTUAL PROPERTY IN NAVAL DESIGN

Intellectual Property is a cornerstone of the naval design and engineering sector, particularly for Small and Medium Enterprises (SMEs) that drive innovation. IP in this context includes ship designs, propulsion systems, navigation technologies, software crucial for the creation and operation of advanced vessels, etc. [3].

Companies in naval design often rely on patents, trade secrets, and copyrights to safeguard their innovations and technical knowledge [5]. For example, the intricate design and construction techniques used in building specialized vessels, such as research ships, naval vessels, and autonomous ships, are highly valuable and proprietary. Without robust IP protection, these companies risk the unauthorized replication of their designs, leading to a loss of market share and a decline in technological leadership.

However, the complexity of the maritime industry, involving various stakeholders in the design, construction, operation, maintenance, and repair of vessels and equipment, requires careful consideration of trade secrets and IP rights. It is essential to balance the need for operational information with the protection of sensitive IP. As SEA Europe points out, it is crucial "to ensure that through the acquisition of a vessel or a piece of equipment, the buyer receives the necessary information for the operation and maintenance of the product but avoiding the transfer of sensitive information under IP protection from the shipbuilder or product supplier" [5].

To address these challenges, the industry has developed specific standards and practices. For example, the IMO implemented the Ship Construction File Industry Standard (SCF IS) in 2016. This standard contains information about vessel design and construction necessary for ensuring safety throughout its operational lifetime, including documents subject to high IP protection. To safeguard IP, sensitive documents are stored at an onshore Archive Centre rather than included in the onboard Ship Construction File [5]. This approach helps limit the transfer of sensitive information during the vessel's lifecycle, protecting the shipbuilder's and equipment supplier's proprietary knowledge.

Furthermore, industry associations advocate for enhanced IP regulations to safeguard maritime technology. SEA Europe, representing European shipyards and maritime equipment suppliers, has called for improved international cooperation to control counterfeit products installed onboard vessels, especially in regions where IP infringements are prevalent [5]. Additionally, SMEs are encouraged to adopt cybersecurity measures as part of their IP protection strategy, given the increasing risk of cyberattacks targeting digital assets and design files [8].

Recent developments in digital technologies have further complicated IP protection in the naval design sector. The integration of autonomous systems, artificial intelligence, and Internet of Things (IoT) devices into ship design has increased the volume of digital IP assets. These digital assets, which include software codes, algorithms, and data, are highly susceptible to cyberattacks and industrial espionage [9]. A breach in cybersecurity can lead to theft of sensitive design information and economic losses as well as damage to the company's reputation [10].

4. COMMON CYBER THREATS IN THE MARITIME INDUSTRY

4.1 Overview of the Maritime threat landscape

Due to the continuous digital transformation, integration of advanced technologies such as the Internet of Things (IoT), autonomous systems, and cloud computing, the maritime industry became increasingly vulnerable to a growing number of cyber threats.

The maritime environment consists of numerous interconnected stakeholders and infrastructures, including authorities, ports, maritime and insurance, shipbuilding companies, banks, supply chains, and other critical sectors, along with both physical and cyber assets. This interconnected nature of modern ships and maritime infrastructure, combined with a complex global supply chain, has expanded the industry's attack surface, making cyber risk management a critical concern. Moreover, due to this interdependence, a cyber-attack on any single entity can result in widespread repercussions throughout the entire maritime ecosystem. Cyber risks in the maritime sector have the potential to affect not only business operations but also the safety of vessels, crew members, and cargo [7].

As noted by ENISA [11], "Cybercriminals are responsible for the majority of attacks on the transport sector (54%), and they target all subsectors."

Cyber threats in the maritime industry are diverse and range from traditional IT-related risks to newer risks targeting operational technology (OT), such as ship navigation and control systems. Although the maritime sector faces numerous cyber threats, ransomware attacks have emerged as one of the most devastating and costly challenges facing the industry.

4.2 Ransomware and malware attacks

Ransomware and malware attacks have increasingly targeted both maritime companies and ports, with these attacks locking critical systems or encrypting data until a ransom is paid. This accounted for over 38% of observed incidents during the reporting period 2021-2022 [11] with threat actors often exploiting web applications, software vulnerabilities, and poorly protected network interfaces.

