Cyber security in the maritime & yachting sector

Introduction

The maritime industry is a compliance-oriented sector and historically deals with security issues on an international level. The adoption of onboard programmable systems has shown that safety and security in maritime industry is highly depending cyber systems, and cybersecurity implementation requirements have begun to be integrated into the maritime industry's regulatory environment. This white paper focuses on Cybersecurity, presenting a systemic approach to maritime cybersecurity aspects, with the main objective to connect the theoretical approach with the adoption of practice solutions with references to procedures and applicable regulatory frameworks.

Cyber resilience & cyber security

Cyber Security and Cyber Resilience are topics of major relevance to both the captain and the yacht owner, and both are needed to address cyber threat on board.

Cyber security refers to the methods and processes of protecting electronic data. This includes identifying data and where it resides and implementing technology and business practices to protect it.

- RINA helps prevent data breaches and reduce the risk of malicious activity

Cyber resilience is defined as an organization's ability to withstand or quickly recover from cyber events that disrupt usual operational and business activities.

- RINA help mitigate the impact of cyber attacks

As cyber threats are constantly evolving, regular commitment and attention are crucial to protect the digital assets of the organisation from critical events. The approach to Cyber Resilience adopted by RINA also includes the correction of vulnerabilities, the identification and mitigation of threats and training and awareness of the shipboard personnel on cyber issues.

RINA is the right partner to approach risk management and address the entire life cycle of all assets on board in terms of cyber. This also includes providing customised technology and tailored solutions to meet any particular needs of the yacht. Cyber Resilience & Cyber Security cannot exist independently without the other. To protect assets such as yachts, both must be in place for the entire operational lifecycle. In these terms RINA can:

- Perform an on-board assessment
- Tailor a suitable technology and digital solution to any particular needs
- Meet the specific requirement of each shipowner and captain

Continuous commitment and focus on protecting assets are crucial. RINA provide the best customised solutions to enable risk management and achieve that goal, thanks to the most advanced technology tools and digital solutions.

Maritime and marine regulations - IMO & flag administrations

Fundamental concepts, awareness and assessments are necessary to successfully prepare and respond to cyber threats in the maritime domain based on the BIMCO & NIST Framework guidelines. According to IMO (MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management), there is the urgent need to raise awareness on cyber risk threats and vulnerabilities. Moreover, IMO strongly recommends taking the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping.

Issuing the Guidelines on Maritime Cyber Risk Management, the IMO responded to an increase in cyber-attacks by accepting the NIST framework based on these five elements: identification, protection, detection, response, and recovery. According to NIST standard, it is essential in fact that actors in maritime and yachting define policies and governance regards to IT and OT, enforcing cybersecurity best practices, especially for most critical assets, with a risk-based approach:

Security policy and organisation commitment:

- Implementing an information systems security policy (ISSP) which describes all organisational and technical means and procedures
- Enforcing security governance of both IT and OT environments through the ISSP
- Sharing this ISSP with all stakeholders involved
- Reviewing annually the ISSP

Risk and Threats Management:

- Conducting and regularly update risk analysis to identify risk and threats
- Setting up security indicators and assessment methods to evaluate the compliance
- Setting up a threat intelligence process to watch continuously for vulnerabilities, identifying new risks and threats and deploy actions to mitigate them

Security and privacy by design:

- Developing a project methodology including security assessments and checkpoints
- Addressing privacy related issues based on applicable local and international regulations, such as the GDPR
- Launching a data classification project to identify critical data to protect them accordingly and to map the data flows

Asset inventory and management:

- Using centralised tools for asset inventory and management and keep them up-to-date
- Defining a policy regarding authorized devices and software
- Use centralised tools to monitor the different assets and detect unauthorized ones

Cyber resilience (Business continuity and crisis management):

- Ensuring cyber resilience of systems by defining objectives and strategic guidelines regarding business continuity and recovery management
- Defining important parameters for business continuity (RTO, RPO, etc.)
- Defining a crisis management plan
- Ensuring the efficiency of recovery procedures by setting up annual training exercises

RINA can provide and certify cyber security compliance with respect to the major requirements of administrations and flags such as: Italian, Isle of Man, Cayman, Marshall, Gibiltair, Bermuda, and USA.

