Cybersecurity Guidelines for Shipowners

Cybersecurity Elements in Ship Safety Management: Guidelines for Implementing Cyber-Secure Procedures

PRS
1936

Introduction

As of January 1st, 2021, new IMO requirements outlined in resolution MSC.428(98) mandate the verification of cybersecurity implementation both ashore in shipowner's offices and aboard ships. These requirements entail ensuring proper implementation of procedures, conducting cyber risk analyses, and employing various mitigation measures against cyber threats and user vulnerabilities. To facilitate shipowners in adhering to these cybersecurity measures and to assist ISM auditors in evaluating the adequacy of cybersecurity within safety management systems, the MMS Bureau has prepared the following guidelines and preparatory materials.

The guidelines aim to provide a comprehensive overview of the actions shipowners must have introduced, effective from January 1st, 2021.

Step 1 – Determination of Information Value

Initially, the company should initiate a risk analysis by identifying critical information and assessing its value. Any information susceptible to compromise can hold significant value for hackers seeking financial gain, such as through blackmail or data theft for resale. Therefore, procedures should emphasize proper and frequent employee training to mitigate social engineering attacks.

Additionally, the company should identify the types of data it handles. Key questions to consider in this identification process include:

- Are there financial or legal ramifications associated with exposing or losing this information?
- How valuable is this information to competitors?
- Is it feasible to recreate this information from scratch, and what would be the associated time and cost implications?
- Would losing this information impact revenue or profitability?
- Would the loss of this data disrupt day-to-day business operations, and could staff function without it?
- What would be the reputational damage if this data were leaked?

These considerations are crucial for determining the level of protection and security measures required for safeguarding critical information assets.

Step 2 – Identification and Prioritization of Assets

After conducting the initial risk analysis, the company must identify assets for evaluation to determine the assessment scope. This process enables the prioritization of assets requiring assessment. It's important to note that not all buildings, employees, electronic data, trade secrets, vehicles, or office equipment necessitate assessment. For each asset, the following information should be considered:

- Software
- Hardware
- Data
- Interface
- End-users
- Support personnel
- Purpose
- Criticality
- Functional requirements
- IT security policies and architecture
- Network topology
- Information storage protection
- Information flow
- Technical security controls
- Physical security controls
- Environmental security

This comprehensive assessment of assets enables the company to prioritize resources and efforts effectively, focusing on areas with the greatest importance and vulnerability to cyber threats.

Step 3 – Identification of Threats

Threats encompass various vulnerabilities that could be exploited to breach security or cause harm, including data theft, system disruption, or unauthorized access. Beyond traditional cyber threats like hackers and malware, organizations must also consider other potential risks:

- **Natural disasters:** Events such as floods, hurricanes, earthquakes, lightning, and fire pose significant risks to data and infrastructure. Organizations should assess the likelihood of such events and plan accordingly, whether using on-premise or cloud-based servers.
- **System failure:** Critical systems should be supported by high-quality equipment with reliable technical support to mitigate the risk of system failures.

- **Human error:** Proper education and training around malware, phishing, and social engineering are essential to prevent accidental breaches caused by employees. Implementing strong IT security controls, including regular data backups and password management, can reduce the risk of human error.
- **Adversarial threats:** These include threats from third-party vendors, insiders, privileged users, hacker groups, corporate espionage, and nation-states.

Common threats affecting organizations include:

- **Unauthorized access:** Unauthorized access by attackers, malware, or employee error.
- **Misuse of information by authorized users:** Typically an insider threat where data is altered, deleted, or used without approval.
- **Data leaks:** Leakage of personally identifiable information (PII) and other sensitive data, either by attackers or due to poor configuration of cloud services.
- **Loss of data:** Organization experiences loss or accidental deletion of data as a result of poor backup or replication practices.
- **Service disruption:** Loss of revenue or reputational damage caused by downtime.

