IMMARBE
INTERNATIONAL MERCHANT MARINE REGISTRY OF BELIZE

Merchant Marine Notice MMN-20-007

"Maritime Cyber Risk Management in Safety Management Systems (IMO Resolution MSC.428(98)"

TO: DEPUTY REGISTRARS, SHIP OWNERS/ISM OPERATORS/RECOGNIZED ORGANIZATIONS/SHIPPING AGENTS/GENERAL SAFETY INSPECTORS

MMN Superseded: N/A Revision No.:N/A
ISSUE DATE: **31 December 2020**

INTRODUCTION

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

2. IMO has adopted on 16 June 2017 the 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 Company's Document of Compliance after 1st January 2021**.

Keystone Building, Suite 502,
304 Newtown Barracks,
Belize City, Belize
+501 223 5031 / +501 223 5026
immarbe@immarbe.com

IMMARBE
INTERNATIONAL MERCHANT MARINE REGISTRY OF BELIZE

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. To perform a cyber risk assessment and to develop a cyber risk management plan,
    b. Handling treats presented by malicious actions or unintended consequences of benign actions,
    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 cyber 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.

PURPOSE

This purpose of this Merchant Marine Notice is to provides information on the requirement to incorporate maritime cyber risk management in the safety management systems (SMS) of companies operating Belize-registered vessels. This document also seeks to inform and remind stakeholders that in June 2017 at the 98th session of the Maritime Safety Committee (MSC), IMO 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.

CONTENT

1. International Maritime Organization Guidelines

1.1. International Maritime Organization (IMO) Circular MSC-FAL.1/Circ.3, Guidelines on Maritime Cyber Risk Management, contains high-level recommendations and functional elements for effective maritime cyber risk management.

1.2. Definitions

1.2.1. ***Maritime cyber risk*** is defined as a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping- related operational, safety, or security failures as a consequence of information or systems being corrupted, lost, or compromised; and

1.2.2. ***Cyber risk management*** is defined as the process of identifying, analyzing, 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.

Keystone Building, Suite 502,
304 Newtown Barracks,
Belize City, Belize
+501 223 5031 / +501 223 5026
immarbe@immarbe.com

1.3. The IMO guidelines set out the following principles in support of an effective cyber risk management strategy:

1.3.1. ***Identify:*** Define the roles responsible for cyber risk management and identify the systems, assets, data and capabilities that, if disrupted, pose risks to ship operations.
1.3.2. ***Protect:*** Implement risk control processes and measures, together with contingency planning to protect against a cyber incident and to ensure continuity of shipping operations.
1.3.3. ***Detect:*** Develop and implement processes and defenses necessary to detect a cyber incident in a timely manner.
1.3.4. ***Respond:*** Develop and implement activities and plans to provide resilience and to restore the systems necessary for shipping operations or services which have been halted due to a cyber incident.
1.3.5. ***Recover:*** Identify how to back-up and restore the cyber systems necessary for shipping operations which have been affected by a cyber incident.

2. Shipping Industry Guidelines on Cyber Security

2.1. The Guidelines on Cyber Security Onboard Ships ("Industry Cyber Guidelines"), published by a consortium of shipping industry organizations, are intended to mitigate the risk of major safety and security issues that could result from a cyber incident on board a ship. The guidelines address managing ship-to-shore interfaces, network segregation, port risks, and maritime cyber insurance coverage. This is a working document which is expected to be updated as necessary.

2.2. The Guidelines on Cyber Security Onboard Ships have been aligned with the IMO Guidelines on Maritime Cyber Risk Management. Taken together, these documents provide a solid basis for mitigating cyber risks throughout the SMS.

2.3. Annex 2 of the Guidelines on Cyber Security Onboard Ships should be referenced by vessel operators to ensure cyber risk management is incorporated throughout the SMS.

3. Maritime Cyber Risk Management Resources

The Administrator maintains, within its Technical Department, maritime cyber risk management resources from shipping industry associations, standard-setting organizations, government agencies, classification societies, and insurers. For resources contact the Technical Department at: technicalofficer@immarbe.com,technicalofficer2@immarbe.com, technicalsupport@immarbe.com.

Keystone Building, Suite 502,
304 Newtown Barracks,
Belize City, Belize
+501 223 5031 / +501 223 5026
immarbe@immarbe.com

IMMARBE
INTERNATIONAL MERCHANT MARINE REGISTRY OF BELIZE

4. Maritime Cyber Risk Management Training

4.1. The Administration considers cyber risk management and awareness training as a specialized subcategory of overall safety and security training. The following training exists for shipboard and shore-based personnel:

4.1.1. Security training for shore-based personnel is covered by IMO Circular MSC/Circ.1154, Guidelines on Training and Certification for Company Security Officers, issued 23 May 2005.

4.2. Many third parties have already developed maritime cyber risk awareness training courses which may be beneficial to the Company in developing a comprehensive cyber risk management system.

4.3. Companies that wish to provide cyber risk awareness training for their personnel should ensure the training courses are based on the principles contained in MSC-FAL.1/Circ.3 and the Industry Cyber Guidelines.

5. Cyber Incident Reporting

5.1. Cyber risks must be identified before they can be effectively managed. Therefore, cyber incident reporting is an essential element of the shipping industry's holistic approach to cyber risk mitigation.

5.2. It is highly recommended that all cyber incidents are reported to the Administration. Data received by the Administration will remain strictly confidential and reported incidents will not be attributed to any ship or Company.

5.3. Feedback or concerns should be directed to: technicalofficer@immarbe.com, technicalofficer2@immarbe.com, technicalsupport@immarbe.com.

ACTIONS REQUESTED

This Administration would like to encourage all Shipowners, Operators, Deputy Registrar and Recognized Organizations to take note of the contents of this Notice and to ensure its provisions are enforced on board vessels registered at IMMARBE on 29 December 2020. Look forward for your cooperation and assistance. The Guidelines on Maritime Cyber Risk Management laid down in MSC-FAL.1/Circ.3 and MSC.1/Circ.1526, contain recommendations for maritime cyber risk management and should be taken into account when developing appropriate safeguards against cyber threats and vulnerabilities.

Keystone Building, Suite 502,
304 Newtown Barracks,
Belize City, Belize
+501 223 5031 / +501 223 5026
immarbe@immarbe.com

IMMARBE
INTERNATIONAL MERCHANT MARINE REGISTRY OF BELIZE

REFERENCES

1. **IMO Resolution MSC.428(98) ,** *Maritime Cyber Risk Management in Safety Management Systems*, adopted 16 June 2017
2. **IMO Circular MSC-FAL.1/Circ.3 ,** *Guidelines on Maritime Cyber Risk Management,* issued 05 July 2017
3. **IMO Circular MSC.1/Circ.1526, Interim Guidelines on Maritime Cyber Risk Management, issued 01 June 2016**
4. **The Guidelines on Cyber Security Onboard Ships** – *Shipping Industry Associations/Organizations*

The Notice was issued in Belize city, Belize 31/12/2020

INTERNATIONAL MERCHANT MARINE REGISTRY OF BELIZE IMMARBE

Eng. Eduardo Simon
Technical Manager
IMMARBE

AnnetteGarel(Mrs.)
Senior Deputy Registrar
IMMARBE

Keystone Building, Suite 502,
304 Newtown Barracks,
Belize City, Belize
+501 223 5031 / +501 223 5026
immarbe@immarbe.com