INTERNATIONAL
MARITIME
ORGANIZATION

E

MARITIME SAFETY COMMITTEE
108th session
Agenda item 6

MSC 108/6/1
11 March 2024
Original: ENGLISH
Pre-session public release: ☒

REVISION OF THE GUIDELINES ON MARITIME CYBER RISK MANAGEMENT (MSC-FAL.1/CIRC.3/REV.2) AND IDENTIFICATION OF NEXT STEPS TO ENHANCE MARITIME CYBERSECURITY

Proposed improvements to MSC-FAL.1/Circ.3/Rev.2

Submitted by IACS

SUMMARY

Executive summary:	This document highlights the increasing vulnerability of the maritime industry to cyberattacks due to increased digitalization and connectivity and provides an insight into existing instruments. The document proposes improvements to MSC-FAL.1/Circ.3/Rev.2 to provide further guidance which could be helpful to the maritime industry.
Strategic direction, if applicable:	2
Output:	2.8
Action to be taken:	Paragraph 23
Related documents:	MSC 108/6; MSC 107/20; MSC-FAL.1/Circ.3/Rev.2 and resolution MSC.428(98)

Background

1 In 2017 IMO issued the *Guidelines on maritime cyber risk management* (MSC-FAL.1/Circ.3) to address the rising concern of maritime cyber risk. The guidelines provide high-level requirements to address cyber risks for onboard systems comprising information technology (IT) and operational technology (OT) through a five-level functional elements approach: identify, protect, detect, respond and recover.

2 Resolution MSC.428(98) on maritime cyber risk management recommended that cyber risks should be suitably addressed in ship's safety management systems not later than 1 January 2021. This resolution refers to MSC-FAL.1/Circ.3 which includes high-level guidelines and provides reference to industry guidelines and IACS recommendations.

Discussion

3 The maritime industry is largely governed by international regulations and any additional requirements of the flag Administration of the ship for the security and safety compliance. When such security and safety depend on cyber systems, a need for detailed guidance or regulations for an effective cyber risk management which would help flag States to achieve common minimum requirements towards a holistic approach is considered necessary; absence of detailed requirements could lead to different interpretations and implementation which may not be uniform across the maritime industry.

4 Digital integration, data analytics, use of decision support systems and artificial intelligence are the core technologies which will dominate future shipbuilding and ship designs. Grouped under the broad terminology of the "fourth industrial revolution" the focus will be on how smart devices will assist the role of humans for the management, optimization and control of machinery. The internet of things, smart sensors and ease in data transmission are some of the technologies which are aiding in this transition. Data sharing is one of the key advantages of digitalization.

5 The United Nations Conference on Trade and Development observed that digitalization is helping the industry to navigate the "efficiency, optimization, reliability, visibility, resilience, predictability, and sustainability" challenges of post-COVID-19 economy.

6 With increased digitalization, systems become more vulnerable as the attack surface (i.e. the systems which can be accessed from external or internal networks) increases**.** While there is a rise in cyberattacks, the percentage of attacks which are automated is also increasing. Automated attacks are used by the hackers which enable them to get insight into vulnerabilities and subsequently use this insight to plan for attacks. The attackers can compromise computer networks on ships and use malware to infect these computer networks. Having access to the computer networks on the ship can interfere with operation of ship systems.

7 The basic principles of cyber risk mitigation measures remain the same, however the solutions or the controls to mitigate risk, especially the technical controls could be ship specific. Changes in hardware and updates of software are to be assessed to identify and mitigate any impending cyber risks due to changes.

8 The challenge for existing ships is in maintaining the continuity of operations in the event of a cyberattack. Limited cyber expertise on board, regular crew changes and minimum shore support while at sea are some of the aspects which need specific attention.

Risk assessment

9 Successful implementation of cyber risk management requires that the cyber risks are assessed from the design stage by following a structured approach and through the use of equipment which provide an effective barrier to cyber risks. Following are the key aspects which play a critical role in effective cyber risk management.

10 Risk assessment is a critical activity to be undertaken in cyber risk management for onboard systems.

11 For certain scenarios the IT standards may not be appropriate for the OT environments as they may have different performance and availability requirements. Moreover, cyberattacks on the IT systems have essentially economic consequences, while cyberattacks on the OT systems can have a severe effect on the safety of the ship, safety of personnel and the environment. The risk evaluating criteria and methodology are to be suitably applied.

12 The risk is higher for specialized or technically advanced ships engaged in oil and gas exploration. It has been noted that offshore supply vessels, drilling rigs and shuttle tankers could be targeted more than a normal bulk carrier.

13 For a similar internal or external threat to onboard cyber systems, the consequences of a cyberattack will differ with type, size and location of a ship.

14 Ships with advanced autonomy, remote operation, maintenance aspects require a more in-depth structured risk assessment with a common understanding across various stake holders. Risk assessment should consider the complexity of onboard systems and their interconnectivity with systems located within and external to the ship.

15 While new build ships can be planned for robust cybersecurity control by addressing the issue at a design and construction phase, for the large fleet of existing ships the challenges in implantation of cybersecurity controls are different and generally one solution may not fit all ships. The challenge for older ships is in the implementation of risk mitigating controls for legacy systems which were not designed with cybersecurity in mind. Even in ships built over the last few years, vulnerability for a cyberattack has increased due to the lack of sufficient cybersecurity controls for the OT systems.