For SMEs in naval design and engineering, ransomware attacks present a particularly severe threat due to their potential to encrypt and deny access to critical intellectual property, including vessel designs, technical specifications, and proprietary engineering solutions. The business impact of such attacks can be catastrophic for smaller enterprises that may lack robust backup systems or incident response capabilities. Nonetheless, the impact of ransomware attacks extends beyond immediate operational disruption. When targeted against SMEs in naval design, these attacks can compromise not only the victim organization's intellectual property but also sensitive information about vessel capabilities, security features, and critical systems.

The interconnected nature of maritime operations further compounds the risk since SMEs often collaborate with larger shipyards, classification societies, and maritime authorities, sharing sensitive design data through various digital platforms. A ransomware attack on an SME could potentially compromise this broader ecosystem, leading to both immediate financial losses and long-term reputational damage that could be particularly devastating. One of the most prominent examples of this type of attack occurred in 2017 when the NotPetya ransomware hit Maersk, one of the largest shipping companies in the world, causing approximately $300 million in damages and severely disrupting global shipping operations [6].

Although ransomware attacks often cause the most visible damage, they frequently begin with a more subtle threat: phishing attacks. These social engineering tactics serve as the initial entry point for many of the most serious cyber incidents in the sector.

4.3 Phishing and social engineering

Phishing and social engineering attacks are also common, as cybercriminals use fraudulent communication methods to trick employees into granting access to sensitive systems by luring them into clicking malicious links or revealing credentials.

In the naval design sector, these attacks frequently aim to gather credentials for accessing sensitive technical documentation or to deploy malware into design and engineering systems. The effectiveness of these attacks is enhanced by the complex network of stakeholders in the maritime industry, making it easier for attackers to impersonate legitimate business contacts. Once access is gained, attackers can move through networks to compromise mission-critical systems, a particularly dangerous prospect given the growing prevalence of remote access to ships' systems [12]. Verizon's 2024 Data Breach Investigations Report highlights that phishing remains a leading cause of initial breaches, with the human element contributing to nearly 68% of breaches across industries, including maritime [13].

While phishing usually targets individual employees, an even broader vulnerability exists in the complex web of relationships that characterize maritime operations. The industry's reliance on extensive supply chains creates additional attack vectors that malicious actors are increasingly exploiting.

4.4 Supply chain vulnerabilities

The maritime industry's heavy reliance on global supply chains has made it highly vulnerable to supply chain attacks, where threat actors infiltrate third-party vendors or service providers to gain access to critical systems. Several incidents have demonstrated how susceptible the entire maritime ecosystem is to attacks on ports, shipbuilders, and logistics companies [6]. In naval design, such attacks might target software development tools, computer-aided design systems, or third-party engineering services. The risk of such attacks has grown with the prevalence of zero-day exploits and supply chain vulnerabilities, where flaws in third-party software can be exploited to launch ransomware and extortion attacks [13]. The impact can be severe, as compromised supply chain elements could introduce vulnerabilities into vessel designs or compromise the integrity of critical systems before they are even deployed.

Beyond the IT infrastructure and supply chain vulnerabilities, a particularly concerning trend has emerged in the maritime sector: the targeting of operational technology systems. These attacks represent a shift from purely digital threats to those that can directly impact physical operations.

4.5 Operational technology (OT) attacks

Operational technology (OT) attacks, which directly target the systems that control physical processes such as navigation and propulsion, have become an increasing concern. As vessels and ports further integrate IT and OT, these attacks are becoming more frequent. The potential for cybercriminals to compromise OT systems, such as disabling a ship’s steering or causing cargo handling systems to malfunction, presents serious safety risks. Also, with the increased use of Low Earth Orbit (LEO) satellite networks to improve vessel connectivity, the potential attack surface widens, providing cybercriminals with greater opportunities to infiltrate OT and IT systems through backdoor vulnerabilities [14].

The 2023 survey by DNV showed that 60% of maritime professionals expect cyberattacks on OT systems to result in physical harm or vessel collisions in the near future.

The geopolitical landscape also influences cyber risks in the maritime sector. For instance, during the Ukraine war in 2022, vessels crossing the Black Sea and the Sea of Azov experienced a series of cyber-attacks, including GPS interference, AIS spoofing, and communications jamming [11].