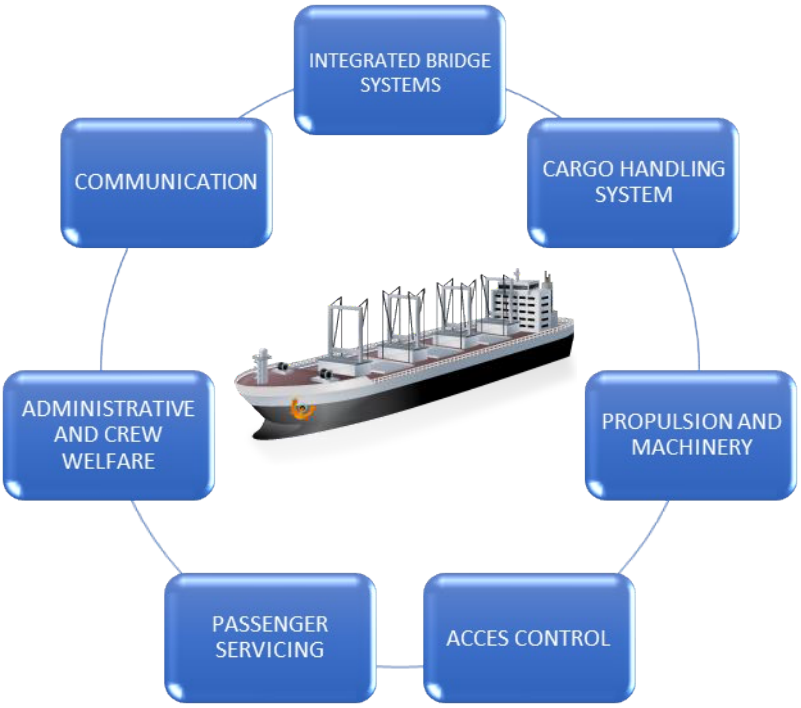
These threats can be executed through various techniques such as:

- **Phishing:** Deceiving recipients into sharing sensitive information.
- **Botnets:** Internet-connected devices, such as PCs, servers, mobile devices, or any virtual devices controlled by common malware.
- **Bugs:** Errors, faults, or flaws in computer programs or hardware systems.
- **Insider attack:** Malicious attacks perpetrated on a network or computer by a person with authorized system access.
- **Jamming:** Transmission of radio signals to disrupt communication by decreasing the signal-to-noise ratio, resulting in unreliable links, increased energy consumption, extended packet delays, and disruption of end-to-end routes.
- **Ransomware:** Malware that infects, locks, or takes control of a system, demanding ransom to undo the changes.
- **Spoofing:** Fraudulent or malicious practice in which communication is sent from an unknown source disguised as a known source to the receiver.
- **Spyware:** Software that infiltrates and secretly monitors unsuspecting users, enabling hackers to obtain sensitive information such as passwords. Spyware is usually attached to free online software downloads or clicked links by users.

After identifying threats, it's crucial to assess their potential impact to prioritize risk management efforts effectively.

Step 4 – Identification of Vulnerabilities

In today's maritime industry, ships rely heavily on information and communication technology (ICT) systems, which not only facilitate crew operations but also enhance efficiency and comfort onboard. However, certain ship systems may be particularly susceptible to cyber-attacks.



A vulnerability refers to any weakness within a system that a threat can exploit to compromise security, cause harm, or gain unauthorized access to sensitive data. Vulnerabilities are typically identified through rigorous risk analysis, audit reports, databases like the National Institute for Standards and Technology (NIST) vulnerability database, vendor data, incident response teams, and software security analysis. Identifying and addressing vulnerabilities is essential to safeguarding ship systems from potential cyber threats.

The vulnerability of organizational software can be mitigated through effective patch management, which involves automatic forced updates to address any known weaknesses. Additionally, physical vulnerabilities can be minimized by implementing keycard access systems to restrict unauthorized entry into computing facilities.

When conducting a Cybersecurity Risk Analysis, it's crucial to consider potential attacks on critical ship systems. Some of the most common vulnerabilities and associated attacks include:

1. GPS Signal Jamming
2. GPS Device Failure or Poor Quality Transmission

3. AIS Device Powered Down
4. AIS Device Malfunction
5. AIS Programming Error
6. AIS Radio Signal Jamming
7. AIS Radio Transmission Error
8. AIS Vessel Spoofing (Message Injection, Deletion, Modification)
9. AIS Traffic Eavesdropping
10. AIS Information Modification (Position, Course, Cargo, Flagged Country, Speed, Name, MMSI)
11. AIS System Flooding
12. Ghost Vessel (Manipulation of AIS Data to Falsify Vessel Location)
13. CPA/AIS-SART Spoofing
14. Vessel Disappearance
15. Aids-to-Navigation Spoofing (Altering Buoy/Lighthouse Data to Mislead Navigation)
16. Data Diddling
17. Weather Forecast Spoofing
18. Modifying Engine Properties (Compromising Engine Systems)
19. Compromising ECDIS (Unauthorized Access, File Manipulation, Insertion of USB Key)
20. Addressing these vulnerabilities and implementing appropriate safeguards is essential to protect ship systems from potential cyber threats.

