Circular 2017-11: Maritime Cyber Risk Management

Overview

Ships are increasingly using systems that rely on digitization, integration, and automation, which calls for cyber risk management on board. As technology continues to develop, information technology and operational technology 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. It may result in shipping related operational, safety or security failures as a consequence of information or system being corrupted, lost or compromised. Risks may also occur from personnel accessing systems on board, for example by introducing malware via removable media.

The safety, environmental and commercial consequences of not being prepared for a cyber incident may be significant. Responding to the increased cyber threat, a group of international shipping organizations, with support from a wide range of stakeholders, have developed guidelines, which are designed to assist companies develop resilient approaches to cyber security onboard ships.

Guidelines and Resolutions on Cyber Risk Management

The International Maritime Organization in June 2017 at the 98th session of the Maritime Safety Committee (MSC) adopted the MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management and the Resolution MSC.428 (98) on Maritime Cyber Risk Management in Safety Management Systems (SMS) to safeguard shipping from current and emerging cyber threats and vulnerabilities.

According to this Resolution MSC.428 (98), an approved Safety Management System (SMS) should take into account cyber risk management in accordance with the objectives and functional requirements of the International Safety Management (ISM) Code. The objectives of the ISM Code include the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment.

The Interim Guidelines on Maritime Cyber Risk Management was adopted in the Maritime Safety Committee (MSC) in session 96, through MSC.1/Circ.1526 which provides recommendations that can be incorporated into existing risk management processes. The Guidelines also include functional elements that support effective cyber risk management.

Actions Required

- Cyber risks should be appropriately addressed in a Safety Management System (SMS) no later than the first annual verification of the company's Document of Compliance that occurs after 1 January 2021.
- Plans and procedures for cyber risk management should be seen as complementary to the existing security and safety risk management requirements contained in the International Safety Management (ISM) Code and the International Ship and Port Facility Security (ISPS) Code.
- A **Cyber Security Management Plan** is recommended to support the Company's SMS for both office and managed vessels Cyber Risk Management.