4.6 Insider threats

Another threat not to be overlooked is the insider threat, as it poses a significant risk to intellectual property, particularly with the widespread adoption of cloud-based collaboration tools. Insider threats can be both intentional actors (who knowingly cause harm) and unintentional actors (who may inadvertently expose sensitive information). The threat is amplified by the ease with which employees can transfer sensitive design files and technical documentation using cloud services such as WeTransfer, Google Drive, or personal email accounts.

In the context of naval design, insider threats present a unique challenge because employees inherently require legitimate access to valuable intellectual property, including detailed technical specifications, design documents, and proprietary engineering solutions. The modern design workflow, which relies heavily on cloud-based file sharing and collaboration tools, creates an environment where sensitive data can be exfiltrated with minimal technical barriers. This situation is particularly problematic because the actions involved in IP theft often mirror legitimate work activities, making detection extremely challenging.

The ability to quickly and discreetly transfer large amounts of technical data through cloud services makes insider threats a significant concern for SMEs in naval design, who must balance the operational benefits of cloud-based collaboration tools with the need to protect their intellectual property.

The prevalence of insider threats highlights a broader issue within maritime cybersecurity: the critical importance of the human factor. This brings us to one of the industry's most persistent challenges: the need for comprehensive security awareness and training.

4.7 Training and compliance challenges

There is a widespread lack of cybersecurity awareness within the maritime industry. Many employees, particularly at the operational level, are not sufficiently trained in cybersecurity best practices. This lack of training creates vulnerabilities, as simple human errors can expose companies to significant risks [7].

Although organizations like the International Maritime Organization (IMO) and IACS have developed cybersecurity guidelines, there is still no unified global regulatory framework for maritime cybersecurity, especially for existing infrastructure. As a result, many companies remain uncertain about how to implement best practices and ensure compliance with evolving standards.

The gaps in training and compliance contribute to a larger concern that affects all maritime organizations: the growing financial burden of cyber incidents. Understanding these costs is crucial for justifying investment in cybersecurity measures.

4.8 Financial impact of cyber threats

The financial losses incurred due to cyber incidents are often substantial, stemming not only from ransom payments but also from downtime, damage to infrastructure, and loss of revenue. Given the continuous nature of maritime operations, the financial ramifications of a cyberattack are severe. Studies reveal that the average cost of a cyber breach in this sector has risen significantly, with some estimates suggesting a 200% increase in recent years due to the escalation of ransomware and other extortion tactics. The financial burden is exacerbated by the challenge of obtaining comprehensive cyber insurance, as many maritime organizations struggle to meet the eligibility requirements due to gaps in cyber risk management maturity [14].

Understanding the various types of cyber threats facing the maritime industry is crucial, but equally important is recognizing their comprehensive impact on maritime organizations, particularly SMEs. The consequences of security breaches go far beyond immediate financial losses, affecting operations, reputation, and long-term business sustainability. As we examine these impacts in detail, it becomes clear that security breaches in the maritime sector create ripple effects that touch every aspect of an organization's operations, from day-to-day activities to strategic planning and market position.

5. IMPACT OF SECURITY BREACHES

The impact of security breaches on Small and Medium Enterprises (SMEs) operating in the maritime industry can be both extensive and multifaceted, encompassing financial, operational, and reputational consequences.

According to the 2024 Cost of a Data Breach Report [15], the global average cost of a data breach reached USD 4.88 million, a significant increase over previous years, driven largely by business disruption and the high costs associated with post-breach recovery efforts. For SMEs in ship design, where intellectual property and operational technology (OT) integrity are paramount, these costs are particularly devastating, as the financial burden can far outweigh an SME's available resources, impacting its long-term viability.

One primary financial consequence of security breaches is the direct cost of data recovery, system repair, and regulatory fines, which are often exacerbated by an SME's limited cybersecurity infrastructure. These immediate expenses are heightened by longer-term financial losses, including potential litigation, fines from regulatory bodies, and the cost of implementing enhanced security measures post-breach. IBM's findings highlight that business disruptions and post-breach expenses can total as much as USD 2.8 million in lost business, further emphasizing the vulnerability of SMEs that rely on continuous operations. For companies that are unable to swiftly recover, these costs can lead to severe revenue loss and, in extreme cases, business closure.

