INTERNATIONAL MARITIME ORGANIZATION

E

MARITIME SAFETY COMMITTEE
98th session
Agenda item 5

MSC 98/5/2
4 April 2017
Original: ENGLISH

MEASURES TO ENHANCE MARITIME SECURITY

The incorporation of Cyber Risk Management in Safety Management Systems

Submitted by the United States

SUMMARY	
Executive summary:	Cyber-related risks are operational risks that are appropriately assessed and managed in accordance with the safety management requirements of the International Safety Management Code
Strategic direction:	6.1
High-level action:	6.1.1
Output:	6.1.1.1
Action to be taken:	Paragraph 10
Related documents:	MSC 95/4/1, MSC 95/4/2, MSC 95/4/3, MSC 95/4/4, MSC 95/4/6; MSC 96/4/1, MSC 96/4/2, MSC 96/4/3, MSC 96/4/5, MSC 96/4/6 and MSC 97/22; MSC.1/Circ.1526

Introduction

1 Cyber Risk Management is a timely and important issue for the maritime industry as the increasing reliance on cyber technology has led to the introduction of cyber-related risks into many shipboard operations. As demonstrated by previous discussions at recent sessions of the Maritime Safety Committee, as well as the subsequent development of MSC.1/Circ.1526 on *Interim guidelines on maritime cyber risk management*, a holistic risk management approach is best for addressing cyber-related risks. In this regard, managing cyber risk is a natural extension of current operational risk management practices currently incorporated into existing Safety Management Systems.

2 Intentionally expressed in broad terms, so as to have the widespread applicability needed to address the many risks of shipping, the International Safety Management (ISM) Code established a comprehensive framework for managing operational risks with the objective of maintaining high standards for safety and environmental protection. This breadth of application is sufficiently wide to include emerging risks associated with cyber-enabled systems. This is particularly true where MARPOL, SOLAS and flag Administration

IMO WORLD MARITIME DAY 2017
CONNECTING SHIPS, PORTS AND PEOPLE

requirements are satisfied by networked or cyber-enabled systems (e.g. computerized navigation systems, computerized engineering control systems, or computerized vessel cargo handling systems). Risks to those systems can quickly lead to non-compliance with regulatory requirements and pose risks to safety and the environment. For this reason, section 1.2.2.1 of the ISM Code requires companies to "assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards." Therefore, it is appropriate that Safety Management Systems developed to meet the ISM Code address cyber-related risks.

Relationship between Cyber Risk Management and the ISM Code

3 Section 1.2 of the ISM Code establishes specific safety management objectives using broad terms that do not identify specific equipment, technologies or operating conditions. Rather, with the goal of ensuring safety and environmental protection through compliance with international and flag Administration requirements, the Code clearly communicates that the objective of a Safety Management System is to provide for safe practices and a safe working environment by establishing appropriate mitigation measures based on an assessment of all identified risks to ships, personnel and the environment.

4 Based on the existing widespread agreement that cyber-enabled systems present operational risks, the justification and expectation for incorporating cyber risk management into Safety Management Systems is self-evident. Cyber-related risks in the maritime environment have been broadly identified and are commonly understood. As such, they need to be assessed and appropriately mitigated in accordance with the objectives and functional requirements of the ISM Code.

5 Verification that companies have adequately and appropriately implemented and incorporated appropriate cyber risk mitigation into their Safety Management System will occur during internal and external audits in accordance with the requirements of the ISM Code. During routine examinations it will be a simple matter to verify that a management system includes cyber risk management with a cursory review of the system's documentation. To satisfy the functional requirements in section 1.4 of the ISM Code, companies can develop instructions and procedures as well as define levels of authority and lines of communication related to cyber risk management. Given the widespread use of cyber systems across the industry, it is reasonable to expect that any present-day ship is vulnerable to cyber risks; therefore, it is reasonable to expect their Safety Management Systems will incorporate appropriate instructions, procedures, training requirements and lines of authority. Evidence of this will be clear upon the review of the Safety Management System.

