INTERNATIONAL MARITIME ORGANIZATION

E

MARITIME SAFETY COMMITTEE
101st session
Agenda item 4

MSC 101/4/4
26 March 2019
Original: ENGLISH
Pre-session public release: ☒

MEASURES TO ENHANCE MARITIME SECURITY

Cyber risk management in Safety Management Systems

Submitted by United States, ICS and BIMCO

SUMMARY

Executive summary:	This document highlights concerns regarding potential inconsistencies in the implementation of the requirements embodied in resolution MSC.428(98) and requests that the Committee takes action to avoid such inconsistencies emerging as significant issues between now and 1 January 2021
Strategic direction, if applicable:	Not applicable
Output:	5.2, 6.1
Action to be taken:	Paragraph 16
Related documents:	MSC 101/4/1; resolution MSC.428(98) and MSC-FAL.1/Circ.3

Introduction

1 This document is submitted by the co-sponsors with concerns regarding the uniform implementation of *Maritime cyber risk management in safety management systems* (resolution MSC.428(98)). Specifically, there are concerns regarding national and regional:

.1 requirements which prioritize, or appear to prioritize, the provisions of the International Ship and Port Facility Security (ISPS) Code over those of the International Safety Management (ISM) Code for cyber risk management; and

.2 guidance which focuses on cyber security to counter external, malicious threats rather than providing a more holistic cyber risk management approach following the principles established in the ISM Code.

Background

2 Resolution MSC.428(98):

.1 recalls the purpose and objectives of the ISM Code;

.2 establishes a clear link between continuous improvement of approved safety management systems and incorporation of cyber risk management by companies; and

.3 encourages Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance (DoC) after 1 January 2021.

3 The *Guidelines on maritime cyber risk management* (MSC-FAL.1/Circ.3) state:

"2.1.4 ……Effective cyber risk management should consider both kinds of threat [malicious actions and unintended consequences of benign actions]."

4 Section 3 of MSC-FAL.1/Circ.3 provides the elements of effective cyber risk management, in particular: identify, protect, detect, respond and recover. These elements apply regardless of whether a cyber incident is the result of malicious action or is an unintended consequence of more benign actions.

5 The ISPS Code requires companies to take appropriate measures on all ships to identify and assess threats, and prevent and recover from security incidents (sections 7 to 9 of part A of the ISPS Code). The focus of the ISPS Code is on physical security threats and associated protective measures. However, paragraph 8.3 of non-mandatory part B of the ISPS Code refers to "computer systems and networks" as elements on board or within the ship which should be addressed in the context of ship security assessments and prevention of unauthorized access.

Discussion

6 For the shipping industry, resolution MSC.428(98) established a clear intent that the regulatory requirements of the Organization for cyber risk management were embodied in the provisions of SOLAS chapter IX and the ISM Code. Administrations are expected to clarify and enforce this intent.

7 Effective management of cyber risks by companies, in accordance with the international regulatory requirements, is understood to be demonstrated by:

.1 evidence of the continuous improvement of approved safety management systems conforming to the requirements of the ISM Code to take into account cyber risks; and

.2 implementation of policies and procedures for effective cyber risk management.

The proper management of cyber risks is expected to be verified by Administrations during the first annual review of a company's DoC following 1 January 2021.

8 The ISM Code provides a comprehensive framework for addressing cyber risks affecting the safe and environmentally sound operation of ships. The provisions for approval and auditing of company safety management systems allow for greater responsiveness to emerging cyber risks identified by the company.

9 The ISPS Code is focused on responding to external threats, malicious actions and physical security, and in this respect provides an incomplete framework for effective cyber risk management as outlined in paragraph 2.1.4 of MSC-FAL.1/Circ.3. Moreover, changes to the approved ship security plan require approval by the Administration. This reduces the responsiveness of companies to newly identified cyber risks, and introduces a potentially significant and frequent administrative burden for Administrations.

10 The co-sponsors consider the intent of resolution MSC.428(98) to be very clear on what is required of companies complying with SOLAS chapter IX and the ISM Code.