RINA can provide "tailored" digital tools to support clients from the design phase, to shipboard personnel, in the correct production of documentation and the successive asset management for the entire lifecycle. In this regard, with a single investment RINA offers a double value through its cyber activities:

- Cyber security and cyber resilience are enforced on board the yacht
- Compliance with respect to an on-board design/installation according to international guides (BIMCO-NIST) is achieved. This allows the issue of an 'Assesment Certificate' or 'Certrificate of complinace' in line with the yacht's flag requirements

Major changes in the cyber requirements are already scheduled for 2024 applicable to yacht in Class. Thanks to RINA, shipowners and captains do not run the risk of being unprepared when these requirements change. Starting from 2024, new yachts will have to be designed and built according to the compliance with the minimum Cyber Resilience criteria established by international standards guides such as NIST and BIMCO, as well as Flagship requirements that refer to IMO requirements related to Cyber Risk Management. In this context, RINA can provide cyber security by-design solutions and apply them from the earliest stages of the design and construction of the yacht, following it through the entire assets life cycle.

Below, a mapping of good practices against challenges in cybersecurity field.

GOOD PRACTICES

ORGANISATION WIDE CHALLENGES	Asset Inventory IT/OT	Threats Identification	Risk management	Enforcing Mitigations	Address lifecycle of assets	Consider Cyber Insurance
Assessment of Measure Effectiveness	■	■	■		■	
Lack of resources			■	■		
Proactive adoption of security measures	■		■	■	■	■
Ensuring top management buy-in		■	■	■	■	■

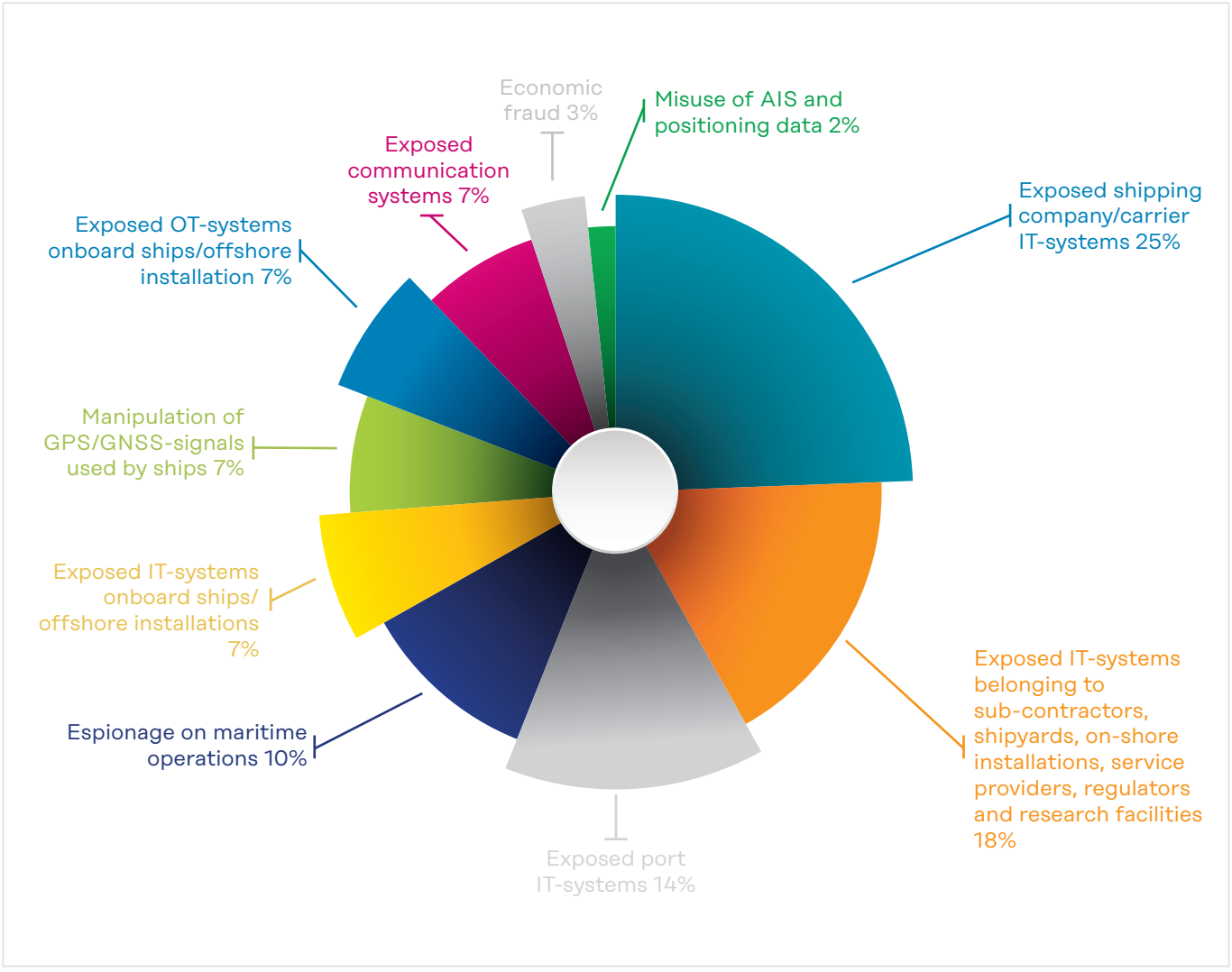
RINA's Cyber Security Division possesses all the necessary expertise to address the critical elements in the above matrix. To ensure that the captain and owner have a better understanding of the cyber situation on the yacht, RINA provides a tailored Yacht Cyber Manual that collects all data and information related to cyber security. This allows the security situation on your yacht to be better tracked and monitored. Only the following is the main differentiation on the contribution RINA can make regarding the type of yacht:

