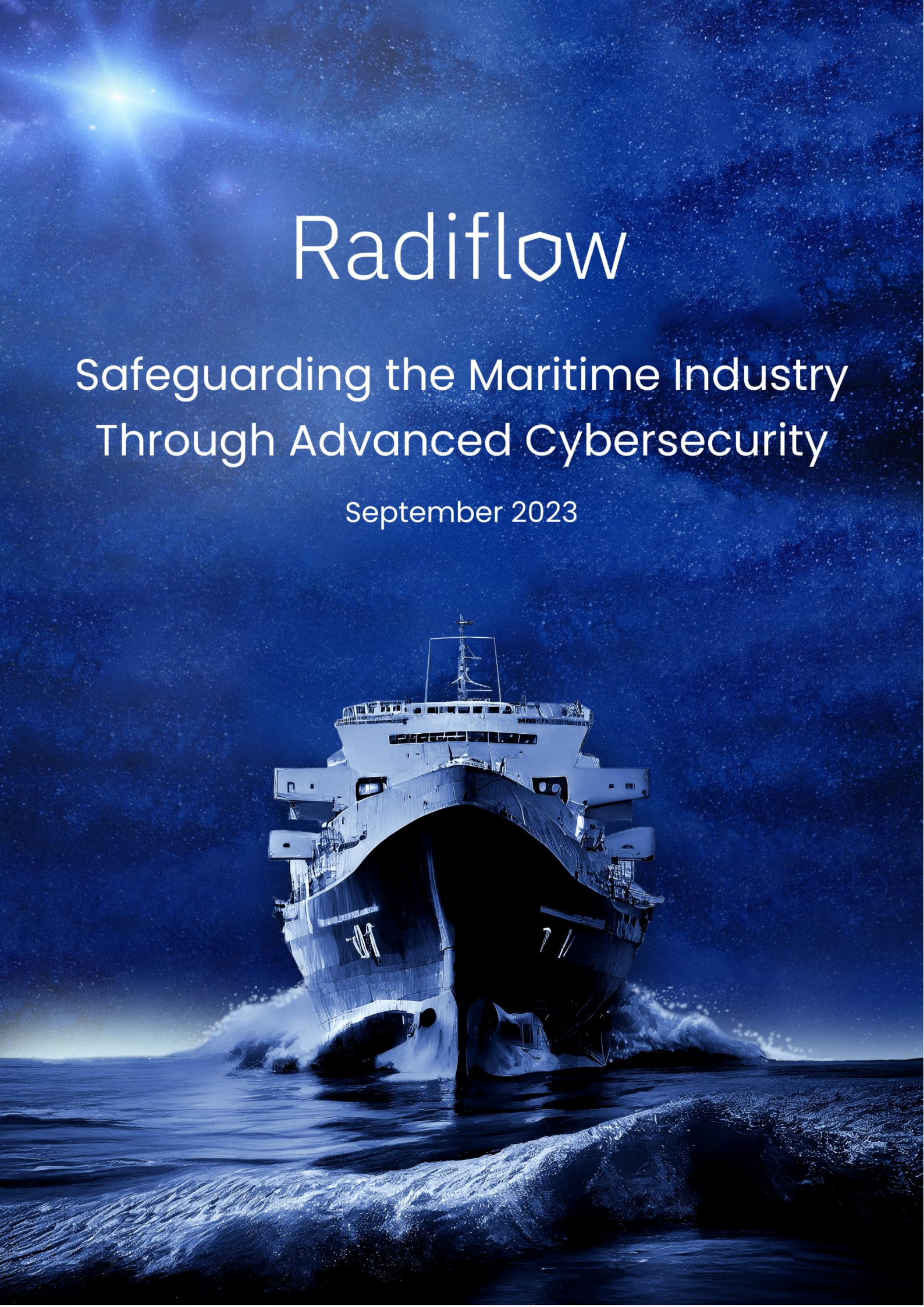
Radiflow

# Safeguarding the Maritime Industry Through Advanced Cybersecurity

September 2023



# Table of Contents

# Introduction

Maritime is one of the largest industries in the world and is responsible for transporting nearly every type of good, from the oil that powers our factories to most of the products we consume like coffee and clothing. Carrying 90% of world trade and with a market size of more than USD 170 billion, maritime is the lifeblood of the global economy.