The financial burden is exacerbated by the challenge of obtaining comprehensive cyber insurance, as many maritime organizations struggle to meet the eligibility requirements due to gaps in cyber risk management maturity [14] and the increasing frequency of attacks.

Operational disruptions resulting from security breaches can severely impact an SME's ability to meet project deadlines and maintain client relationships [16] especially because there is often a need to halt ongoing projects to assess and mitigate security vulnerabilities, leading to project delays and potential contractual penalties. For SMEs, which may not have the resources to maintain redundant systems or advanced recovery strategies, these disruptions can be catastrophic, resulting in the inability to fulfil contracts and meet client expectations. Delays can strain partnerships and hinder future business opportunities. Moreover, in a sector where project-specific customizations are common, any delay or breach of trust can discourage repeat business, impacting the SME's long-term viability.

Reputational damage following a security breach can be particularly severe. The interconnected nature of maritime operations means that a breach affecting one organization can have cascading effects throughout the supply chain. Entire supply chains can be disrupted through a security breach originating in an SME, as evidenced by high-profile incidents like the NotPetya attack on Maersk, which resulted in weeks of operational downtime and hundreds of millions of dollars in losses [16].

Trust and reliability are essential in the maritime industry, particularly when working with sensitive data and proprietary technologies. A security breach can lead clients, partners, and classification societies to question a company's ability to safeguard sensitive information, weakening existing relationships and deterring potential customers. This loss of trust is difficult to rebuild and can hinder a company's ability to secure future projects or funding.

Furthermore, legal and regulatory consequences of security breaches have become increasingly significant. With the implementation of stricter cybersecurity regulations and data protection requirements, organizations face potential fines and legal liabilities following a breach. For SMEs, the cost of regulatory compliance and potential penalties can represent a substantial burden on their resources.

However, the impact of security breaches extends beyond immediate financial and reputational losses. In the context of naval design, compromised intellectual property can have long-term strategic consequences. The loss of proprietary design information can erode competitive advantages. Cybercriminals and state-sponsored attackers often target SMEs for proprietary information, particularly in innovative sectors such as ship design [6]. Once stolen, intellectual property can be exploited by competitors or malicious actors, effectively nullifying an SME's competitive advantage and jeopardizing years of investment in research and development but may also be posing risks to national security in cases involving naval or defence-related ship designs.

6. CYBER RISK MANAGEMENT FOR SMES

Small and Medium Enterprises (SMEs) in the maritime industry, particularly those engaged in naval design and engineering, are increasingly vulnerable to cyber threats due to their reliance on digital technologies and limited resources. Thus, implementing effective cyber risk management is essential to protect their operations and intellectual property.

6.1 Framework implementation and governance

SMEs in the maritime industry are vulnerable to various cyberattacks, including ransomware, phishing, and attacks on their operational technology (OT) systems [6]. According to ENISA [11], maritime cybersecurity must be treated holistically, addressing IT and OT systems while considering the complex interactions between physical and cyber assets.

One of the most effective ways for SMEs to manage cyber risks is by adopting established cybersecurity frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework [17] or the International Organization for Standardization (ISO) 27001 standard [7]. These frameworks provide a structured approach to identifying, assessing, and mitigating cyber risks. They also encourage companies to develop incident response plans and ensure that systems and data are protected against potential cyber threats.

The Baltic and International Maritime Council (BIMCO) and ENISA's approach to cybersecurity management are based on the NIST Risk Management Framework. This framework provides a structured methodology that identify assets and threats, assess vulnerabilities, estimate risk exposure, develop protection measures, establish contingency plans, and create incident response procedures. It is particularly relevant for SMEs in naval design, where protecting intellectual property is crucial.

The importance of framework implementation is illustrated by several significant incidents in the maritime sector. For instance, COSCO's successful defence against ransomware in 2018 demonstrates the value of following established frameworks. Their Americas region remained operational due to proper implementation of NIST framework principles, particularly network segmentation, while other regions suffered significant disruptions [11].

6.2 Asset identification and risk assessment

The first step of an efficient risk management process is the identification of critical assets and weak points. This is also essential for protecting SMEs' IP in ship design, focusing on valuable data like design files, R&D, technical specifications, and proprietary engineering processes. Digital assets may also include software codes, algorithms, and data highly susceptible to cyberattacks and industrial espionage.

