SUBJECT: GUIDANCE FOR MARITIME CYBER SECURITY SYSTEM

The International Maritime Organization (IMO) adopted "MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS" by RESOLUTION MSC.428 (98) and “GUIDELINES ON MARITIME CYBER RISK MANAGEMENT” by MSC-FAL.1/Circ.3.

Compliance

The adopted resolution encourages administrations to ensure that cyber risks are appropriately addressed in safety management systems (SMS) no later than the first annual DOC audit after 1 January 2021.

Introduction

Maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised. Cyber risk management means the process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders. The goal of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyber risks.

Stakeholders should take 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.

Threats are presented by malicious actions (e.g. hacking or introduction of malware) or the unintended consequences of benign actions (e.g. software maintenance or user permissions). In general, these actions expose vulnerabilities (e.g. outdated software or ineffective firewalls) or exploit a vulnerability in operational or information technology. Effective cyber risk management should consider both kinds of threat.

Cyber security and safety management

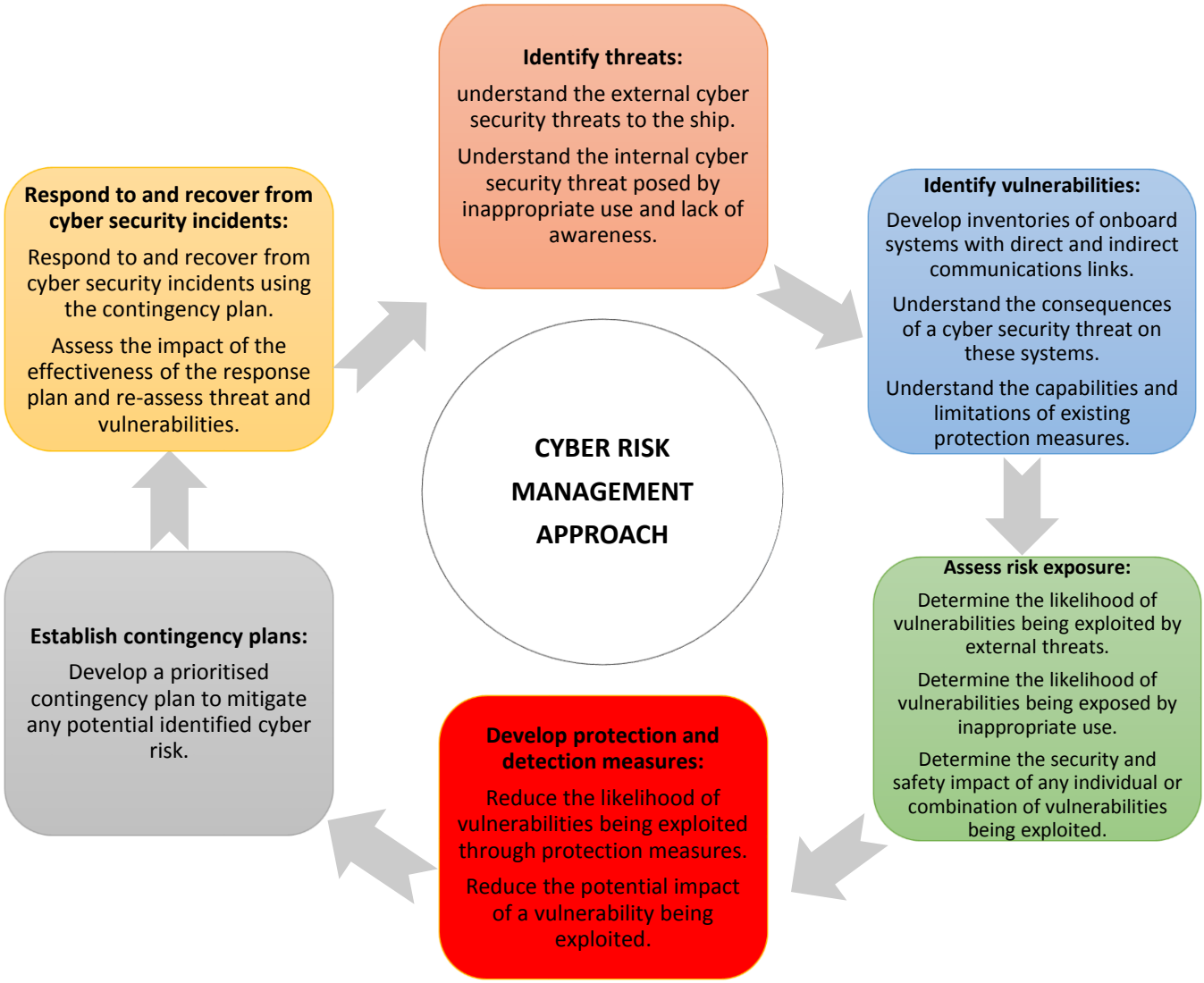
Cyber security is concerned with the protection of IT, OT, information and data from unauthorized access, manipulation and disruption. Cyber safety covers the risks from the loss of availability or integrity of safety critical data and OT. Cyber safety incidents can arise as the result of:

