INTERNATIONAL MARITIME ORGANIZATION

E

MARITIME SAFETY COMMITTEE
101st session
Agenda item 4

MSC 101/4/1
11 March 2019
Original: ENGLISH

MEASURES TO ENHANCE MARITIME SECURITY

The Industry Guidelines on cyber security on board ships, version 3

Submitted by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, CLIA, INTERCARGO, InterManager and WSC

SUMMARY

Executive summary:	This paper informs about the third version of the Industry Guidelines on cyber security on board ships
Strategic direction, if applicable:	SD 5
Output:	Not applicable
Action to be taken:	Paragraph 8
Related documents:	MSC 95/4/1; FAL 40/INF.4; resolution MSC.428(98) and MSC-FAL.1/Circ.3

Introduction

1 The first version of the Industry Guidelines on cyber security on board ships (the Industry Guidelines) was published in 2016, and the authors at that time agreed that the Industry Guidelines should be a 'living' document to reflect developments, including in threats and protection measures. Version 2 of the Industry Guidelines was published in July 2017 and version 3 in December 2018.

2 In addition to the co-sponsors, version 3 of the Industry Guidelines was developed by a wide range of stakeholders. These are listed in annex 5 of the Industry Guidelines, available through the official IMO website at the following address: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx

3 The Industry Guidelines are designed to continuously enhance understanding and awareness of key aspects of cyber risk management by companies. They are not intended to give technical guidance for the ship or personnel on board.

The revision

4 Resolution MSC.428(98) on *Maritime Cyber Risk Management in Safety Management Systems* (SMS) states that an approved SMS should consider cyber risk management in accordance with the objectives and functional requirements of the International Safety Management (ISM) Code. MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities.

5 The Industry Guidelines provide authoritative guidance on how to comply with resolution MSC.428(98) at the first annual verification of the company's Document of Compliance after 1 January 2021. This authoritative guidance, which may also be considered valuable by Administrations, is aligned with MSC-FAL.1/Circ.3 and is provided in annex 2 of the Industry Guidelines.

6 The revision has furthermore enhanced existing text in accordance with industry's practical cyber risk management experience and knowledge. The following paragraphs highlight the updates to version 3 of the Industry Guidelines:

.1 The difference between operational technical systems (OT) and information technical systems (IT) has been further elaborated, emphasizing that the possible effect that OT has on the physical world should be considered bearing in mind that the physical and the digital worlds are now intertwined.

.2 The NotPetya attack, which took place in 2017, affected shipping companies and container terminals but did not affect any ships; however, it showed the need for guidance on the immediate disconnection of the ship's systems to shore connections during a cyberattack where appropriate and warranted. Some systems may not be strictly necessary for operating the ship safely, but they could represent a potential attack vector to the systems that are required for the ship's safe operation. Furthermore, the chapter on how to respond to and recover from cyber security incidents has been updated in accordance with the lessons learnt from this and other attacks.

.3 Recalling that a ship is an integral part of the global supply chain, version 3 of the Industry Guidelines includes guidance on the relationship between the shipowner, ship agent, ship manager and vendors from a cyber risk management perspective. These relationships should not only be based on trust but also a common understanding of a mutually acceptable level of cyber risk.

.4 Seven examples of verified cyber incidents on board ships have been added to the Industry Guidelines to highlight the extent of known examples of cyber incidents.

Individual chapters of the Industry Guidelines

7 The content of the version 3 of the Industry Guidelines remains consistent with previous versions:

.1 Chapter 1 continues to address important overarching issues with regard to cyber risk management, including incorporation into the SMS.

.2 Chapter 2 outlines the potential cyber threats. Cyber risk reflects the circumstances of the company, the ship, the IT and OT systems and the communication technology used, as well as the organizations and persons with which the ship is in contact.

.3 Chapter 3 addresses vulnerable IT and OT systems found on board ships, so that an assessment can be made of their importance to safety and security.

.4 Chapter 4 gives guidance on how to conduct a cyber risk assessment.

.5 Chapter 5 concentrates on how to reduce the risk by using technical and procedural protection measures, emphasizing defence in breadth and depth.

.6 Chapter 6 continues to address the development of contingency and response plans in the case of a cyber incident. It recognizes that some of the existing procedures in the ship's SMS already address the impacts of cyber incidents. However, the potential for multiple, simultaneous failures of systems and loss of data should be considered.

.7 Response and recovery from cyber incidents are addressed in chapter 7.

.8 The chapters are supplemented by annexes providing more detailed guidance on issues including network design and incorporation of cyber risk management into an SMS.

Action requested of the Committee

8 The Committee is invited to note the information provided and take action, as appropriate.