- For large yachts → RINA provides the Additional Class Notation
- For small yachts → RINA provides Assessment activities

In addition, RINA can assess the level of cyber resilience of naval assets on board yachts for cyber insurance purposes. Not only does Cyber Threats mean hacker attacks, but it also means misconfigurations, need for appropriate updates or upgrades, necessary patching, maintenance and much more. To manage all these aspects, Cyber Security Division at RINA developed HOLOS, an appropriate, fully customizable, digital Cyber Threat Management tool which can be used to address all these elements.

Research: threats, incidents and attacks in maritime and marine ecosystem

Cyber threats at a glance
Figure below: Top-10 cyber threats pie chart.



Malware insertion, in particular ransomware and ransomtheft, have been the prevalent attack methods. There are also many examples of fraud, using social engineering techniques, fake invoices and theft of user accounts. These attacks stem from cybercrime actors with "pure" economic motives.

Threats related to espionage on maritime operations, attacks on sub-contractors, shipyards and research facilities, as well as attacks on GNSS-systems, may be linked to another breed of actors, particularly state-sponsored actors or cyber warriors. These are well-funded, motivated by political factors or acquiring foreign technology, and can be extremely difficult to defend against.

Cyber threats categorization

A threat is the potential cause of an unwanted incident, which can result in harm. The categories are not mutually exclusive and can overlap for a single incident.

- Exposed shipping company/vessel IT-systems → Ransomware represents the most common attack vector, usually in the form of email attachments or links. Not differently from other sectors, there is an increasing trend of ransomtheft viruses, that combine outages and information theft. Furthermore, there is no shortage of examples of economic fraud resulting from social engineering attacks. In the case of social engineering, the attackers try to cause harm via e-mail which seems harmless at a glance, via fake web site, sharing platforms or social media as well. On the other hand, malware phishing uses malwares installed on client's PC and devices

- Committing criminal activities by using ransomware and malware, unauthorized access results in data theft and data deletion in order to hide the traces or to cause a lot of harm to business

- Exposed IT-systems belonging to sub-contractors, shipyards, on-shore installations, service providers, regulators and research facilities → The incidents typically involve theft of business-critical information, as well as more random cases of extortion. Incidents show that social manipulation, hacking and ransomware are commonly used attack vectors