Cyber resilience

16 Cybersecurity and cyber resilience are two major topics, and both play distinct and significant roles; they are needed to address cyber threats on board.

17 Cybersecurity refers to the methods and processes implemented to protect digital data. Data identification, categorization and protection through technical and procedural controls form part of such processes. Cyber resilience is the ability of an organization to withstand or quickly recover from cyber incidents.

18 Cyber resilience is the capability to reduce the occurrence and to mitigate the effects of cyber incidents arising from the disruption or impairment of the OT used for the safe operation of a ship; the effects from incidents potentially lead to dangerous situations for human safety, safety of the ship and/or threat to the environment.

19 Further guidance to ensure secure implementation of both the OT and IT equipment into the ship's network during all stages of her life, from design and construction to commissioning and operation, is needed. The scope should include requirements for suitable barriers to prevent cyber-attacks for onboard IT and OT systems. Network design and protection of data play an important role in cyber resilience.

Identification of next steps to enhance maritime cybersecurity

20 As the industry prepares itself to address cybersecurity through a holistic approach, the need for cyber-secured components for ship systems, including navigation and communication systems, will be the need of the hour. The reliance on new builds shall be the implementation of more and more technical controls to fight cyberattacks. Considering that many of the existing control systems are legacy systems, the reliance on procedural, managerial controls is being increasingly adopted. There is a requirement to identify minimum technical controls for ships in operation.

21 Recognizing that cyber incidents on ships can have a direct and detrimental impact on life, property and the environment, there is a need to focus on the reliability and functional effectiveness of onboard safety-critical computer-based systems. The equipment and systems are to be designed and tested as per international standards to withstand and prevent a cyberattack.

Proposal

22 Considering the challenges brought out in paragraphs 9 to 21, IACS proposes that the existing *Guidelines on maritime cyber risk management* (MSC-FAL.1/Circ.3/Rev.2) be reviewed with the objective to provide additional guidance to maritime stakeholders as follows (the proposed amendments to the circular are shown in annex of this document):

.1 To amend paragraph 3.4 of MSC-FAL.1/Circ.3/Rev.2 to elaborate the risk assessment aspects, as discussed in paragraphs 9 to 15 of this document.

.2 The aspects of cyber resilience are spread over the five functional elements, as specified in paragraph 3.5 of MSC-FAL.1/Circ.3/Rev.2. To help achieve the implementation of effective cyber resilience and address the cyber resilience aspects as detailed in paragraphs 16 to 21 of this document, the requirements for cyber resilience should be included under each of the five functional elements (identify, protect, detect, respond and recover).

.3 To include an additional paragraph in MSC-FAL.1/Circ.3/Rev.2 on cyber secured equipment and systems. As detailed in paragraph 21 of this document, the equipment and systems are to be designed and tested as per international standards to withstand and prevent a cyberattack.

4 Subsequent to the publication of MSC-FAL.1/Circ.3/Rev.2, various guidelines and standards have been published which can serve as useful references. Reference to such documents should be included in paragraph 4.2 of MSC-FAL.1/Circ.3/Rev.2.

Action requested of the Committee

23 The Committee is invited to consider the proposals made in paragraph 22, together with the annex, and take action, as appropriate.

***

ANNEX

IACS PROPOSED AMENDMENTS OF MSC-FAL.1/CIRC.3/REV.2 ON THE *GUIDELINES ON MARITIME CYBER RISK MANAGEMENT*

"3 ELEMENTS OF CYBER RISK MANAGEMENT

…

3.4 One accepted approach to achieve the above is to comprehensively assess and compare an organization's current, and desired, cyber risk management postures. Such a comparison may reveal gaps that can be addressed to achieve risk management objectives through a prioritized cyber risk management plan. This risk-based approach is to evaluate the cyber risks, considering ship type and operational profile as well as onboard system's complexity and connectivity, which will enable an organization to best apply its resources in the most effective manner.

3.5 These Guidelines present the functional elements that support effective cyber risk management. These functional elements are not sequential – all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework:

.1 Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities, interdependencies between safety critical systems (including the information flow) that, when disrupted, pose risks to ship operations, human safety, safety of the vessel and/or threat to the environment.

.2 Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations, human safety, safety of the vessel and/or threat to the environment. Implement appropriate safeguards to protect the ship against cyber event and limit impact towards maximising ship operational continuity.

.3 Detect: Develop and implement activities necessary to detect a cyber-event arising from internal or external threat in a timely manner. Implement appropriate measures to detect unintended activity on computer-based systems and timely identification of a cyber event.

.4 Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event. Implement appropriate measures to minimise the effect of detected cyber event to other parts of ship systems.

.5 Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event. Implement appropriate measures to restore onboard computer-based systems including networks, after a cyber event.

…

3.8 Implementation of cyber resilient equipment and systems is to be considered. As part of technical measures, equipment and systems should be designed and tested as per international standards to assure cyber resilience onboard ships.

4 BEST PRACTICES FOR IMPLEMENTATION OF CYBER RISK MANAGEMENT

4.2 Additional guidance and standards may include, but are not limited to:*

…

.6 IACS UR E26 Cyber resilience of ships.

.7 IACS UR E27 Cyber resilience of on-board systems and equipment."