Cyber risk implementation guide

INTRODUCTION

Ships are increasingly using systems that rely on digitization, digitalization, integration, and automation, which call for cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the internet.

This brings the greater risk of unauthorized access or malicious attacks to ships' systems and networks. Risks may also occur from personnel accessing systems on board, for example by introducing malware via removable media.

In 2017, the International Maritime Organization (IMO) adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management System (SMS). The Resolution stated that an approved SMS should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code. It further 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 after 1 January 2021.

ELEMENTS OF CYBER RISK MANAGEMENT

Cyber risk management means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders.

The following functional elements should be incorporated appropriately in a risk management framework:

Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.

Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.

Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.

Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

CYBER RISK MANAGEMENT AND THE SAFETY MANAGEMENT SYSTEM

IMO Resolution MSC.428(98) makes clear that an approved SMS should take into account cyber risk management when meeting the objectives and functional requirements of the ISM Code. The guidance provided in the Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3) provides high level recommendations regarding the elements of an appropriate approach to implementing cyber risk management. Find here the minimum measures that all companies should consider implementing in an approved SMS.

IDENTIFY

Roles and responsibilities	
Action	Remarks
ISM Code 3.2 Update the safety and environment protection policy to include the risk posed by unmitigated cyber risks.	An updated safety and environment protection policy may include: • A commitment to manage cyber risks as part of the overall approach to safety management and protection of the environment.
ISM Code 3.3 Update the responsibility and authority for cyber risk management (CRM).	Responsibility and authority may need to be updated this can include: • Including compliance with cyber risk management policies and procedures into the existing responsibility and authority of the Master.
ISM Code 6.5 Identify any training which may be required to support the incorporation of cyber risk management into the SMS.	Existing company procedures for identifying training requirements can be used for: • All company personnel to receive basic cyber awareness training. • Company personnel, who have been assigned CRM duties, to receive a type and level of cyber training appropriate to their responsibility and authority. *Note: Cyber awareness training is not a mandatory requirement.*

Identification of systems that pose risks to ship operations when disrupted	
Action	Remarks
ISM Code 10.3 Identify equipment and technical systems (OT and IT) the sudden operational failure of which may result in hazardous situations.	An SMS has to identify the equipment and technical systems (including OT and IT), and capabilities, which may cause hazardous situations if they become unavailable or unreliable.
ISM Code 1.2.2.2 Assess all identified risks to ships, personnel and the environment and establish appropriate safeguards.	The full scope of risk control measures implemented by the company should be determined by a risk assessment. The following measures should be considered before a risk assessment is undertaken: • Hardware inventory and maintenance • Software inventory and maintenance • Awareness and training • Physical security

PROTECT

Development of contingency plans	
Action	Remarks
ISM Code 7 Update procedures, plans and instructions for key shipboard operations	Consideration should be given to developing instructions on the actions to be taken if disruption to critical systems is suspected. This could include procedures for reverting to back-up or alternative arrangements as a precaution whilst

concerning the safety of the personnel, ship and protection of the environment which rely on OT.	any suspected disruption is investigated.
ISM Code 8.1 Update emergency plans to include responses to cyber incidents.	Consideration should be given to the development of a cyber incident module in the integrated system of shipboard emergency plans for significant disruption to the availability of OT or the data used by them.

DETECT

Development and implement activities to detect a cyber-event in a timely manner	
Action	Remarks
ISM Code 9.1 Update procedures for reporting non-conformities, accidents and hazardous situations to include reports relating to cyber incidents.	Examples of non-conformities and cyber incidents: • unauthorized access to network infrastructure • unauthorized or inappropriate use of administrator privileges • suspicious network activity • unauthorized access to critical systems • unauthorized use of removable media • unauthorized connection of personal devices • failure to comply with software maintenance procedures • failure to apply malware and network protection updates • loss or disruption to the availability of critical systems • loss or disruption to the availability of data required by critical systems.

RESPOND

Develop and implement plans to provide resilience to a cyber incident	
Action	Remarks
ISM Code 3.3 Ensure that adequate resources and shore-based support are available to support the DPA in responding to the loss of critical systems.	The incorporation of CRM into the SMS should require that this resourcing includes appropriate IT expertise. This resource could come from within the company but may also be provided by a third party.
ISM Code 9.2 Update procedures for implementing corrective actions to include cyber incidents and measures to prevent recurrence.	The procedures should help ensure that consideration of non-conformities and corrective actions involves the personnel with responsibility and authority for CRM. This should help ensure that corrective actions, including measures to prevent recurrence, are appropriate and effective.
ISM Code 10.3 Update the specific measures aimed at promoting the reliability of OT.	A SMS, which incorporates CRM, should have procedures for: • Software maintenance • Version management for updating • Authorizing remote access • Preventing the use of uncontrolled or infected removable media. • Controlled use of administrator privileges to limit software maintenance tasks to competent personnel. • Possible alternative equipment, instruments and/or systems.

RECOVERY

Identify measures to back-up and restore cyber systems after a cyber incident	
Action	Remarks
ISM Code 10.4 Include creation and maintenance of back-ups into the ship's operational maintenance routine.	A SMS, which incorporates CRM, should include procedures for: • checking back-up arrangements for critical systems, if not covered by existing procedures • checking alternative modes of operation for critical systems, if not covered by existing procedures • creating or obtaining back-ups, including clean images for OT to enable recovery from a cyber incident • maintaining back-ups of data required for critical systems to operate safely • offline storage of back-ups and clean images, if appropriate • periodic testing of back-ups and back-up procedures.