- A cyber security incident, which affects the availability and integrity of OT.
- A failure occurring during software maintenance and patching.
- Loss of or manipulation of external sensor data, critical for the operation of a ship.

Cyber risk management should:

- Identify the roles and responsibilities of users, key personnel, and management both ashore and on board.
- Identify the systems, assets, data and capabilities, which if disrupted, could pose risks to the ship's operations and safety.
- Implement technical and procedural measures to protect against a cyber-incident and ensure continuity of operations.
- Implement activities to prepare for and respond to cyber incidents.

Cyber risk management approach as set out in the guidelines is according to below:



1. Identify threats

When assessing the risk, companies should consider any specific aspects of their operations that might increase their vulnerability to cyber incidents. In general, there are two categories of cyber-attacks, which may affect companies and ships:

- Untargeted attacks, where a company or a ship's systems and data are one of many potential targets. Examples of some tools and techniques that may be used in these circumstances include:
    - Malware – Malicious software which is designed to access or damage a computer without the knowledge of the owner including Trojans, ransomware, spyware, viruses, and worms.
    - Phishing – Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information.
    - Water holing – Establishing a fake website or compromising a genuine website to exploit visitors.
    - Scanning – Attacking large portions of the internet at random.
- Targeted attacks, where a company or a ship's systems and data are the intended target include:
    - Social engineering – A non-technical technique used by potential cyber attackers to manipulate insider individuals into breaking security procedures, normally, but not exclusively, through interaction via social media.
    - Brute force – An attack trying many passwords with the hope of eventually guessing correctly.
    - Denial of service (DoS) – Prevents legitimate and authorized users from accessing information, usually by flooding a network with data.
    - Spear-phishing – Like phishing but the individuals are targeted with personal emails, often containing malicious software or links.
    - Subverting the supply chain – Attacking a company or ship by compromising equipment, software or supporting services being delivered to the company or ship.

2. Identify vulnerabilities

Care should be taken to understand how critical shipboard systems might be connected to uncontrolled networks. When doing so, the human element should be taken into consideration, as many incidents are initiated by personnel's actions. Vulnerable systems could include, but are not limited to:

- Bridge systems- A cyber incident can extend to service denial or manipulation and, therefore, may affect all systems associated with navigation, including ECDIS, GNSS, AIS, VDR and Radar/ARPA.
- Cargo handling and management systems- Digital systems used for the loading, management and control of cargo, including hazardous cargo, may interface with a variety of systems ashore, including ports, marine terminals.

- Propulsion and machinery management and power control systems- The vulnerability of these systems can increase when used in conjunction with remote condition-based monitoring and/or are integrated with navigation and communications equipment on ships using integrated bridge systems.
- Access control systems- Digital systems used to support access control to ensure physical security and safety of a ship and its cargo, including surveillance, shipboard security alarm, and electronic "personnel-on-board" systems are vulnerable to cyber-attacks.
- Passenger servicing and management systems- Digital systems used for property management, boarding and access control may hold valuable passenger related data. Intelligent devices (tablets, handheld scanners etc.) are themselves an attack vector as ultimately the collected data is passed on to other systems.
- Passenger facing public networks- Fixed or wireless networks connected to the internet, installed on board for the benefit of passengers, for example guest entertainment systems.
- Administrative and crew welfare systems- Onboard computer networks used for administration of the ship or the welfare of the crew are particularly vulnerable when providing internet access and email.
- Communication systems- Availability of internet connectivity via satellite and/or other wireless communication can increase the vulnerability of ships. The cyber defence mechanisms implemented by the service provider should be carefully considered but should not be solely relied upon to secure every shipboard system and data.

