REPUBLIC OF THE UNION OF MYANMAR
MINISTRY OF TRANSPORT AND COMMUNICATIONS
DEPARTMENT OF MARINE ADMINISTRATION
No-363/421, Corner of Merchant &Theinbyu Road,
Botataung Township, Yangon, Myanmar

E-mail: dma@motc.gov.mm, dma.myan@gmail.com Tel: +95-1-397640
P.O. Box: 194 Fax: +95-1-397641

Date: 8 October 2020

Marine Guidance (6/2020)

Maritime Cyber Risk Management

Applicable to: **Shipowners, Operators, Managers, Masters and Officers of Myanmar ships and Recognized Organizations (ROs)**

References:
(a) **IMO Resolution MSC.428(98),** Maritime Cyber Risk Management in Safety Management Systems, adopted on 16 June 2017
(b) **IMO Circular MSC-FAL.1/Circ.3,** Guidelines on Maritime Cyber Risk Management, 05 July 2017

Summary

The Department of Marine Administration circulates this Marine Guidance to provide information on the requirement to incorporate maritime cyber risk management in the safety management systems (SMS) of companies operating Myanmar ships.

PURPOSE

1. The purpose of this guidance is to provide information on the maritime cyber risk management required for establishing policies and procedures for mitigating maritime cyber risks.

2. The goal of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyber risks.

APPLICATION

3. This Guidance is intended for companies operating Myanmar ships and designed to establish safeguarding measures against cyber risks in order to foster safety and security management practices in the cyber domain.

BACKGROUND

4. Ships are increasingly using systems that rely on digitization, integration, automation and network-based systems. As a result, security of data and other sensitive information has become a major concern of the maritime industry, increasing the need for maritime cyber risk management.

5. Threats are presented by malicious actions (e.g. hacking or introduction of malware) or the unintended consequences of benign actions (e.g. software maintenance or user permissions).

6. Vulnerabilities can result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyber discipline. In general, where vulnerabilities in operational and/or

information technology are exposed or exploited. (e.g. weak passwords leading to unauthorized access, the absence of network segregation, inappropriate use of removable media such as a memory stick)

7. In accordance with the IMO Resolution MSC.428(98), an approved SMS should take into account cyber risk management in accordance with the objectives and functional requirements of the **ISM Code**. Companies are required to appropriately address cyber risks in the company's SMS no later than **the first annual verification of the ISM company's Document of Compliance after 1 January 2021**.

8. The DMA considers the **International Ship and Port Facility Security (ISPS) Code** as an extension of the ISM Code and an integral part of emergency preparedness and compliance with international conventions in a Company's Safety Management System.

CYBER RISK MANAGEMENT

9. IMO Circular MSC-FAL.1/Circ.3, Guidelines on Maritime Cyber Risk Management, defines **Cyber risk management** as 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.

10. **Maritime cyber risk** refers to a measure of the extent to which a technology asset is 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.

11. IMO Guidelines set out *five functional elements* to address maritime cyber risks in support of an effective cyber risk management strategy, namely: IDENTIFY; PROTECT; DETECT; RESPOND; and RECOVER.

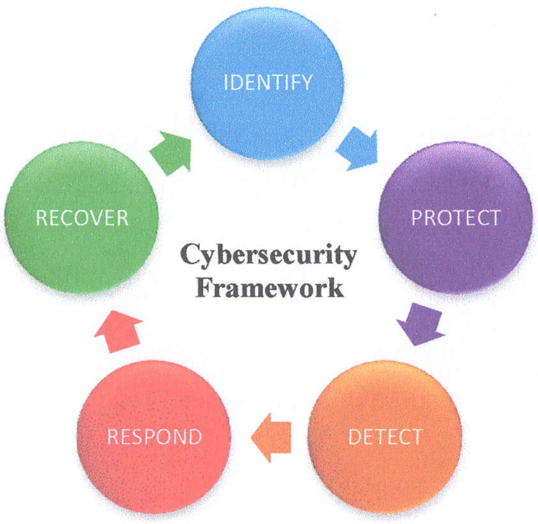

Fig: Cybersecurity Framework

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.

12. Companies of Myanmar registered ships are encouraged to review the identified risks to its ships, personnel and the environment and to establish appropriate safeguards to ensure that maritime cyber risks are appropriately addressed in the SMS, and that the five functional elements stated in para 11 have been incorporated into their risk management framework.

MARITIME CYBER RISK MANAGEMENT TRAINING

13. The DMA considers that cybersecurity trainings are specialized components of overall security training. The following trainings are required for shipboard and shore-based personnel:

    (a) Security training for shipboard personnel as required by the STCW Mandatory Training; and

    (b) Security training for shore-based personnel as covered by IMO Circular MSC/Circ.1154, *Guidelines on Training and Certification for Company Security Officers*.

14. Recognized Organizations (ROs) are encouraged to develop maritime cybersecurity training courses and relevant consultancy services to assist ISM Companies in developing and preparing their cyber risk management strategy and procedures.

ADDITIONAL GUIDANCE

15. The following shipping industry guidelines on cybersecurity have been published:

    (a) The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.

    (b) ISO/IEC 27001 standard on Information technology – Security techniques Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

    (c) United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).

CONTACT

16. Any queries relating to this guidance should be addressed to the DMA:

    Email: sse@dma.gov.mm

17. Any suspicious activity and breaches of security should be reported to:

    Myanmar Computer Emergency Response Team (MMCERT)

    Email: infoteam@mmcert.org.mm
    incident@ncsc.gov.mm

    Website: https://mmcert.org.mm/

8/10/20

Soe Naing
Director General