## Digitized, Converged, and Interconnected

The maritime industry has become increasingly digitized, IT/OT converged, and interconnected, especially as it adopts advanced technologies like Internet of Things (IoT) devices, satellite communications, electronic navigation, and more. While these advancements deliver considerable benefits – safety, efficiency, and convenience – they come at the price of a widening attack surface exposing vulnerabilities that can be exploited by malicious actors. Digitized systems like container management, shipboard controls, navigation, buoys, and even HVAC are in play. In fact, the value of maritime assets is so great and its efficient operation is so critical to countries, global enterprises, and billions of individuals, that cyber criminals and highly trained, state-sponsored cyber syndicates are actively involved.

## Securing Maritime Operations

Since seafaring vessels are part of a larger ecosystem – they participate in fleets and visit a variety of ports –– a successful attack on any single onboard system on a given ship can soon spread to other onboard systems. And the damage doesn't necessarily stop there. Since vessels are in constant communication with their fleet-sisters, today's sophisticated threat actors can leverage their unwanted access to one vessel as a springboard to other vessels, rapidly infecting them as well. From there, port systems and even corporate networks are also within reach.

In this paper, we discuss the cyber risks that maritime operators face and offer practical suggestions for safeguarding their valuable assets and operations.

# Brief History of Maritime Cyberattacks

Maritime cyberattacks are a relatively recent phenomenon, but they have become a rapidly growing concern. Here is an overview of some significant maritime cyberattacks.

2013

## Port of Antwerp

The Port of Antwerp in Belgium fell victim to a cyberattack whereby attackers gained access to the port's systems through a phishing email. While the attack did not cause significant damage, it highlighted the vulnerability of ports and maritime infrastructure to cyber threats.

2015

## Sea Star Line

The Sea Star Line, a shipping company based in the United States, reported a cyberattack that disrupted operations and caused service outages, leading to financial losses.

## South Korea Shipping

South Korean maritime entities, including Hyundai Merchant Marines, the country's largest shipping company, fell victim to cyberattacks that disrupted operations. These attacks revealed the potential impact on global supply chains.

2017

## Maersk

NotPetya, a ransomware attack, targeted numerous global industries, including maritime. It crippled operations of Danish shipping giant, Maersk, for several days, signaling the potential for widespread disruption.

## Port of Barcelona

The Port of Barcelona experienced a cyberattack that disrupted its IT systems. This incident highlighted the potential for cyberattacks to upset port operations, hampering the movement of goods.

2018

## Port of San Diego

This large US port suffered a ransomware attack that led to system outages and disruption of normal operations, underscoring the many vulnerabilities of port systems.

## IMO 2021

2021

The International Maritime Organization (IMO) suffered a cyberattack that impacted its website and internal systems. While the attack didn't directly affect maritime operations, it raised concerns about the potential for cyberattacks to target the very international maritime regulatory bodies that are dealing with cybersecurity.

# Types of Maritime Cyberattacks

Enterprising threat actors are using a wide variety of methods (attack vectors) to gain access to networks, systems, and devices, sometimes to disrupt and other times to take control or to steal information. Here are some examples of maritime cyberattack vectors that Radiflow confronts:

- Phishing Attacks: Attackers may send deceptive emails or messages to ship personnel, port authorities, or shipping company employees to trick them into revealing sensitive information, such as login credentials, or opening malicious attachments.
- Malware and Ransomware: Malicious software can be introduced into a ship's systems through infected files or devices. Ransomware attacks can encrypt critical data, demanding a ransom for its release.
- Network Intrusion: Cybercriminals may attempt to breach the ship's network security through vulnerabilities in communication systems, onboard WiFi, or other networked devices.
- Satellite Communication Interception: Hackers may intercept satellite communication signals to eavesdrop on sensitive information or inject malicious data into the communication stream.
- GPS Spoofing and Jamming: Manipulating Global Positioning System (GPS) signals can cause inaccurate ship navigation, posing a serious safety risk. This can be done through jamming (blocking GPS signals) or spoofing (providing false GPS coordinates).
- Automatic Identification System (AIS) Manipulation: AIS is used for vessel tracking and collision avoidance. Attackers can manipulate AIS data to hide a ship's true identity or to create false collision warnings.
- Electronic Chart Display and Information System (ECDIS) Manipulation: ECDIS is critical for navigation. Attackers may tamper with electronic charts or navigation data, leading to incorrect routes or collision risks.
- Physical Access and Device Tampering: Insiders or malicious actors gaining physical access to a ship's systems can install malware or manipulate hardware components.
- Supply Chain Attacks: Malicious software or hardware can be introduced into a ship's systems through compromised equipment or components during the supply-chain process.
- Remote Access Exploitation: Vulnerabilities in remote access systems, such as those used for ship maintenance or monitoring, can be exploited by attackers to gain control over critical ship functions.