The critical nature of asset identification is highlighted by the 2020 Port of Long Beach assessment, which discovered over 200 exposed industrial control systems connected to the internet without proper security controls. The assessment revealed multiple OT systems using default passwords and unencrypted communications, with 25% running outdated software versions with known vulnerabilities. Similarly, a 2021 Mediterranean Shipping Company audit across 30 vessels identified 150+ unpatched navigation systems with direct internet connectivity, demonstrating the importance of regular asset assessment and vulnerability identification [6].

Organizations must also identify potential threats, vulnerabilities, and risks to these assets, considering internal and external threat actors. This includes mapping data flows, understanding system dependencies, and documenting the organization's role within the broader maritime supply chain. This step also includes assessing weak points in network access, remote collaboration tools, and third-party vendor relationships.

SMEs can use risk assessments, audits, and asset inventories to prioritize high-risk assets and align their cybersecurity efforts to protect the most valuable resources.

Clear governance structures and security plans should be established to cover both physical and cyber domains. Organizations should develop and maintain comprehensive security plans, including roles and responsibilities, asset ownership, and specific security responsibilities. This structured approach helps maintain an acceptable level of risk across physical, cyber, and hybrid threats. Business Impact Analyses and regular risk assessments are also essential elements of this phase, supported by Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) to ensure that both physical and cybersecurity aspects are continually monitored and evaluated [11].

Supply chain security is another critical aspect, especially for SMEs that rely on a network of contractors, suppliers, and service providers. Managing third-party risks includes conducting security assessments of partners, establishing clear security requirements in contracts, and monitoring partner compliance with these requirements [5]. Given the increasing frequency of supply chain attacks in the maritime sector [11], SMEs must carefully assess the security practices of all entities with access to sensitive design data or critical systems, ensuring that these external relationships do not compromise the organization's IP security.

6.3 Protection strategies and controls

Once critical assets are identified, a comprehensive protection strategy should be implemented. At its foundation, this strategy requires robust access control mechanisms, including multi-factor authentication (MFA) and strong password policies. Network segmentation plays a crucial role in creating secure boundaries that limit unauthorized access to sensitive systems.

The effectiveness of robust protection strategies is demonstrated by the 2019 Hamburg Port Terminal incident, where multi-layer authentication systems and network segmentation successfully thwarted a concentrated attack on cargo management systems. The properly implemented zero-trust architecture prevented lateral movement when attackers attempted to compromise systems through third-party logistics software [11]. This case exemplifies how comprehensive protection strategies can prevent operational disruption even when initial access is achieved.

For SMEs in ship design, protecting intellectual property demands particular attention to securing computer-aided design (CAD) systems, simulation software, and other specialized design tools through secure configurations and regular security updates.

Data encryption forms another vital layer of protection, especially critical when sensitive design files are stored or shared in cloud environments. The increasing adoption of cloud-based services in ship design, while offering cost-effective storage and collaboration opportunities, requires additional security considerations. SMEs must carefully evaluate cloud services to ensure that they implement appropriate security controls, maintain compliance with data protection regulations, and address data residency requirements.

Protection measures must also extend to operational technology (OT) systems through secure configurations and protocols for remote access, thereby minimizing exposure to external threats.

However, technical controls alone are insufficient. A structured approach to security governance, incorporating mandatory policies, standards, procedures, and baselines, provides the baseline for comprehensive protection. This governance structure must be supported by regular employee training and awareness programs to address the human element of security [14].

All personnel, including third-party contractors, must understand their roles in protecting intellectual property, handling sensitive data, recognizing security threats such as phishing attempts, and following established security protocols. This human-centric approach is fundamental in reducing cybersecurity risks, particularly those stemming from human error. By combining technical controls, governance structures, and human awareness, SMEs can establish a robust defence against cyber threats while maintaining efficient design operations.

Although protection measures form the first line of defence, they cannot guarantee complete security. This reality necessitates robust detection capabilities that can identify potential security incidents before they escalate to major breaches.

6.4 Detection capabilities and monitoring

The next step is detection. Detection capabilities represent a crucial component of cybersecurity defense, requiring a comprehensive approach to identifying potential security events before they escalate into serious incidents. This involves implementing sophisticated monitoring tools that provide real-time alerts for unusual activity across IT and OT systems. Central to this detection strategy is the deployment of Intrusion Detection Systems (IDS), which are specifically configured to flag unauthorized access attempts and monitor traffic patterns that might indicate an impending breach.