The following are common cyber vulnerabilities, which may be found onboard existing ships, and on some new build ships:

- Obsolete and unsupported operating systems
- Outdated or missing antivirus software and protection from malware
- Inadequate security configurations and best practices, including ineffective network management and the use of default administrator accounts and passwords.
- Shipboard computer networks, which lack boundary protection measures and segmentation of networks.
- Safety critical equipment or systems always connected with the shore side
- Inadequate access controls for third parties including contractors and service providers.

3. Assess risk exposure

the company should delegate authority and allocate the budget needed to carry out a full risk assessment and develop solutions that are best suited for the company and the operation of their ships. The following should be addressed:

- Identify systems that are important to operation, safety and environmental protection
- Assign the persons responsible for setting cyber policies, procedures and enforce monitoring
- Determine where secure remote access should use multiple defence layers and where protection of networks should be disconnected from the internet
- Identification of needs for training of personnel.

The level of cyber risk will reflect the circumstances of the company, ship (its operation and trade), the IT and OT systems used, and the information and/or data stored. The maritime industry possesses a range of characteristics, which affect its vulnerability to cyber incidents:

- the cyber controls already implemented by the company onboard its ships
- multiple stakeholders are often involved in the operation and chartering of a ship potentially resulting in lack of accountability for the IT infrastructure
- the ship being online and how it interfaces with other parts of the global supply chain
- ship equipment being remotely monitored, e.g. by the producers
- business-critical, data sensitive and commercially sensitive information shared with shore-based service providers, including marine terminals and stevedores and also, where applicable, public authorities
- the availability and use of computer-controlled critical systems for the ship's safety and for environmental protection.

Potential impacts could be safety-related, operational, environmental-related, financial, reputational and compliance-related. Several assessment methodologies offer criteria and techniques that can help define the magnitude of the impact from a cyber-attack.

Potential impact	Definition	In practice
Low	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on company and ship, organizational assets, or individuals	A limited adverse effect means that a security breach might: (i) cause a degradation in ship operation to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The loss of confidentiality, integrity, or availability could be expected to have a substantial adverse effect on company and ship, assets or individuals	A substantial adverse effect means that a security breach might: (i) cause a significant degradation in ship operation to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
High	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on company and ship operations, assets, environment or individuals	A severe or catastrophic adverse effect means that a security breach might: (i) cause a severe degradation in or loss of ship operation to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to environment and/or organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

the risk assessment process starts by assessing the systems on board, in order to map their robustness to handle the current level of cyber threats. The assessment should assess the IT and OT systems on board. When conducting the assessment, the company should consider the outcomes of the ship security assessment.

Risk assessment process

Phase 1: Pre-assessment activities

Prior to starting a cyber-risk assessment on board, the following activities should be performed:

- map the ship's key functions and systems and their potential impact levels
- identify main producers of critical shipboard IT and OT equipment
- review detailed documentation of critical OT and IT systems including their network architecture, interfaces and interconnections
- identify cyber security points-of-contact with each of the producers and establish a working relationship with them
- review detailed documentation on the ship's maintenance and support of the IT and OT systems
- establish contractual requirements and obligations that the ship-owner/ship operator may have for maintenance and support of shipboard networks and equipment
- support, if necessary, the risk assessment with an external expert to develop detailed plans and include producers and service providers.

Phase 2: Ship assessment

The activities performed during an assessment could include reviewing the configuration of all computers, servers, routers, and cyber security technologies including firewalls. It could also include reviews of all available cyber security documentation and procedures for connected IT and OT systems and devices.

Phase 3: Debrief and vulnerability review/reporting

Following the assessment, each identified vulnerability should be evaluated for its potential impact and the probability of its exploitation. Recommended technical and/or procedural corrective actions should be identified for each vulnerability. Whilst cyber risk management policies and procedures should be included in the company safety management system, these should not contain information, which if made available outside the company could become a vulnerability.

Phase 4: Producer debrief

Once the ship owner has had an opportunity to review, discuss and assess the findings, a subset of the findings may need to be sent to the producers of the affected systems. Any findings, which are approved by the ship owner for disclosure to the producers, could be further analyzed with support from external experts, who should work with the producer's cyber security point of contact to ensure that a full risk and technical understanding of the problem is achieved. This supporting

activity is intended to ensure that any remediation plan developed by the producer is comprehensive in nature and identifies the correct solution to eliminate the vulnerabilities.

