**MARITIME ACTIVITIES CONSULTANTS S.A.**
***"CONNECTING YOUR BUSINESS TO THE MARITIME RESOURCES YOU NEED"***

**TECHNICAL SERVICE CIRCULAR No. 02/2020, Date: 11/12/2020**

**Subject: "Maritime Cyber Risk Management in Safety Management Systems (I.M.O. Resolution MSC.428(98)"**

**Background Brief:**

**1.** Technology has become essential to the operation and management of systems critical to the safety and security of shipping. This technological advancement also means increased exposure to the maritime sector to a greater risk of cybercrime.

**2.** IMO has adopted **resolution MSC.428 (98) on "Maritime Cyber Risk Management in Safety Management Systems"** to address the issues and raising awareness related to cyber risk threats and vulnerabilities. Emphasis is assigned to the fact that ships are becoming more and more complex and increasingly dependent on the extensive use of digital and communications technologies. The IMO provided also high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities.

**3.** Admittedly, there is no single solution to managing cyber risks. It is a collaboration involving people, processes, and IT systems. Following the respective guidelines establishing awareness in all levels of an organization is the important first step when implementing cybersecurity management. As advocated by all maritime stakeholder organizations Cyber technologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment.

**4.** Being mindful of the above, Resolution MSC.428(98) requires cyber risk management to be undertaken under the objectives and requirements prescribed by the ISM Code. **Cyber risks should be appropriately identified, analyzed, and addressed within the Safety Management**

**System no later than the first annual verification of the Document of Compliance after 1st January 2021.** In practice, this means that vessel owners need to identify and manage cyber risks the soonest as possible in preparation for the first annual verification of the company's document of compliance after 1 January 2021.

**5.** Appropriate safeguards should be developed and implemented based on the company's risk assessment taking into account guidance provided within MSC FAL.1/Circ.3. These provide actionable advice on (a) Developing a cybersecurity assessment and plan to manage risk, (b) Handling security breaches and incidents, (c) Highlighting national and international standards used, and (d) The relationship to existing regulation. Besides, the IMO guidelines on cyber risk management (MSCFAL.1/Circ.3) provide concrete functional elements of the risk management framework: identifying risk, detecting risk, protecting assets, responding to risk, and recovering from attacks. Based on these guidelines, shipping companies are recommended to undergo a cyber risk analysis to assesses threats and vulnerabilities, as well as the impact of potential hackers on systems critical for the safe operation of their ships.

**Follow-up Action:**

**6.** Via the issuance of Technical Circulars Flag States and International Registers are guiding shipping companies to ensure for vessels flying their flag that cyber risks are appropriately addressed in the safety management system no later than the first annual verification of the company's Document of Compliance after 1st January 2021.

***"SIMPLIFYING YOUR MARITIME NEEDS"***

Maritime Activities Consultants

PIRAEUS OFFICE:
110-112 Notara str., 185 35 Piraeus, Greece
Tel: +30 2104287112, Fax: +30 2104530310,
www.mac.com.gr, e-mail: mac-gr@otenet.gr