Step 5 – Evaluation of Existing Controls and Implementation of New Measures

An assessment of the controls currently in place to mitigate or eliminate the likelihood of a threat or vulnerability is essential. Controls can take various forms, including technical solutions such as hardware or software, encryption protocols, intrusion detection systems, two-factor authentication, automatic update mechanisms, and continuous data monitoring. Non-technical measures such as security policies and physical barriers like locks or keycard access also play a crucial role.

These controls can be categorized as preventive or detective measures. Preventive controls aim to thwart attacks before they occur, such as encryption protocols, antivirus software, or continuous security monitoring. Detective controls are designed to identify and respond to attacks after they have happened, such as continuous data leak detection.

It is imperative that the organization's leadership recognizes the severity of cybersecurity threats and acknowledges that conducting a comprehensive risk analysis is essential for mitigating these risks effectively. This top-down commitment sets the tone for the entire organization and ensures that cybersecurity measures are prioritized and implemented effectively.

Step 6 – Estimation of Likelihood and Impact of Scenarios on an Annual Basis

This step involves evaluating the financial costs associated with potential data loss or operational interruptions for the company, as well as assessing the likelihood of such incidents occurring. These assessments should be reflected in the company's annual budget to ensure appropriate allocation of resources and mitigation strategies.

Step 7 – Prioritization of Risks Based on Prevention Costs vs. Information Value

Senior management or designated individuals should utilize the determined risk levels as a foundation for devising risk mitigation strategies. Here are some general guidelines:

- **High Risk:** Immediate development of corrective measures is essential.
- **Medium Risk:** Corrective measures should be developed within a reasonable timeframe.
- **Low Risk:** Decide whether to accept the risk or pursue mitigation.

Once the value of the asset and the allocated budget for protection have been established, the next step is to assess whether the cost of protection outweighs the asset's value. If the cost exceeds the value, alternative approaches may be warranted. However, it's crucial to consider potential reputational impacts in addition to financial considerations.

Other factors to consider include:

- Organizational policies
- Reputational damage
- Feasibility
- Regulations
- Effectiveness of controls
- Safety
- Reliability
- Organizational attitude towards risk
- Tolerance for uncertainty regarding risk factors
- Organizational weighting of risk factors

Step-by-Step Instruction for Cybersecurity Threat and Vulnerability Assessment

Identify Assets: Begin by identifying the assets within your organization that may be vulnerable to cybersecurity threats. This includes hardware, software, data, interfaces, end-users, support personnel, and more.

Determine Information Value: Evaluate the criticality and value of the information associated with

each asset. Consider factors such as financial penalties, competitiveness, data recreation feasibility, revenue impact, operational dependency, and reputational damage.
Identify Threats: Identify potential threats to your organization's assets. These threats may include natural disasters, system failures, human error, adversarial threats, unauthorized access, misuse of information, data leaks, and service disruptions.

Assess Vulnerabilities: Determine weaknesses or vulnerabilities within your organization's systems that could be exploited by threats. This may involve analyzing risk reports, audit findings, vulnerability databases, incident response data, and software security assessments.

Prioritize Risks: Evaluate the likelihood and impact of various threats and vulnerabilities on a per-year basis using numeric rating scales. Prioritize risks based on the costs of prevention versus the value of the information at risk.

Implement Controls: Develop and implement controls to mitigate identified risks. These controls may include technical measures (e.g., encryption, intrusion detection), nontechnical measures (e.g., security policies, physical access controls), preventative controls, and detective controls.

Calculate Likelihood and Impact: Calculate the likelihood and impact of potential cybersecurity incidents on an annual basis. Consider the financial costs, operational disruptions, reputational damage, and other relevant factors.

Prioritize Risks: Prioritize risks based on their severity, likelihood, and potential impact. Focus on addressing high-risk vulnerabilities first, followed by medium and low-risk vulnerabilities.

Develop Remediation Plans: Develop remediation plans to address identified vulnerabilities and mitigate potential cybersecurity risks. Assign responsibilities, establish timelines, and allocate resources as needed.

Monitor and Review: Continuously monitor and review the effectiveness of implemented controls and remediation efforts. Stay vigilant for emerging threats and vulnerabilities, and adjust cybersecurity strategies accordingly. Regularly update risk assessments and threat profiles to ensure ongoing protection against cyber threats.