11 Consequently, it is with concern that the co-sponsors have become aware of potential inconsistencies in national and regional approaches to implementation; specifically, requirements and guidance on cyber risk management focused on the security objectives of the ISPS Code. The co-sponsors consider such requirements and guidance encouraging the establishment of separate cyber security management systems to be inconsistent with the intent of resolution MSC.428(98). Such approaches have the potential to introduce:

.1 gaps and inflexibility in company approaches to cyber risk which will undermine the Organization's intent to require effective cyber risk management; or

.2 an increased administrative burden for companies as cyber risk management would need to be addressed separately, and in parallel, in both approved safety management systems and approved ship security plans for it to be considered effective. This also risks documentary inconsistencies between the content of safety management systems and ships' security plans; and

.3 an increased administrative burden for Administrations required to approve changes to approved ship security plans.

12 In addition, the co-sponsors consider that having requirements for cyber risk management linked to both the ISM Code and the ISPS Code is unnecessary and problematic. Both the functional objectives of the ISM Code and the functional requirements of part A of the ISPS Code can be achieved by:

.1 implementing an approach to cyber risk management which incorporates the elements of effective cyber risk management (section 3 of MSC-FAL.1/Circ.3). This will address both malicious actions and unintended consequences of more benign actions; and

.2 adopting recognized procedural and technical protection measures for operational technology (OT), information technology (IT) and network infrastructure. Industry standards, class requirements or recommended practices, and Administration policies should provide guidance on recommended measures to integrate effective cyber risk management into the company's safety management regime. An example, recommended by the co-sponsors, is the Industry Guidelines on cyber security on board ships, version 3 (MSC 101/4/1).

13 Notwithstanding, the co-sponsors recognize that information, assessments and measures required by SOLAS chapter XI-2 and part A of the ISPS Code are relevant and necessary to support effective cyber risk management:

.1 Physical security is a procedural protective measure necessary to support at least the protect element described in section 3 of MSC-FAL.1/Circ.3. In particular, the prevention of unauthorized physical access to the ship and OT, IT and network infrastructure therein. In this regard, the identification and protection of restricted areas required as part of the ship security assessment (SSA) and ship security plan (SSP) required by SOLAS chapter XI-2 and part A of the ISPS Code should take into account the accessibility of OT, IT and network infrastructure. This means that compliance with the provisions of resolution MSC.428(98) may require consequential work by companies on the designation and protection of additional restricted areas; and

.2 Assessments of security threats as a functional requirement of part A of the ISPS Code should be considered relevant to the development of policies and procedures to meet the functional objectives of the ISM Code with regard to identification of security threats which may impact on the safe operation of ships and protection of the environment.

14 Port State control activities related to a failure to properly implement cyber risk management elements of an approved Safety Management System should follow IMO resolution A.1119(30) on *Procedures for port state control, 2017,* appendix 8, *Guidelines for port state control related to the ISM Code*.

Proposal

15 With a view to ensuring consistent implementation of the requirements of the Organization with respect to cyber risk management, and avoiding the potential difficulties outlined in paragraph 11, the co-sponsors propose that the Committee:

.1 reaffirms that Administrations are encouraged to ensure that cyber risks are appropriately addressed in approved safety management systems conforming to the requirements of SOLAS chapter IX and the ISM Code. After the first annual verification of the DoC after 1 January 2021, an endorsed DoC and Safety Management Certificate should be taken as demonstrating that cyber risks have been appropriately addressed by the company;

.2 recognizes that certain provisions of SOLAS chapter XI-2 and part A of the ISPS Code support effective cyber risk management (see paragraph 13), however, these provisions should not be considered as requiring a company to establish a separate cyber security management system operating in parallel with the company safety management system; and

.3 encourages Administrations to engage with other national and regional authorities to explain the Organization's requirements for cyber risk management by companies.

Action requested of the Committee

16 The Committee is invited to consider the concerns raised in this document, and the actions requested in paragraph 15, and take action as appropriate.