- Exposed port IT-systems → Interruptions are expensive, and therefore attackers prefer this technique to carry out extortions. In addition, information theft and manipulation have been used for smuggling operations

- Espionage on maritime operations → This includes incidents characterized by extensive and targeted attacks related to espionage, tapping and surveillance of maritime operations. Mentioned attack vectors tend to be spear-phishing or general hacking, as well as communication tapping

- Exposed IT- systems onboard ships/offshore installations → Typical attack vectors for this category are email attachments and links, enough to render ship servers and clients useless. There has been limited forensic evidence left afterwards as all data are usually wiped clean

- Manipulation of GNSS-signals used by ships → This category is mainly related to jamming or spoofing of GPS/GNSS-signals that ships use for navigational purposes. State-sponsored actors tend to be put under suspicion for these events, and the consequences have been more of a disturbing than critical nature

- Exposed OT-systems onboard ships/offshore installations → The systems are typically entered by attackers via infected USB units or computers unintentionally connected to the wrong network. ECDIS (during map updates) and propulsion control systems are just few examples of targets

- Exposed communication systems → Because of many different and necessary communication systems onboard, this category represent a highly potential victim. According to the incident statistics, the main consequences tend to be loss of availability caused by generic hacking or ransomware. Data theft usually goes unnoticed or is discovered too late

- Economic fraud → These incidents are typically caused by targeted and specialized attacks, where counterfeit emails or hacked user accounts are used as attack vectors to initiate or manipulate economic transactions. Incident data shows that among the most frequent occurrences are alteration of account information or sending of fake invoices

- Misuse of AIS and positioning data → There are several known events where AIS-systems onboard ships have been unlawfully manipulated or deactivated. These incidents are generally related to smuggling operations, trafficking, illegal fishing or military conflicts. Among the worst potential consequences could be collisions, but it is more likely that other ships are forced to alter their course unnecessary

Specific threat and common vulnerabilities on board of a yacht

- As far as cybersecurity onboard yachts is concerned, the main common mistake is to primarily focus on the usual computer equipment (navigation, PC, servers, CCTV ...), but the entry points for criminals are generally on everyday applications or common objects: smartphones, audio-video on board, Wi-Fi, home automation equipment, gaming devices, emails, connected objects

- IT/OT convergence has led the yachting sector to rely on commercially available technologies for part of its processes, often using the Internet of Things (IoT). This leads to an increased risk of unauthorised access or malicious attacks on yachts' systems and networks. Even the most unsuspected device (with its 24/7 access to internet) can be an attack vector for cyber criminals:

    - A gaming console connected to the yacht's network could be hacked by third parties. The hackers could get access to the camera and the speaker-microphone system and used them to invade users' privacy, getting sensitive information or data and put in place an extortion. In addition, online multiplayer gaming is a typical attack vector for scams, using phishing and malware
    - The fish tank is provided with sensors that monitor temperature, food and cleanliness. By accessing this, it is possible to reach other areas of the network onboard yacht
    - Malicious attackers could gain remote control of common smart devices if they are not sufficiently protected. There have been cases where thermostat systems and sound systems have been hacked to excessively raise the temperature and play unpleasantly music at very high volume in the middle of the night
    - A group of students successfully proved weaknesses and imperfections of Global Positioning System (GPS). In 2013 they hacked the GPS signal on a private yacht and distributed false position data to navigational equipment. As the track-pilot was active, automatic correction of course had been initiated in order to put the yacht back on route
    - A remote hacker attack could allow attackers to open the yacht's garage door and operate the tender's release mechanisms, even while cruising and without anyone realising it
    - Risks can occur both on-board and off-board systems. Satellite communication systems and, when close to the coast, 4G and 5G networks allow access to on-board networks and data
    - Isolated systems with disabled connectivity are still exposed to a number of cyber risks. For example, malware introduced through a removable media or other connected data storage device to upload/download data from the network of a critical system
    - Real-time connectivity, aimed at optimising maritime operations and customer experience and satisfaction, is increasing the cyber attack surface and lethality of potential incidents. Among the most sensitive and vulnerable systems are the navigation systems, GNSS (global navigation satellite system), VDR (voyage data recorder) and radar. Equally critical are propulsion management systems, access control systems, on-board surveillance, tablets used by the crew, and communication systems. A lack of security could expose all these systems to the risk of sabotage or tampering, seriously compromising both availability and safety