	Impact scale		Likelihood scale
1	Impact is negligible	0	Unlikely to occur
2	Effect is minor, major operations are not affected	1	Likely to occur less than once per year
3	Organization operations are unavailable for a certain amount of time, costs are incurred or organization's confidence is minimally affected	2	Likely to occur once per year
4	Significant loss of operations, significant impact on organization's confidence	3	Likely to occur once per month
5	Effect is disastrous, systems are down for extended period of time. Systems need to be rebuilt and data replaced	4	Likely to occur once per week
6	Effect is catastrophic, critical systems are offline for an extended period of time. Data has been lost or irreparably corrupted. Safety of people or environment is affected.	5	Likely to occur every day

When assessing impact, it's crucial to consider the value of the resources at risk, taking into account both their inherent (replacement) value and their importance (criticality) to the organization's successful operation.
Likelihood is influenced by factors such as threat capability, the frequency of threat occurrence, and the effectiveness of current countermeasures (security controls). Human threats pose a significant risk to an organization's ability to operate effectively.

Human threat sources include:

- **Insiders:** Employees, owners, stockholders, etc.
- **General contractors and subcontractors:** Cleaning crews, developers, technical support personnel, computer and telephone service repair crews.
- **Former employees:** Those who retired, resigned, or were otherwise terminated.
- **Unauthorized users:** Computer criminals, terrorists, intruders (like hackers or crackers) who attempt to access the organization's resources for any reason.

Human threats			Impact (1-6)	Probability (0-5)	Score (Impact x Probability)
1	**Human error**				
		Accidental destruction, modification, disclosure or incorrect classification of information			
		Ignorance, inadequate security awareness, lack of security guidelines, lack of proper documentation, lack of knowledge			
		Workload – too many or too few system administrators, too much workload on users			
		Users may inadvertently give information on security weaknesses to attackers			
		Incorrect system configuration			
		Security policy not adequate			
		Security policy not enforced			
		Security analysis may have omitted something important or be wrong			
2	**Dishonesty, fraud, theft, embezzlement, selling of confidential organization's information**				
3	**Attacks by social engineering**				
		Attackers may use telephone to impersonate employees to persuade users/administrators to give user name, password or any other sensitive information, such us employee ID number, initials, room number, etc.			
		Attackers may deceive or persuade users to execute trojan horse programs			
4	**Abuse of privileges or trust**				
General threats			**Impact** (1-6)	**Probability** (0-5)	**Score** (Impact x Probability)
1	**Unauthorized use of not protected computers/laptops/smartphones**				
2	**Mixing of test and production data or environments**				

3	Introduction of unauthorized software or hardware				
4	Time bombs – software programmed to damage the system on a certain date or time				
5	Operating system design errors – systems not designed to be highly secure				
6	Protocol design errors – protocol weaknesses in TCP/IP can result in:				
		Source routing, DNS spoofing, TCP sequence guessing, unauthorized access			
		Hijacked sessions and authentication session/transaction replay, data is changed or copied during transmission			
		Denial of service (due to bombing, flooding or large packet pinging the servers, etc.)			
7	Logic bomb – software programmed to damage a system under certain conditions				
8	Viruses in programs, documents, e-mail attachments				
Identification authorization threats			**Impact** (1-6)	**Probability** (0-5)	**Score** (Impact x Probability)
1	Attack programs masquerading as normal programs (trojan horses)				
2	Attack hardware masquerading as normal commercial hardware				
3	External attackers masquerading as valid users or customers				
4	Attackers masquerading as helpdesk or support personnel				

Privacy threats			Impact (1-6)	Probability (0-5)	Score (Impact x Probability)
1	**Eavesdropping**				
		Electromagnetic eavesdropping or Van Eck phreaking			
		Telephone/fax eavesdropping (via "clip- on" telephone bugs, inductive sensors, or hacking the public telephone exchanges)			
		Network eavesdropping. Unauthorized monitoring of sensitive data crossing the internal network, unknown to the data owner			
		Subversion of ONS to redirect email or other traffic			
		Subversion of routing protocols to redirect email or other traffic			
		Radio signal eavesdropping			
		Rubbish eavesdropping (analyzing waste for confidential documents, etc.)			
Integrity/accuracy threats			**Impact** (1-6)	**Probability** (0-5)	**Score** (Impact x Probability)
1	**Malicious, deliberate damage of information or information processing functions from external sources**				
2	**Malicious, deliberate damage of information or information processing functions from internal sources**				
3	**Deliberate modification of information**				