- Man-in-the-Middle Attacks: Attackers may intercept and potentially modify data exchanged between ship systems or between a ship and onshore facilities.
- Denial of Service (DoS) Attacks: These attacks flood a ship's systems or networks with excessive traffic, causing them to become overwhelmed and unresponsive.
- Social Engineering: Attackers may use social engineering techniques to manipulate ship crew or personnel into revealing sensitive information or performing actions that compromise security.
- Insider Threats; Employees or crew member with malicious intent or even accidental actions can pose a significant threat.

# Vulnerable Systems and Facilities

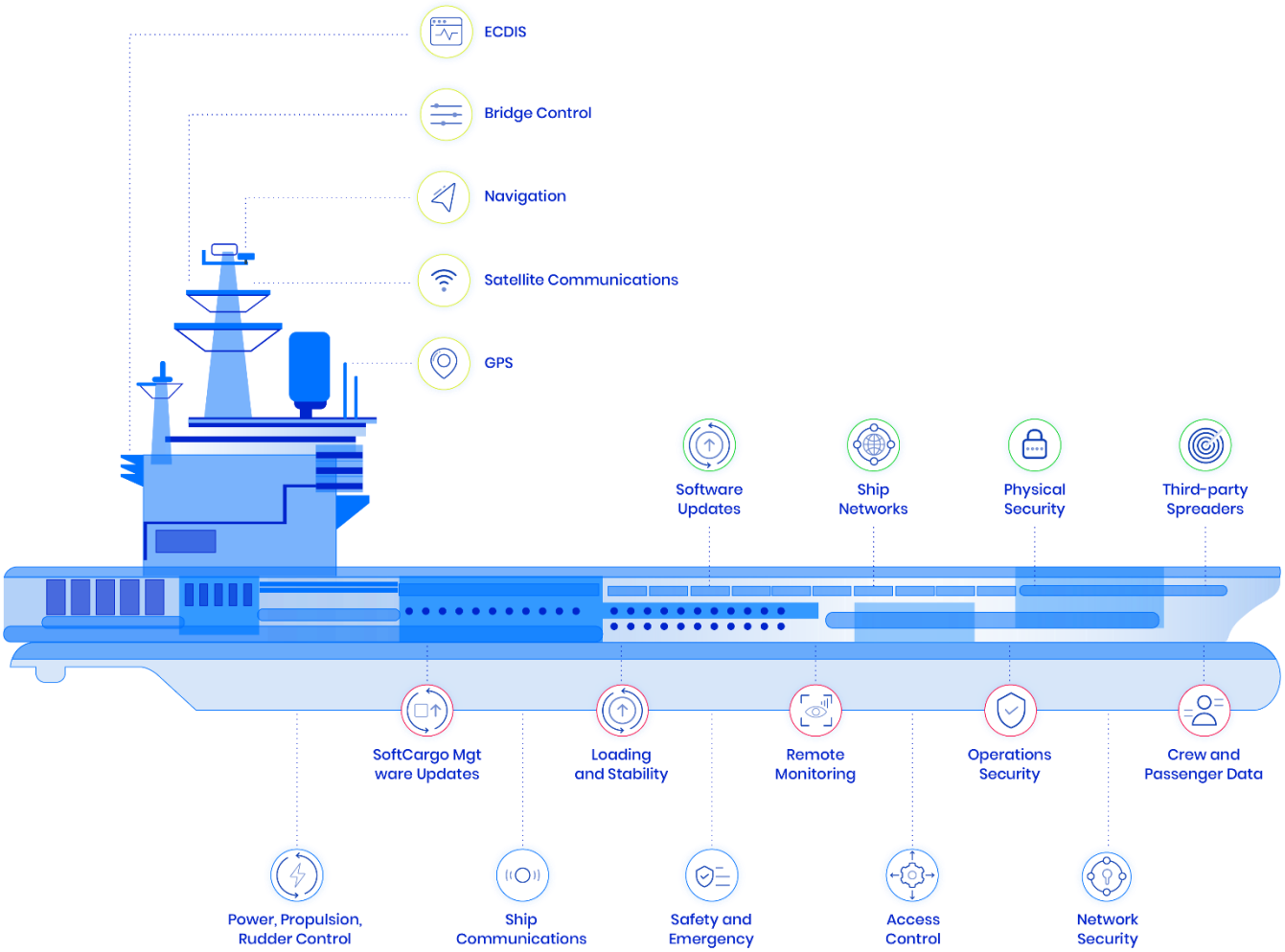
Seafaring vessels carry numerous pieces of digital equipment, systems, networks, and communications facilities. They also produce a great deal of operational and business data. They are in frequent communication with shore facilities. Altogether, these constitute a ship's attack surface. As ships become more digitally connected and integrated, their attack surface expands.

