INTERNATIONAL MARITIME ORGANIZATION

E

MARITIME SAFETY COMMITTEE
105th session
Agenda item 8

MSC 105/8/2
11 February 2022
Original: ENGLISH
Pre-session public release: ☒

MEASURES TO ENHANCE MARITIME SECURITY

Voluntary cyber risk management guidelines for shipboard operational technology (OT) systems

Submitted by Singapore

SUMMARY

Executive summary:	This document provides a set of voluntary cyber risk management guidelines for major shipboard operational technology (OT) systems, relevant for personnel directly responsible for the day-to-day ship operations and security of shipboard systems, such as engineers as well as Information Technology (IT) and OT system specialists
Strategic direction, if applicable:	5
Output:	Not applicable
Action to be taken:	Paragraph 18
Related documents:	MSC 98/23; MSC-FAL.1/Circ.3/Rev.1 and resolution MSC.428(98)

Introduction

1 Ships are increasingly reliant on digital technologies for their operations. However, rising in tandem are evolving cyber threats that can lead to severe consequences such as ship damage, loss of lives as well as reputational and economic loss for the company which might take years to recover financially. Hence, the application of appropriate cybersecurity practices plays a crucial role in safeguarding ships from emerging and existing cyber threats.

2 As vessels connect to the Internet for efficient operations, shipboard systems are becoming more interconnected. This translates to a bigger attack surface for the attackers to exploit and underscores the growing need to strengthen cybersecurity controls and processes on board vessels. As such, there are merits to introduce a cyber risk management approach for ships to aid the maritime industry in the implementation of IMO resolution MSC.428(98) requirements on maritime cyber risk management more effectively and consistently.

3 In this regard, Singapore, in collaboration with the Singapore University of Technology and Design, has developed a set of voluntary guidelines which can be used by the maritime industry to manage the cyber risks associated with major shipboard OT systems. A set of guidelines that includes actionable mitigation measures for managing the cyber risks associated with crucial shipboard systems will be useful in assessing the cyber readiness of a vessel.

4 While there are existing guidelines on maritime cyber risk management published by maritime organizations and educational institutions, these generally provide high-level guidance that are targeted at executives at the managerial level. There is a gap in the availability of guidelines relevant for personnel directly responsible for the day-to-day ship operations and security of shipboard systems (such as engineers as well as Information Technology (IT) and OT system specialists). The voluntary guidelines developed in this document are therefore focused on shipboard OT systems and include a checklist designed to provide specific technical and actionable mitigating plans to manage the cyber risks in shipboard OT systems.

Voluntary guidelines for cyber risk management on shipboard OT systems

5 In the voluntary guidelines developed, an overview of the cyberattack surfaces and the potential cyber risks associated with the shipboard OT systems are first addressed to highlight the impacts that can result from exploiting a particular attack surface. This provides the maritime industry with a clearer picture of how cyberattacks can target various shipboard systems and the impact that may result from such attacks.

6 After which, a set of specific mitigation measures for each of the risks in the shipboard systems is included to better prepare ships in managing the risks and to help limit the consequences from cyber incidents. These mitigation measures include technical, procedural, and physical security measures such as firewall and antivirus installation, crew training and awareness as well as access control lists.

7 The voluntary guidelines focus on the cyber risk management of the following major shipboard OT systems that are crucial for the day-to-day operation of ships:

.1 Communication Systems;
.2 Propulsion, Machinery and Power Control Systems;
.3 Navigation Systems; and
.4 Cargo Management Systems.

8 Ship-to-ship communication and ship-to-shore communication are crucial for activities such as alerting, reporting, and sending or receiving maritime safety information. Hence, a secure and reliable communication medium for the ship is fundamental. Cyberattacks targeting essential communication systems such as satellite communication systems and Voice over Internet Protocol (VoIP) phones can cause disruption in communication between ships and between ship and shore.

9 The ship's propulsion as well as power generation and management systems are very crucial to propel the ship and to provide power for various ship operations. The performance parameters of such systems are typically monitored and controlled through a computer console. Since this system is connected to the Internet for various reasons (such as operational requirements and remote updates), the system can fall victim to cyberattacks which could result in implications such as the disruption of the vessel's power supply.

10 Vessels are also equipped with various advanced navigational equipment that provide accurate navigation data. These systems are important in determining the position, speed and heading of the vessel which allow the vessels to navigate and reach their destination safely. Cyberattacks targeting the navigation systems may leave the ship without any means for safe navigation, which could result in catastrophic consequences such as collision.

11 The cargo management system that assists in the controlling and tracking of cargo, and the ballast water system that helps in maintaining a ship's stability under various voyage

conditions can also be subject to cyberattacks due to human factors and the reliability on the Internet for management and operational purposes. Cyberattacks on these systems can lead to severe repercussions on cargo operations and the vessel's stability.

12 The voluntary guidelines further include a cyber risk assessment approach to aid in assessing the risks in each shipboard OT system. The risk assessment approach involves a 4x4 risk score matrix to evaluate the risk score based on the severity and likelihood of different cyber risks. The severity score will be determined by the impact caused by a cyberattack on (i) the level of confidentiality, integrity and availability; (ii) the extent of environmental damage; and (iii) economic loss incurred by the company. The likelihood score will be determined by (i) the technical capabilities and resources required for an attacker to exploit a particular vulnerability; (ii) the frequency of occurrence of crew related factors that can lead to a cyberattack; and (iii) the complexity of a cyberattack. By combining both the impact severity and the likelihood score, the risks are divided into three categories, namely, high, medium and low risk.

13 Apart from the cyber risk assessment, having a checklist with the recommended mitigation measures can help ships ensure that the most crucial safety measures are in place. This checklist is included in the voluntary guidelines, which provides actionable cybersecurity measures to each of the cyber risks associated with the shipboard systems.

14 The concept of security tiers is also introduced in the checklist to address the urgency in managing the cyber risks. This will provide a more targeted approach and allow shipowners and managers to quickly zoom in on the critical cybersecurity measures that need to be implemented. There are three security tiers (Tier 1, Tier 2, Tier 3), where a tier of security refers to the urgency of cyber risks of a ship that need to be managed.

15 The security tiers are defined as follows:

.1 Tier 1: The Tier 1 checklist includes cybersecurity measures for managing high risk cyber threats, which means that the measures stated under this tier are highly recommended for vessels to implement on board.

.2 Tier 2: The Tier 2 checklist includes cybersecurity measures for managing medium risk cyber threats, which means that the security controls mentioned under this tier are recommended to have on board.

.3 Tier 3: The Tier 3 checklist includes cybersecurity measures for managing low risk cyber threats, which means that the measures listed under this tier are good to have on board, even though the risk level of the cyber threats is low.

16 The shipowner or ship manager may first perform the risk assessment, identify the risk category of cyber risks, and then choose to mitigate the cyber risks accordingly depending on the security tiers that the cyber risks lie in.

17 The voluntary cyber risk management guidelines developed by Singapore, in collaboration with the Singapore University of Technology and Design, are easy to implement, and it will allow the maritime industry to adopt good cybersecurity practices to manage the cyber risks associated with the shipboard OT systems. Singapore has released the guidelines to owners and operators of the Singapore Registry of Ships, for their reference and use since 1 November 2021. The complete voluntary guidelines can be found here and are freely available to all entities that may find them useful.

Action requested of the Committee

18 The Committee is requested to note the voluntary cyber risk management guidelines for shipboard operational technology (OT) systems.