Access control threats		Impact (1-6)	Probability (0-5)	Score (Impact x Probability)
1	Password cracking (access to password files, use of bad-blank, default, rarely changed passwords, etc.)			
2	External access to password files, network sniffing			
3	Attack programs allowing external access to systems (backdoors visible to external networks)			
4	Attack programs allowing internal access to systems (backdoors visible to internal networks)			
5	Unsecured maintenance modes, developer backdoors			
6	Modems easily connected, allowing uncontrollable			
7	Bugs in network software, which can open unknown or unexpected security holes, that can be further exploited from external networks to gain access. (This threat becomes bigger and bigger with more complexity of the software)			
8	Unauthorized physical access to system			
Repudiation threats		**Impact** (1-6)	**Probability** (0-5)	**Score** (Impact x Probability)
1	Receivers of confidential information may refuse to acknowledge receipt			
2	Senders of confidential information may refuse to acknowledge source			
Legal threats		**Impact** (1-6)	**Probability** (0-5)	**Score** (Impact x Probability)
1	Failure to comply with regulatory or legal requirements (e.g. to protect confidentiality of employee data)			

2	Liability for acts of internal users or attackers who abuse the system to perpetrate unlawful acts (e.g. incitement to racism, gambling, money laundering, distribution of pornographic or violent material, etc.)			
3	Liability for damages if an internal users attacks other sites			
Service reliability threats		Impact (1-6)	Probability (0-5)	Score (Impact x Probability)
1	Major natural disasters (fire, smoke, water, earthquake, storm or hurricane, power outage, etc.)			
2	Minor natural disasters of short duration, or causing little damage			
3	Major human-caused disasters (war, terrorist incident, bomb, civil disturbance, dangerous chemicals, radiological or biological accidents)			
4	Equipment failure from defective hardware, cabling or communication system			
5	Equipment failure from airborne electricity			
6	Denial of Service			
	Network abuse – misuse of routing protocols to confuse and mislead systems			
	Server overloading (by processes, swap space, memory, temporary directories, overloading services, etc.)			
	Email bombing			
	Downloading or receipt of malicious applets, active x controls, macros, postscript files, etc.			
7	Sabotage – malicious, deliberate damage of information or information processing functions			
	Physical destruction of network interface devices or cables			

		Physical destruction of computing devices or media			
		Destruction of electronic devices and media by electromagnetic radiation weapons (EMP/T gun, HERF gun)			
		Deliberate electrical overloads or shutting off electrical power			
		Viruses or worms			
		Deletion of critical system files			

After conducting a thorough review of current security controls and assessing potential threats and vulnerabilities, it's essential to determine a series of actions to mitigate risk to an acceptable level. These actions may involve implementing missing security controls or enhancing the strength of existing ones.
Security controls should aim to reduce or eliminate vulnerabilities while aligning with the needs of the business. It's important to strike a balance between cost and expected security benefits and risk reduction. Typically, remediation efforts will prioritize addressing high-risk threats and vulnerabilities.
Below are examples of remediation activities focusing on commonly identified high-risk threats and vulnerabilities.

	Remediation action	Cost	Benefit	Risk
1	**Develop a foundation of Security Policies, Practices and Procedures, especially in the area of Change Control**	*Low*	*High*	*High*
2	**Establish and enforce a globally-accepted password policy**	*Low*	*High*	*High*
3	**Address vulnerability results in order of high risk to low risk**	*Low*	*High*	*High*
4	**Establish an Operations group facilitated discussion to improve processes and communications, and to eliminate any misunderstandings**	*Low*	*High*	*High*
5	**Establish router configuration security standards, forming baseline practices**	*Low*	*High*	*High*
6	**Harden servers on the internal network**	*Low*	*High*	*High*
7	**More closely integrate worker termination activities between HR and IT. Incorporate new-hire orientation and annual security "refresher" for all employees.**	*Low to moderate*	*High*	*High*

