INTERNATIONAL MARITIME ORGANIZATION

MARITIME SAFETY COMMITTEE
108th session
Agenda item 6

MSC 108/INF.11
11 March 2024
ENGLISH ONLY

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

## The incorporation of cyber risk management in safety management systems

**Submitted by IACS**

**SUMMARY**

| | |
|---|---|
| *Executive summary:* | The document informs about IACS Recommendation No.171 on incorporating cyber risk management into safety management systems. |
| *Strategic direction, if applicable:* | 2 |
| *Output:* | 2.8 |
| *Action to be taken:* | Paragraph 15 |
| *Related documents:* | MSC 108/6/1; MSC-FAL.1/Circ.3/Rev.2 and resolution MSC.428(98) |

## Background

1 Cybersecurity in maritime industry is fast evolving and is a major concern due to lack of proper security controls and procedures for onboard vulnerable systems. Use of advanced communication technologies, high end computers, state of the art control and automation systems is on the rise for various shipboard operations including machinery control, cargo control and E-navigation. Recent cyberattacks on maritime cyber systems clearly indicate their vulnerability against targeted attacks.

2 Maritime Safety Committee, at its ninety-eighth session, approved the *Guidelines on maritime cyber risk management* (MSC-FAL.1/Circ.3) and subsequently at its 104th session approved Rev.2 of MSC-FAL.1/Circ.3. By resolution MSC.428(98), Maritime Safety Committee also affirmed that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code.

3 IACS and other industry stakeholders developed and published documents which provide high level recommendations to address maritime cyber risks.

4 The fourth version of the industry *Guidelines on cybersecurity on board ships*, provides guidance to shipowners and operators on procedures and actions to maintain the security of cyber systems in the company and onboard ships.

5 IACS published its *Recommendation on cyber resilience* (IACS Recommendation No.166) (hereinafter referred to as Rec.166). The purpose of this recommendation, developed through close interaction with members of the Joint Industry Working Group on Cyber Systems, is to provide technical guidance to stakeholders which would lead to delivery of cyber resilient ships whose resilience can be maintained throughout their service life.

**Discussion**

6 Risk assessment is a critical activity in the process of addressing cyber risks. A holistic approach considering various types of threats is to be considered while analysing impact not only at the system level but also the overall impact on ship safety and environment. The risk assessment in effect lays a strong foundation on which the complete cyber risk management is built.

7 Multiple tools are available for carrying out the risk assessment; each industry over the last few years has produced methods/guidelines to suit their particular needs. With specific reference to maritime cyber systems, the type of a ship, the fact that a ship is in motion and could cover various geographical zones and integration of the IT and the OT systems are only some challenges which need more attention while addressing maritime cyber risks.

8 With the objective to provide guidance on cyber risk assessment while considering the above criterion, IACS has published *Recommendation on incorporating cyber risk management into safety management systems* (IACS Recommendation 171) (hereinafter referred to as Rec.171). Developed also with the objective of addressing cyber incidents in the maritime sector, Rec.171 considers the complexity of onboard systems and their interconnectivity within and external to the ship. Rec.171 provides information to Companies on how to undertake risk assessments considering human factors in relation to cyber systems, determining what should be done to mitigate risks.

9 The methodology provided in Rec.171 can be used as one of the possible methods to address cyber safety issues within the context of MSC-FAL.1/Circ.3.

10 Rec.171 approaches its objective to identify cyber risks through:

.1 defining a methodology to assess the impact of cyber incidents on a ship covering risks from technology and daily activities of personnel;

.2 a step-by-step approach in performing cybersecurity risk assessments while considering all relevant factors; and

.3 risk mitigation measures and their impact on risk levels.

11 An outline of Rec.171 sections and related content is as follows:

.1 Section 1 gives brief outline of the background on IMO documents on cyber risk management and informs the user as to the intent of the recommendation.

.2 Section 2 introduces the importance of risk assessment and provides reference to various methods in use for risk assessment. This section informs the user on how to use the recommendation and provides a proposed risk assessment methodology flow chart. The users are informed that it is not mandatory to use the risk assessment methodology proposed in the recommendation as other available risk assessment methods can also be used. However, it highlights the advantages of the proposed methodology.

.3 Section 3 provides details of terms and definitions used in the recommendation.

.4 Section 4 details the scope of application and provides a systems reference table with details of various onboard systems which could be included in the analysis.

.5 Section 5 provides requirements and categories for identification of key equipment and technical systems. The recommendation uses the same categories for identification of technical systems as defined in IACS Unified Requirement E22 on *Computer based systems*. Technical systems categories are assigned based on their effects on system functionality.

.6 Section 6 provides a non-exhaustive list of cybersecurity threats, attacks, and techniques.

.7 Section 7 provides a deeper understanding of various factors to be considered while assessing cyber risk. The section, while outlining the methodology, brings out two critical factors: threat impact and the threat likelihood.

In a cyber system, complexity of the systems and its connectivity play a major role in risk assessment. Combination of these two factors brings a new dimension of cyberattack surface into risk assessment.

It also brings out the importance of considering the human element, either as a target with various degrees of awareness, or as attacker with different levels of attacking capability ranging from an unintentional attacker to cyber warfare attacker.

Rec.171 details how to perform cybersecurity risk assessment (including assessing potential operational impacts and likelihood of occurrence), which should take into account human factors, emerging threats, known vulnerabilities, and operational data in relation to the systems in scope. The recommendation provides guidance on how to identify and implement risk treatment measures and plans for mitigating cybersecurity risks.

.8 Section 8 provides the approach to mitigation measures and outlines types of measures which range from "human related" or "non-technical" measures to the most elaborate "technical" measures. Mitigation measures should be chosen and implemented until an acceptable (and assumed by ship-owner) Residual Risk Level is achieved.

12 Rec.171 also provides guidance on how a "risk level factor" can be reduced through the implementation of various types of mitigation measures.

13 Rec.171 is supported with appendixes which provide further guidance and information as follows:

.1 Appendix 1 provides a table on threats, attacks and techniques reference.

.2 Appendix 2 brings out the importance of human element and notes that human element is not limited to crew members but shall also include personnel ashore as the safety management system is also implemented in Company offices. This emphasizes the importance of providing training and awareness to all such personnel. Lack of training and awareness is identified as potential vulnerability which can be exploited by attackers. The need for different levels of training based on the role and responsibility of the personnel is emphasized.

.3 Appendix 3 provides a list of topics which should be considered while developing the procedures to be included in safety management system.

.4 Appendix 4 gives information on sections of Rec.166, which should be referred when building a response to the type of attack or threat.

14 Rec.171 can be downloaded by following this link:

https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2023/08/10125414/rec171-1.pdf

**Action requested of the Committee**

15 The Committee is invited to note the information provided.

___