The consequences of inadequate detection capabilities are starkly illustrated by the 2017 Maersk NotPetya attack, where lack of adequate monitoring allowed malware to spread for 7 hours before detection, ultimately affecting 49,000 laptops and 1,000 applications across 600 locations [6] [16]. Conversely, the 2020 Port of San Diego breach demonstrates both the value and limitations of detection systems - while early detection identified anomalous encryption activities, incomplete sensor coverage (affecting 60% of systems) significantly hampered response effectiveness.

A successful detection model requires continuous monitoring through a dedicated incident-handling team, responsible for forecasting, identifying, analyzing, and responding to security incidents. This team must implement regular vulnerability scans and system audits to proactively identify potential weaknesses while establishing clear thresholds for alerts that enable quick identification and containment of threats before they can compromise critical intellectual property or disrupt operations.

The detection strategy must extend beyond internal systems to encompass supply chain vulnerabilities, a known risk in the maritime sector. SMEs must implement monitoring practices that ensure their third-party partners comply with established security protocols. This includes regular security posture assessments of contractors and suppliers, particularly those with access to valuable intellectual property or sensitive design data. Monitoring tools and anomaly detection systems play a vital role in identifying suspicious activity across these extended networks, enabling organizations to detect potential security incidents early in their lifecycle.

A key aspect of effective detection is the establishment of baseline system behavior patterns and clear definitions of what constitutes suspicious activity. This includes monitoring access patterns to sensitive design files, unusual data transfers, and unexpected system changes. Regular testing and refinement of these detection capabilities ensure they remain effective as threats evolve and new technologies are adopted. By maintaining comprehensive monitoring across all systems and supply chain interactions, SMEs can better protect their intellectual property and maintain the integrity of their design operations while quickly identifying and addressing potential security incidents.

6.5 Incident response planning

The response step implies a well-defined incident response plan that enables a swift and effective reaction to cyber incidents. This plan must outline specific procedures for isolating affected systems, containing the breach, and mitigating potential damage to digital assets and business operations. For SMEs in ship design, where intellectual property has significant value, the response plan must prioritize the protection of sensitive design data while maintaining business continuity.

The CMA CGM ransomware attack in 2020 demonstrates the importance and challenges of incident response. While their team executed a rapid response - shutting down external access points within 15 minutes and progressively closing e-commerce platforms over 2 hours - booking systems remained offline for 12 days, resulting in estimated losses of $50M [11]. In contrast, the European Container Terminal's 2021 response team successfully contained a ransomware outbreak within 30 minutes through automated containment procedures and immediate OT system air-gapping, maintaining basic operations throughout the incident.

A designated incident handling team should execute the response plan, following established protocols for different incidents, from ransomware attacks to intellectual property theft. This team must be empowered to make quick decisions about system isolation, stakeholder communication, and implementing mitigation measures. Clear communication channels and escalation procedures ensure that all relevant stakeholders, including management, clients, and regulatory bodies, are informed appropriately about incidents and their potential impact.

The response strategy must also address business continuity, ensuring that critical design operations can continue even during incident handling. This includes having predetermined procedures for operating in a degraded mode while maintaining the security of intellectual property and design data. The plan should detail specific steps for different scenarios, such as ransomware attacks targeting design systems, data breaches affecting proprietary information, or supply chain compromises that could impact ongoing projects.

Regular testing of response capabilities through cybersecurity drills and tabletop exercises is essential for maintaining readiness [14]. These exercises should simulate various scenarios specific to ship design operations, allowing the incident handling team to practice their roles and identify potential gaps in the response plan. By regularly reviewing and updating response procedures based on exercise outcomes and lessons learned from actual incidents, companies can continuously improve their ability to handle cyber incidents effectively while protecting their valuable intellectual property and maintaining critical business operations.

After containing and responding to an incident, organizations face the critical challenge of returning to normal operations. The recovery phase represents not just technical restoration, but an opportunity to strengthen security posture and rebuild stakeholder confidence.

6.6 Recovery and business continuity

The recovery phase focuses on restoring normal operations and ensuring business continuity following a cyber incident, with particular emphasis on protecting intellectual property and maintaining client trust throughout the recovery process. For SMEs in ship design, this phase requires a comprehensive recovery plan that addresses both technical restoration and business relationships.