8	**Redesign the internet perimeter, incorporating concepts of N-tier architecture and "defense in depth" into the redesign of the Internet perimeter and Enterprise Architecture**	*Low to moderate*	*High*	*High*
9	**Migrate to a more centralized and integrated model of operations management, including centralized logging, event correlation, and alerting**	*Low to moderate*	*High*	*High*
10	**Complete the intrusion detection infrastructure**	*Moderate*	*High*	*High*
11	**Install encryption on mobile computers to protect the confidentiality and integrity of data.**	*Moderate to expensive*	*High*	*High*
12	**Perform data classification to determine security levels to protect that data**	*Moderate to expensive*	*High*	*High*
13	**Institute vulnerability scanning as a regular scheduled maintenance task**	*Moderate to expensive*	*High*	*High*
14	**Reclassify email as a mission critical application**	*Low*	*Moderate*	*Medium*
15	**Complete security staffing for the ISO Security Group**	*Expensive*	*High*	*High*
16	**Complete Computer Security Incident Response Team (CSIRT) capability**	*Moderate to expensive*	*High*	*High*

These actions are ranked in priority order based on their effectiveness:

- Implementing multi-factor authentication for all user accounts.
- Conducting regular security awareness training for all employees to mitigate the risk of human error.
- Installing intrusion detection and prevention systems to monitor network traffic and detect suspicious activity.
- Implementing encryption protocols for sensitive data both in transit and at rest.
- Conducting regular vulnerability scans and penetration tests to identify and address weaknesses in systems and networks.
- Establishing incident response procedures to effectively respond to and mitigate security incidents.
- Enforcing least privilege access controls to limit user access to only the resources necessary for their role.
- Implementing robust patch management procedures to ensure timely application of security updates and patches.
- Conducting regular audits of security controls and procedures to ensure compliance and effectiveness.

- Developing and maintaining a comprehensive disaster recovery and business continuity plan to minimize the impact of security incidents or disasters.

What will be checked/verified during the external audits?

During external audits focusing on cybersecurity, the following procedures should be checked and verified as a minimum:

1. **Designation of Responsible Personnel:**
   Identification of person(s) responsible for investigating and mitigating cybersecurity incidents.
2. **Data Identification:**
   Identification of sensitive and non-sensitive data within the organization's systems.
3. **Backup Procedures:**
   Process for creating retrievable backups of vital data to ensure data integrity and availability in case of incidents.
4. **Physical Access Control:**
   Measures for controlling physical access to facilities, rooms, and computers to prevent unauthorized entry.
5. **Personnel Training:**
   Training programs for personnel to recognize and mitigate human-based attacks, such as social engineering, and to ensure password security and computer protection.
6. **External Device Management:**
   Implementation of physical prevention measures or special precautions for the use of external data storage devices, such as USB flash drives, to prevent unauthorized data transfer or malware infection.
7. **Incident Reporting and Response:**

   Procedures for reporting and responding to cybersecurity incidents, including proper follow-up actions to address vulnerabilities and prevent future incidents.
8. **Connection Windows Management:**

   Consideration of time windows for online connections between the ship and shore terminals to minimize exposure to potential cyber threats (if applicable at all).
9. **Procedure Revisions and Improvement Plans:**

   Program for regular review and revision of cybersecurity procedures and continuous improvement plans to adapt to evolving threats and technologies.
10. **Security System Testing and Drills:**

    Regular testing and drills of security systems and procedures to ensure their effectiveness and readiness to respond to cybersecurity threats.

These checks and verifications aim to ensure that the organization has robust cybersecurity measures in place to protect sensitive data, prevent unauthorized access, and effectively respond to incidents to maintain operational resilience.

Additional sources for Cyber Security (PRS is not responsible for external content)

IACS – the International Association of Classification Societies Recommendations (Rec) and United Requirements (URs)

Rec 166 – Recommendation on Cyber Resilience – New Corr.2 Apr 2022 Clean.
UR E26 Cyber resilience of ships – Rev.1 Nov 2023 – Complete Revision.
UR E27 Cyber resilience of on-board systems and equipment – Rev.1 Sep 2023 Clean

IMO guidance

IMO has issued MSC-FAL.1-Circ.3-Rev.2 Guidelines on maritime cyber risk management.
The guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities and include functional elements that support effective cyber risk management. The recommendations can be incorporated into existing risk management processes and are complementary to the safety and security management practices already established by IMO.

The Maritime Safety Committee, at its 98th session in June 2017, also adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems. The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

Other guidance and standards

Cyber Security Guidelines on board Ships issued by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss.

IAPH Port Community Cyber Security Report.

Thank you
and
stay cyber safe!

For any inquiries, please reach out to PRS Marine Management Systems Bureau e-mail: kz@prs.pl

PRS
1936