A wide scope of ship systems, assets, and processes could be subject to cyberattack including:

- Bridge Control: Gaining access to bridge control systems could result in access to the automatic identification system (AIS), voyage data recorder (VDR), automatic radar plotting aid (ARPA), and other critical functions.
- Navigation: Disrupting a ship's ability to accurately determine its position, course, and speed via attacks on GPS/GNSS, electronic chart display and information system (ECDIS), radar, or weather systems. could lead to collisions, grounding, or even intentional misdirection of the ship.
- Communications: Ship-to-shore and ship-to-ship communications, such as handheld radios or Voice-Over-IP (VoIP), crucial to safety, coordination, and emergency response, could be disrupted, hampering, or even shutting down, communication between ships or between a ship and land-based authorities.
- Power, Propulsion, and Rudder Control: Targeting engine control, steering, fuel management, generators, and other related systems, an attack could lead to engine failure, loss of power, or even manipulation of propulsion systems, leaving a ship dead in the water or even in an undesired port.
- Cargo Management: Attacks targeting cargo management systems could lead to mismanagement of cargo, unauthorized access to containers, and theft.
- Loading and Stability: Interfering with ballast water management, hull stress, or stability control, necessary for maintaining the ship's stability and preventing the spread of invasive species, could affect a ship's stability and environmental compliance.

- Safety and Emergency: Cyberattacks on systems such as fire and flood control, tracking, CCTV, emergency shutdown, lifeboat, and release mechanisms could jeopardize crew safety during critical situations.
- Electronic Chart Display and Information Systems (ECDIS): Affecting electronic navigational charts that display vital navigation information could compromise the accuracy of navigation data.
- Global Positioning System (GPS): Spoofing or jamming GPS signals could lead to inaccurate positioning and navigation.
- Satellite Communications: As many modern ships depend on satellite communications, a cyberattack could disrupt their communication with onshore operations centers and other ships.
- Crew and Passenger Data: Ships often store personal and sensitive data about crew members and passengers; exfiltration of such data could compromise privacy and run afoul of PII regulations.
- Remote Monitoring: Increasingly, ships are monitored remotely exposing a vulnerability whereby threat actors could exploit this capability to gain unauthorized access and commandeer a ship.
- Access Control: Once they compromise credentials to gain unauthorized access, hackers can gain full administrative privileges, subjecting the entire ship to their whims, including physical security and critical ship systems.
- Operations Security: Ships today set sail with numerous Human-Machine Interfaces (HMIs), logic controllers (PLCs), and digital and analog sensors, as well as other electronics. These are subject to cyber breach, resulting in loss of operations security.
- Network Security: A large ship resembles a typical OT environment, including firewalls and network segmentation devices. Compromises to these can destroy communications between network-connected devices or across systems.
- Software Updates and Vendor Patches: Third-party vendors of computers, IoT devices, and other digital components frequently issue software updates. There are cases where these very security updates contain within them new, exploitable vulnerabilities.

- Ship Networks: Ships host extensive local area networks (LANs) over which email, customs and immigration, personnel, maintenance, spares management, and other IT services flow. Unauthorized access to the LAN can result In data-flow interruption and data exfiltration.
- Physical Security: Server and network infrastructure rooms, access control, the bridge, and other physical locations onboard are protected by digital security mechanisms. These can be breached and physical security compromised.
- Third-Party Spreaders: An attack on a supplier-furnished device, machine, software, or other onboard component, can spread to the on-ship network. In addition, an attack on a satellite provider who provides a communication for a ship can use that channel to gain access to the vessel's network.