The 2019 Port of Barcelona attack provides a model for effective recovery, achieving full-service restoration within 48 hours through the implementation of prepared business continuity procedures and validated backup systems [11]. Key success factors included segregated backups, practiced recovery procedures, and established communication protocols.

Similarly, the Mediterranean Port Authority's 2022 recovery efforts demonstrated the importance of forensic analysis in preventing future incidents, as it led to the identification of the initial compromise through third-party maintenance software and subsequent implementation of enhanced monitoring systems [14].

The cornerstone of effective recovery is the secure restoration of systems and data from verified backups. This process must be methodical and secure, ensuring that restored design files and technical documentation maintain their integrity while preventing the reintroduction of any malware or vulnerabilities that may have contributed to the initial incident. A thorough post-incident analysis must be conducted to detect any remaining vulnerabilities, and necessary improvements should be made to prevent similar incidents in the future.

Recovery efforts must align with regulatory requirements and industry standards. Additionally, organizations must document all recovery activities, maintaining detailed records of security assessments, incident responses, and system modifications to demonstrate compliance and support future improvements.

Clear communication with stakeholders is crucial during the recovery phase. SMEs must establish and maintain transparent communication channels with clients, partners, and regulatory bodies throughout the recovery process. This includes providing realistic timelines for service restoration and regular updates on progress, which helps rebuild trust and maintain business relationships. Regular testing of recovery protocols through drills ensures that organizations can execute their recovery plans effectively when needed, minimizing operational downtime and maintaining client confidence.

Financial considerations also play a vital role in recovery planning. SMEs should consider cyber insurance as part of their recovery strategy, as it can provide crucial financial support and additional resources during the recovery process.

Engagement with industry associations, such as the International Association of Classification Societies (IACS), can provide valuable guidance on recovery best practices, particularly through standards like UR E26 and E27, which enhance overall security posture and support effective recovery capabilities.

6.7 Limitations and challenges

Adhering to cybersecurity frameworks like NIST provides structured guidance and reduces cyber risks but does not guarantee complete protection from incidents. Attackers continuously develop new tactics that can circumvent even robust security measures, particularly in complex environments where IT and OT systems intersect, as seen in the maritime industry. Human error remains a significant vulnerability, with misconfigurations or phishing scams often leading to breaches, despite training and access controls. For SMEs, limited resources can create protection gaps, leaving critical assets under-monitored. Furthermore, frameworks address known risks, but unknown (zero-day) vulnerabilities still pose threats that can bypass existing defences. While cybersecurity frameworks are essential for establishing a strong security posture, they must be part of a broader, adaptive strategy involving continuous updates, threat intelligence, and proactive incident response.

7. CONCLUSIONS

The increasing digitalization of the maritime industry, particularly in naval design and engineering, has created unprecedented opportunities for innovation while simultaneously introducing significant cybersecurity challenges for Small and Medium Enterprises. This research demonstrates that maritime SMEs face a complex threat landscape that endangers both their operational resilience and valuable intellectual property (IP), which often represents their primary competitive advantage in a global market [16].

Our analysis reveals that the convergence of information technology (IT) and operational technology (OT) in modern ship design has expanded the attack surface, making SMEs particularly vulnerable to sophisticated cyber threats. The financial impact of security breaches poses an existential risk as smaller enterprises often lack resources for comprehensive cybersecurity programmes [15]. This vulnerability is compounded by the increasing frequency of ransomware attacks, the sophistication of supply chain compromises, and the persistent challenge of insider threats.

The research emphasizes that effective cyber risk management for maritime SMEs requires a holistic approach that balances security needs with operational efficiency. Established frameworks, such as NIST and ISO 27001, provide a structured methodology for protecting intellectual property while allowing for the agility essential to ship design innovation. However, the success of these frameworks depends on their adaptation to the specific constraints and requirements of maritime SMEs, especially those with limited resources. Furthermore, this study highlights the critical importance of supply chain security in the maritime sector.

The interconnected nature of modern shipbuilding operations means that vulnerabilities in one organization can have cascading effects throughout the entire industry. This interdependence necessitates a collaborative approach to cybersecurity, where SMEs work closely with partners, suppliers, and classification societies to establish robust security protocols and foster trust.