6 It is up to shipowners and operators to assess prevailing cyber risks and to implement appropriate mitigating measures. The ISM Code encourages companies to take into account any guidelines or standards recommended by the Organization itself, flag Administrations, classification societies or maritime industry organizations. In this regard, companies may find the interim, non-mandatory guidelines contained in MSC.1/Circ.1526 provide useful guidance when assessing risk and implementing risk mitigation measures. Similarly, companies may find the guidance developed and promulgated by recognized organizations and non-governmental organizations to also be helpful, and are encouraged to refer to such guidance in the development of their Safety Management System. The risks to any specific ship are unique and dependent upon the specific integration of cyber systems aboard the ship. Therefore, the resulting incorporation of cyber risk mitigation measures into any particular Safety Management System will be correspondingly unique. For this reason, companies should carefully consider the selection of any guidance to ensure it is appropriately tailored to their unique circumstances.

7 The necessary risk assessment and incorporation of mitigation measures into an existing Safety Management System is a significant task that requires both time and resources to complete effectively. Shipowners and operators will need to assemble subject matter experts, identify relevant standards and guidance, conduct necessary assessments, design appropriate mitigation strategies and incorporate the required doctrine into the Safety Management System. Due to the effort and time needed, Administrations and port States will need to provide adequate time to owners and operators. One approach that could provide an acceptable length of time for implementation is to delay enforcement of the requirement on owners and operators to incorporate cyber risk management into their Safety Management System no later than the first annual verification of a company's Document of Compliance following the next renewal of the same after the effective date.

Way forward

8 In this regard, the Committee is invited to agree that:

.1 the management of cyber risks aboard vessels need to be accounted for in the same manner as other operational risks, namely through a Safety Management System that meets the requirements of the ISM Code; and

.2 shipowners and operators are expected to incorporate cyber risk management into their Safety Management System no later than the first annual verification of the company's Document of Compliance following the next renewal of the same after 1 January 2018.

9 If the Committee so agrees, a draft resolution reflecting this agreement has been attached as an annex for consideration.

Action requested of the Committee

10 The Committee is invited to consider the comments provided, and in particular the proposal in paragraph 8 and the draft resolution attached as an annex, and to take action as appropriate.

***

ANNEX

RESOLUTION MSC.[…]

ADOPTED ON […]

GUIDELINES FOR INCORPORATION OF CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARINE SAFETY COMMITTEE,

RECALLING Article 28(b) of the Convention on the International Maritime Organization concerning the functions of the Committee,

RECALLING ALSO resolution A.741(18) by which the Assembly adopted the *International Management Code for the Safe Operation of Ships and for Pollution Prevention* (International Safety Management (ISM) Code),

RECALLING FURTHER resolution A.788(19) by which the Assembly adopted the *Guidelines on implementation of the International Safety Management (ISM) Code by Administrations*,

NOTING that the ISM Code became mandatory, under the provisions of chapter IX of the International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended, for companies operating certain types of ships, on 1 July 1998; and for companies operating other cargo ships and mobile offshore drilling units propelled by mechanical means of 500 gross tonnage and upwards, on 1 July 2002,

NOTING resolution A.1071(28) by which the Assembly adopted the *Revised Guidelines on the implementation of the International Safety Management (ISM) Code by Administrations*,

HAVING CONSIDERED circular MSC.1/Circ.1526, by which the Committee approved the *Interim guidelines on maritime cyber risk management* at its ninety-sixth session,

1 AFFIRMS that cyber risks onboard vessels are identified risks that should be assessed as a part of an approved Safety Management System, in accordance with the objectives and functional requirements of the ISM Code;

2 ENCOURAGES Member Governments to ensure that cyber risks are appropriately incorporated in Safety Management Systems no later than the first annual verification of the company's Document of Compliance following the next renewal of the same after 1 January 2018;

3 REQUESTS Member Governments to bring this resolution to the attention of all stakeholders.