# Cybersecurity Challenges

Many of the common cybersecurity challenges that affect the maritime industry mirror those in other industries that deal with OT and IT networks. Radiflow confronts these every day. In our vast experience, we note these major maritime challenges:

- Inability to discover and identify all the onboard systems and devices on a specific ship and across the fleet
- Lack of visibility into each vessel's networks – what it's carrying, from and to which devices and systems, for and by service or system
- No or improper network segmentation to limit incident damage
- No real-time monitoring of traffic flows
- Inadvertently connected IT and OT networks
- Unsecured wireless networks
- Remote access granted to third-parties
- Poor physical security controls
- Lack of threat intelligence – knowing what's coming
- Insufficient cyber awareness on the part of crew, employees, and third parties

# Maritime Regulations

Maritime cybersecurity regulations are still evolving, but several international, regional, and national initiatives are in place or are being developed to address cybersecurity concerns. Some of the notable regulations and guidelines include:

- International Maritime Organization (IMO) Guidelines: The IMO has been working on developing guidelines for maritime cyber risk management. In 2017, the IMO adopted resolution MSC.428(98), which encourages shipping companies and vessel operators to address cybersecurity risks and implement measures to protect their assets.
- International Ship and Port Facility Security (ISPS) Code: The ISPS Code primarily focuses on the security of ships and port facilities against security threats, including cyber threats that could impact maritime operations. While not exclusively focused on cybersecurity, it does provide a framework for addressing security risks in the maritime sector.
- European Union Network and Information Systems (NIS 2) Directive: The EU NIS 2 Directive requires certain critical infrastructure operators, including some in the maritime sector, to implement cybersecurity measures to ensure the security of their networks and information systems. This directive aims to enhance the overall cybersecurity posture across various sectors, including maritime.
- US Coast Guard Maritime Cybersecurity Guidelines: The U.S. Coast Guard has issued guidelines for addressing cybersecurity risks in the maritime sector. These guidelines provide recommendations for identifying, protecting, detecting, responding to, and recovering from cyber incidents.
- NIST Cybersecurity Framework (CSF): While not specific to maritime, the NIST Cybersecurity Framework offers a widely accepted set of guidelines for organizations to manage and reduce cybersecurity risks. Many maritime organizations might use this framework as a reference for building their cybersecurity strategies.
- BIMCO Guidelines: The Baltic and International Maritime Council (BIMCO) has released guidelines to assist shipowners and operators in addressing cybersecurity risks. These guidelines provide practical advice on implementing cybersecurity measures.

- Guidance for Maritime Cyber Security Systems: South Korea released its own guidelines in 2021 covering processes for protecting cyber assets by preventing, detecting, and responding to cyber attacks with a comprehensive system for maintaining a high cybersecurity level.
- Maritime Cybersecurity in the Western Hemisphere: The Organization of American States (OAS) has developed an overview document to assist maritime stakeholders in the Western Hemisphere to understand maritime cyber risk and to lay out initial steps that maritime organizations can take to manage it, while highlighting best practices.
- Various National Regulations: Many countries are developing or have developed their own regulations and guidelines related to maritime cybersecurity. These regulations may vary in scope and applicability.

Given the evolving nature of regulations, it's important to stay updated with the latest developments in maritime cybersecurity standards and regulations. Organizations operating in the maritime industry should closely monitor relevant authorities, industry associations, and international bodies for the most current guidelines.

# A Primer on Preventing Cyberattacks

Preventing maritime cyberattacks requires a combination of cybersecurity measures, best practices, and ongoing vigilance. As the maritime industry becomes increasingly digitized and reliant on technology, the risk of cyberattacks targeting vessels, ports, and maritime infrastructure grows.