Looking ahead, the maritime industry must address several emerging challenges. The increased adoption of autonomous systems and Internet of Things (IoT) devices in ship design will continue expanding the cyber-attack surface. Additionally, the growing sophistication of state-sponsored attacks on maritime IP necessitates greater collaboration between industry stakeholders and government agencies to develop stronger defence mechanisms.

For future research, we recommend exploring the potential of emerging technologies such as artificial intelligence and blockchain in enhancing maritime cybersecurity, particularly for resource-constrained SMEs. Further studies should also evaluate the effectiveness of current regulatory frameworks in protecting maritime IP and investigate sector-specific security standards that address the unique challenges faced by naval design SMEs [14].

In conclusion, IP protection and ensuring cybersecurity in maritime SMEs requires a delicate balance between innovation and security. Success in this endeavour demands not only technical solutions but a shift in organizational culture, where cybersecurity is seen as an enabler of innovation rather than a barrier. As digital transformation progresses, the ability of SMEs to safeguard their IP while maintaining operational efficiency will be increasingly critical to their survival and success in the global maritime landscape.

REFERENCES

[1]. T. Pseftelisa and G. Chondrokoukisb, "A Study about the Role of the Human Factor in Maritime," *SPOUDAI - Journal of Economics and Business,* vol. 71, no. 1-2, pp. 55-72, 2021.

[2]. EUROSTAT, "International trade in goods by mode of transport," EUROSTAT, 2024.

[3]. SEA Europe, "Position Paper on the European Commission's Communication "Making the most of the EU's innovative potential. An intellectual property action plan to support the EU's recovery and resilience," 19 February 2021. [Online]. Available: https://www.seaeurope.eu/images/files/2021/Position-papers/Regulatory-Affairs/sea-europes-position-paper-on-the-eu-ip-plan.pdf. [Accessed 9 October 2024].

[4]. F. Torres Pérez and S. Louredo Casado, "Advantages and Challenges of Intellectual Property Rights Related to the Shipbuilding Process," *Comparative Maritime Law,* vol. 61, no. No. 176, pp. 363-386, 2022.

[5]. SEA Europe, "SEA Europe's Position Paper on the European Commission's new package for IPR Protection," 7 February 2018. [Online]. Available: https://www.seaeurope.eu/images/files/181/660/290433/3660/4/SEA%20IPR%20position%20on%20EC%20IPR%20Protection%20package%20FINAL.pdf. [Accessed 9 October 2024].

[6]. DNV, "Maritime Cyber Priority: Staying secure in the era of connectivity," DNV, 2023.

[7]. Department for Transport, UK, "Cyber Security Code of Practice for Ships," Department for Transport, London, 2023.

[8]. G. C. Kessler and S. D. Shepard, Maritime Cybersecurity: A Guide for Leaders and Managers, Independently published, 2022.

[9]. E. Tijan, M. Jović, S. Aksentijević and A. Pucihar, "Digital transformation in the maritime transport sector," *Technological Forecasting and Social Change,* vol. 170, no. September 2021, 120879, 2021.

[10]. R. Foote, "Cybersecurity in the Marine Transportation Sector: Protecting Intellectual Property," *Cybaris,* vol. 8, no. 2, pp. 231-264, 2017.

[11]. European Union Agency for Cybersecurity, "ENISA Threat Landscape: Transport Sector," 2023.

[12]. Mission Secure, "A Comprehensive Guide to Maritime Cybersecurity," 2023.

[13]. Verizon, "2024 Data Breach Investigations Report," 2024.

[14]. M. Kenney and F. Macdonald, "Shifting Tides, Rising Ransoms and Critical Decisions: Progress on maritime cyber risk management maturity," CyberOwl, HFW & Thetius, 2023.

[15]. IBM Security & Ponemon Institute, "Cost of a Data Breach Report 2024," IBM Corporation, 2024.

[16]. I. Progoulakis, P. Rohmeyer and N. Nikitakos, "Cyber Physical Systems Security for Maritime Assets," *Journal of Marine Science and Engineering,* vol. 9, no. 12 : 1384, 2021.

[17]. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," 2018.

[18]. BIMCO et al., Cyber Security Guidelines Onboard Ships, Version 4, 2021.

Paper received on November 2nd, 2024