4. Develop protection and detection measures

The outcome of the company's risk assessment and subsequent cyber security strategy should be a reduction in risk to be as low as reasonably practicable. At a technical level, this would include the necessary actions to be implemented to establish and maintain an agreed level of cyber security. It is important to identify how to manage cyber security on board and to delegate responsibilities to the master, responsible officers and when appropriate the company security officer.

Effective segregation of systems, based on necessary access and trust levels, is one of the most successful strategies for the prevention of cyber incidents. Effectively segregated networks can significantly impede an attacker's access to a ship's systems and is one of the most effective techniques for preventing the spread of malware. Onboard networks should be partitioned by firewalls to create safe zones. The fewer communications links and devices in a zone, the more secure the systems and data are in that zone. Confidential and safety critical systems should be in the most protected zone.

Procedural controls are focused on how personnel use the onboard systems. Plans and procedures that contain sensitive information should be kept confidential and handled according to company policies. Examples for procedural actions can be:

- Training and awareness
- Access for visitors
- Upgrades and software maintenance
- Anti-virus and anti-malware tool updates
- Remote access
- Use of administrator privileges

5. Establish contingency plans

Any cyber incident should be assessed to estimate the impact on operations, assets etc. In most cases, and with the exception of load planning and management systems, a loss of IT systems on board, including a data breach of confidential information, will be a business continuity issue and should not have any impact on the safe operation of the ship. In the event of a cyber-incident affecting IT systems only, the priority may be the immediate implementation of an investigation and recovery plan.

In general, appropriate contingency plans for cyber incidents, including the loss of critical systems and the need to use alternative modes of operation, should be addressed by the relevant operational and emergency procedures included in the safety management system. Some of the existing procedures in the ship's safety management system will already cover such cyber incidents. However, cyber incidents may result in multiple failures causing more systems to shut down at the same time.

The following is a non-exhaustive list of cyber incidents, which should be addressed in contingency plans on board:

- loss of availability of electronic navigational equipment or loss of integrity of navigation related data
- loss of availability or integrity of external data sources, including but not limited to GNSS
- loss of essential connectivity with the shore, including but not limited to the availability of Global Maritime Distress and Safety System (GMDSS) communications
- loss of availability of industrial control systems, including propulsion, auxiliary systems and other critical systems, as well as loss of integrity of data management and control
- the event of a ransomware or denial or service incident.

it is important to help ensure that a loss of equipment or reliable information due to a cyber-incident does not make existing emergency plans and procedures ineffective. Contingency plans and related information should be available in a non-electronic form as some types of cyber incidents can include the deletion of data and shutdown of communication links.

6. Respond to and recover from cyber security incidents

A team, which may include a combination of onboard and shore-based personnel and/or external experts, should be established to take the appropriate action to restore the IT and/or OT systems so that the ship can resume normal operations. The team should be capable of performing all aspects of the response. An effective response should at least consist of the following steps:

- Initial assessment
- Recover systems and data
- Investigate the incident
- Prevent a re-occurrence.

Recovery plans should be available in hard copy on board and ashore. The purpose of the plan is to support the recovery of systems and data necessary to restore IT and OT to an operational state. To help ensure the safety of onboard personnel, the operation and navigation of the ship should be prioritized in the plan. The recovery plan should be understood by personnel responsible for cyber security. The detail and complexity of a recovery plan will depend on the type of ship and the IT, OT and other systems installed on board.

Investigating a cyber-incident can provide valuable information about the way in which a vulnerability was exploited. Companies should, wherever possible, investigate cyber incidents affecting IT and OT on board in accordance with company procedures. A detailed investigation may require external expert support. The information from an investigation can be used to improve the technical and procedural protection measures on board and ashore. It may also help the wider maritime industry with a better understanding of maritime cyber risks.

References

1. GUIDELINES ON MARITIME CYBER RISK MANAGEMENT (MSC-FAL.1/Circ.3).
2. MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS (RESOLUTION MSC.428 (98)).
3. The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.
4. ISO/IEC 27001 standard on ISMS by the ISO and IEC.
5. United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).

For any questions about this Technical Information, please contact:
Iranian Classification Society (ICS)
Convention & Legislation Department
Phone: +98-21-42186210
Fax: +98-21-88837744
E-Mail: cld@ics.org.ir
Person in charge: Management system Department