Here is a 16-part, comprehensive program to maximize prevention of maritime cyberattacks:

1. Risk Assessment and Management: Conduct a comprehensive risk assessment to identify vulnerabilities, potential threats, and critical assets. Develop a risk management plan to prioritize and address these vulnerabilities. Radiflow *CIARA* is a perfect cyber platform for conducting risk assessments and managing risk over the long haul.
2. Security Policies and Procedures: Establish clear cybersecurity policies and procedures that cover all aspects of maritime operations, including shipboard systems, port operations, and communication networks.
3. Access Control and Authentication: Implement strong access controls and authentication mechanisms for all maritime systems. Use multi-factor authentication (MFA) where possible to enhance security.
4. Regular Training and Awareness: Educate maritime personnel about the risks of cyberattacks and the importance of following cybersecurity best practices. Regular training can help prevent human errors that could lead to exposing vulnerabilities.
5. Network Segmentation: Divide maritime networks into segments based on their functions, and implement strict controls between these segments. This can help contain the spread of attacks and limit their impact.
6. Firewalls: Deploy firewalls to provide protection by shielding the network from malicious or unnecessary network traffic.
7. Threat Detection: Deploy an effective threat detection system to regulate and monitor network traffic for suspicious activities and block unauthorized access or improper operations. Radiflow *iSID* is the leading threat detection system used in thousands of industrial operations to protect them from predators.

8. Patch Management: Keep all software and systems up to date with the latest security patches. This applies to both onboard and onshore systems and infrastructure.
9. Secure Communications: Use encrypted communication protocols to secure data transmission between ships, ports, and other entities. Encrypted communication makes it more difficult for attackers to intercept or manipulate data.
10. Vessel and Port Security: Implement physical security measures to protect vessels and port facilities from unauthorized access, as physical breaches can lead to cyberattacks.
11. Incident Response Plan: Develop a well-defined incident response plan that outlines steps to take in case of a cyberattack. This plan should include communication protocols, roles and responsibilities, and coordination with relevant authorities.
12. Vendor Management: Ensure that third-party vendors and suppliers adhere to cybersecurity standards. Weaknesses in vendor systems could be exploited by attackers to gain access to the network.
13. Regulatory Compliance: Stay up to date with relevant maritime cybersecurity regulations and standards, and ensure that operations align with them.
14. Continuous Monitoring and Testing: Regularly monitor networks, systems, and applications for any signs of unusual activity. Conduct penetration testing and vulnerability assessments to identify weaknesses before attackers can exploit them.
15. Backup and Recovery: Maintain secure and up-to-date backups of critical data and systems, enabling quick recovery in case of a cyberattack or data breach.
16. Collaboration and Information Sharing: Collaborate with other maritime stakeholders, industry organizations, and government agencies to share information about cyber threats and best practices.

Remember that cybersecurity is an ongoing process and the threat landscape is constantly evolving. By adopting these measures, maritime organizations can significantly reduce the risk of cyberattacks and protect the integrity and safety of their operations.

# Radiflow Security Solutions for Maritime

The Radiflow Team comprises cybersecurity professionals who work together with partners and customers to provide the full spectrum of cyber protection for vessels, fleets, off-shore facilities, and ports. Our highly adaptable and flexible solutions and services address the overall and unique cybersecurity challenges of our maritime customers.

## Threat Detection

iSID, Radiflow's advanced threat detection system, delivers full network, communication, and asset visibility, while detecting anomalies and cyber threats. iSIDs can be deployed per vessel, port, or facility.