- Common vulnerabilities onboard yachts have to be more focused also in the OT assets:

    - Use of obsolete operating systems
    - Absence of adequate software for security purposes
    - Inefficiency and ineffectiveness in the management of information systems
    - Inadequate security configurations, including wrong use of default administrator accounts and passwords
    - On-board computer networks that lack perimeter protection and measures of network segmentation
    - Safety-critical equipment always connected to the coast
    - Inadequate access controls

- In the case of charter contracts established between a shipowner company and a client, it is important to sign a specific cyber risk management agreement. This practice protects both the client in terms of privacy and sensitive information and the ship owner in terms of business continuity

- A major vulnerability occurs when yacht is docked. All data that can be exchanged between the yacht and the ground flows through internet and Wi-Fi networks. In addition, dedicated Wi-Fi networks are often opened to services of specific equipment in the port or marina (e.g. for maintenance personnel). For all these circumstances there is no regulation that applies, and cases of data leakage are frequently reported

Holistic approach for cybersecurity onboard yachts

Issues concerning cyber security do not apply on the basis of gross tonnage, length, class or type, but it is a topic that deeply impacts all yachts. Where on-board entertainment systems and innovative digital technologies are present, exposure to cyber threats increases exponentially. Furthermore, due to the increasing integration between IT/OT systems, it is important that the demarcation line between those two environments is clear. One of the main weaknesses lies in the mild cyber regulation in the maritime field.

This makes yachts and vessels even more vulnerable, as they represent an easy target. What IMO asks for ensuring cybersecurity onboard yachts:

- Have clear and operational documentation on the yacht's digital perimeter, access to systems, sensitive applications, emergency situations and backups.
- Awareness training for crew and management-oriented training for captains and first officers.

The following points are part of a holistic overview to assess and ensure cyber security onboard yachts:

- Technology - e.g., Isolate yacht's virtual networks, including Wi-Fi access. This can prevent criminal from reaching sensitive networks (like "audio-video", "CCTV", "work", "owner", etc.) through simply gaining access to a minor network (like "guests" or "crew")
- Organization - e.g., Manage passwords carefully, as well as access rights. Introducing the use of a password manager to manage and share passwords and accesses onboard yachts only among authorized people
- Human - e.g., An ordinary smartphone can be considered the most exposed cyber equipment of the yacht. If corrupted, criminals can read messages, listen to discussions in cabins, control the email box, spoof the identities, and get codes received by text
- Procedures - e.g., Introduce compliant procedures that apply for any level: yacht, crewmates, external contractors, suppliers, etc
- Security reporting - e.g., Add digital security to the management practices onboard yachts. Use simple appropriated dashboards
- Training & Awareness - e.g., Train the crew on best practices. Training Awareness sessions offer the required crew awareness (2hr) and management-orientated training for captains and first officers (2-3hr) required by the IMO. Sharing experiences, debriefing criminal attempts or incidents are excellent practices for cyber risk awareness at all levels: crew, suppliers, and yacht managers

RINA can be the partner who can tangibly tackle cyber threats on board yachts, validating an adequate level of cyber posture:

- OT/IT Asset Inventory, Rysk Assesment, Gap analysis & Ship Assessment
- Design ofsecure products, services and processesfrom the requirements specification to the certification
- Technical advisory for the development and deploy of secure systems, as well as process establishment
- Security-related services to monitor and improve cybersecurity aspects
- Improve IT/OT resilience to cyber incidents by means of properly designed processes and procedures
- Requirement definition, verification & validation, security evaluation process according to international schemes, security technology scouting and procurement
- Vulnerabilities assessment, penetration tests, awareness and training campaigns, periodical audit to verify the correct "Cyber Posture"
- Risk Management, Change management, Cyber threat intelligence, supply chain audits.
- Support during the entire Asset's life-cycle ready to develop secure tailored solutions for your needs and priorities
- Finding the right settings and avoiding misconfigurations of devices installed on board the yacht