conarina

TECHNICAL CIRCULAR No. 553 of 05th April 2019

To:	All Surveyors/Auditors
Applicable to flag:	All Flags

Guidelines on ISM/SMS Maritime Cyber Security

Reference: ISM, MSC.428(98)

Guidelines on ISM/SMS Maritime Cyber Security

This part provides guidance on what an approved Safety Management System should address to deal with current and emerging cyber security concerns.

IMO Resolution MSC.428(98) Maritime Cyber Risk Management in SMS

- IMO Resolution MSC.428(98) Affirms that an approved safety management system should consider cyber risk management in accordance with the ‘objectives’ and ‘functional requirements’ of the ISM Code.
  - **1.2 Objectives of ISM Code**, require the Companies to:
    - 1.2.2.1 provide for safe cyber practices in ship operation and a safe working environment;
    - 1.2.2.2 assess all identified cyber risks to its ships, personnel and the environment and establish appropriate cyber security safeguards; and
    - 1.2.2.3 continuously improve safety management skills of personnel ashore and aboard ships, including preparing for cyber emergencies
  - **1.4 Functional Requirements for a SMS**, may need to document:
    1. How identified cyber risks have been addressed in the safety management system
    2. Cyber risk mitigation instructions and procedures to ensure safe operation of ships and protection of the environment in compliance with relevant international and flag State legislation;
    3. Defined levels of cyber security authority and lines of communication between, and amongst, shore and shipboard personnel;
    4. Procedures for reporting cyber security accidents and non-conformities
    5. Procedures to prepare for and respond to cyber security incidents and emergency situations; and
    6. Procedures for addressing cyber security during internal audits and management reviews.

Cyber Security Threats:

Most cyber issues are preventable. The leading cause of cybersecurity breaches are from unintentional acts via common points of vulnerability.

The most common points of vulnerability include:

- Web browsers
- USB ports
- Wireless routers
- Mobile telephones
- Remotely operated engines/parts
- Navigation/GPS systems (chart updates)
- Crew personal devices
- Entertainment systems/WiFi – Internet/Satellite Systems

These common points of vulnerability can be breached at any time affecting most important activities onboard and ashore, including:

1. Propulsion plant control
2. Navigation/ship control
3. Drilling system control
4. Dynamic Positioning system control
5. Ballast system control
6. Crew management
7. Power Management Systems
8. Fire & Gas Detection/Alarm
9. Terminal operations

Purpose of Cyber Security Risk Assessment:

1. Assess and define the current state of cyber security profile and capabilities of a facility:
    1. OT/IT* technologies, policies, procedures
    2. OT/IT* cybersecurity functional documentation
2. Provide a gap analysis of risk
3. Provide a Cybersecurity Management system to close gaps
4. Assess implementation for organizational capability

REFERENCES:

- IMO Resolution MSC.428(98)

- ATTACHMENTS: No

Kindest Regards,

Val Bozenovici
Naval Architect – Conarina Technical Director