## Risk Management

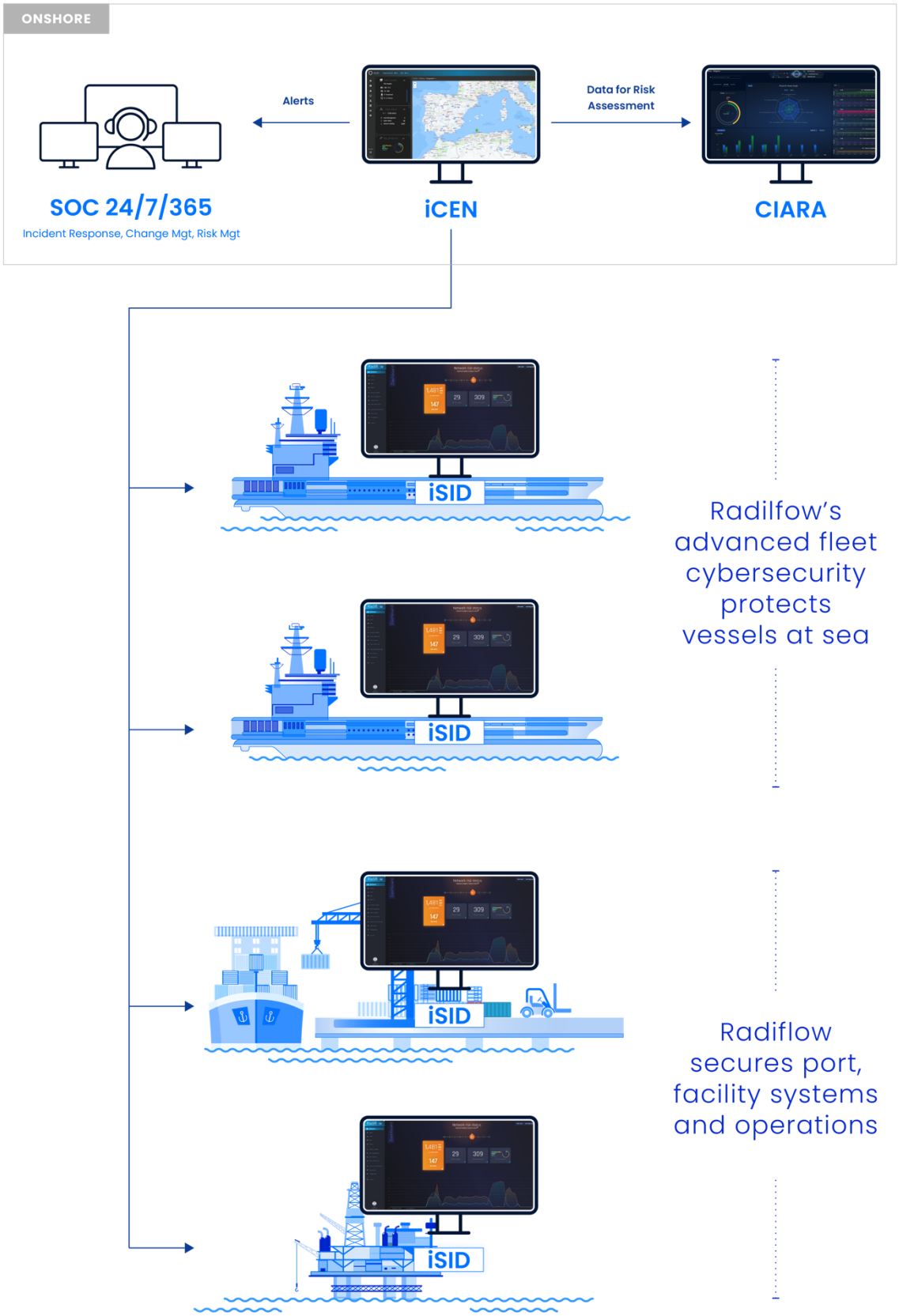
The CIARA Risk Assessment and Management platform analyzes threat intelligence, network traffic, asset properties and more to calculate impacts of cyberattacks on operations. Operating onshore, CIARA ingests countless data points, calculates the risk score, and determines how to prioritize mitigation controls based on their risk-reduction capabilities, compliance requirements, and optimal cybersecurity expenditure.

## Centralized, Onshore Cyber Management

The onshore iCEN Central Management platform centralizes cyber management and monitoring of OT cyber defenses. Communicating with any number of iSIDs via secure, remote connectivity, iCEN collects information from the iSIDs and makes it available to CIARA for accurate risk assessment and to the Security Operations Center for rapid incident response. iCEN enables maritime operators to visualize and manage the state of security across their fleets and operations.

## Outsourcing Cybersecurity

Maritime operators may elect to outsource some or all of their cybersecurity functions. Radiflow works with international Managed Security Service Providers who employ Radiflow solutions to manage cybersecurity from their SOC. These MSSPs monitor vessels, ports, and facilities 24/7/365, providing the full gamut of cyber functions, including threat detection, incident response, risk management, compliance assessments, and more.




Radilfow's advanced fleet cybersecurity protects vessels at sea

Radiflow secures port, facility systems and operations

# About Radiflow

Radiflow is a leading, global provider of OT security solutions and services for critical infrastructure and industrial automation. We enable operators to continuously safeguard their operations while they manage risk, optimize their security budget, and comply with regulations and industry best practices.

Radiflow OT security solutions and services are deployed at more than 8000 sites worldwide, supported from offices and partners in Europe, APAC, and North America.

Radiflow is part of the Sabanci Group, an international conglomerate involved in financial services, energy, cement, retail, and other critical infrastructure and industrial sectors.

Visit us at www.radiflow.com