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
P.O. Box: 194

Tel: +95-1-397640
Fax: +95-1-397641

Date: 9 October 2020

Marine Guidance (7/2020)

Port Cyber Risk Management

Applicable to: **Port Operators, Managers, Port Facility Security Officers (PFSOs) and Port Security Consultants**

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

(c) **CYBER RISK MANAGEMENT: Best Practices for the Towing Industry, Version 1.0**

Summary

The Department of Marine Administration circulates this Marine Guidance to provide information on the requirement to incorporate maritime cyber risk management in the Port Facility Security Plans.

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 port operations and ship-port interface, which are operationally resilient to cyber risks.

APPLICATION

3. This Guidance is intended for international port facilities and designed to establish safeguarding measures against current and emerging cyber threats and vulnerabilities in order to foster risk management practices in the cyber domain.

BACKGROUND

4. The port industry plays an important role in protecting our national security and economy. The global digitalization trend and recent policies and regulations require ports to face new challenges regarding information and communication technology. Ports tend to rely more on technologies to be more competitive, comply with some standards and policies and optimize operations. This brings new challenges in the area of cybersecurity, both in the Information Technologies (IT) and Operation Technologies (OT).

5. Cyber criminals are targeting the industry at unprecedented rates, and cyber disruptions – whether from an attack or from an accident – can have far-reaching consequences. The maritime industry must more focus on protecting human life, maritime assets, and the marine environment from cyber-related incidents.

6. The nature of ports is characterized by depending on data systems, massive volumes of cargo handling and passengers, high valued and immense number of transactions, as well as number of stakeholders involved. Sometimes, non-transparent ownership of goods end equipment makes ports particularly vulnerable to cyber threats.

7. Port Facility Operators are incredibly diverse in size and complexity, and the safeguards necessary to protect one facility's cyber systems against attack and disruption may not be practicable for another's. Therefore, the Designated Authority (DA) recommends port facilities to take a tailored approach that incorporates cyber risks into existing risk assessment and management processes, allowing port facilities to decide whether and how to mitigate its unique risks.

8. The loss, or compromise, of one or more of the assets (buildings, linear infrastructure, plant and machinery, and information and communications systems) has the potential to impact upon port efficiency, security, health and safety of port personnel.

9. Greater reliance on digitization, integration, automation and network-based systems has created an increasing need for cyber risk management in the shipping industry.

10. 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).

11. 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)

12. Pursuant to the IMO Resolution MSC.428(98), maritime cyber risk management should be incorporated into existing risk management processes and security management practices established by the IMO. Port Facilities are required to appropriately address cyber risks in the Port Facility Security Plans no later than the first annual audit after 1 January 2021.

13. The DA considers the International Ship and Port Facility Security (ISPS) Code as an integral part of emergency preparedness as well as compliance with SOLAS Convention in a Port Facility Security Plan.

CYBER RISK MANAGEMENT

14. 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.

15. Cybersecurity not only prevents hackers from gaining access to systems and information, but also addresses the maintenance, integrity, confidentiality and availability of information and systems, ensuring business continuity and the continuing utility of cyber assets.

16. 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 port related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

17. 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.

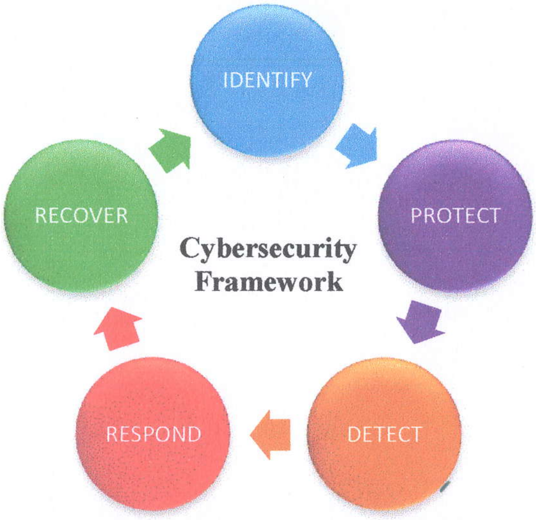

Fig: Cybersecurity Framework

IDENTIFY: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to port operations.

PROTECT: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of port 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 port operations or services impaired due to a cyber-event.

RECOVER: Identify measures to back-up and restore cyber systems necessary for port operations impacted by a cyber-event.

IDENTIFY	▪ Identify and diagram all critical Operational Technology (OT) control systems. ▪ Identify all Information Technology (IT) assets, including computer systems and services, that the company relies on. This includes those hosted shore-side, on vessels and by 3rd party providers. Identify those computer systems and services that are critical to the operations of the port facility. ▪ Assign a person responsible for cyber risk management. Analyze the risk of OT and IT assets at least once a year. Assess the potential business impact of downtime and data loss. Prioritize those assets that are critical to port operations, such as those that impact employee safety, environmental safety and the ability of port facility to conduct business. ▪ Establish a cyber-risk management policy within the port facility's existing security system and integrate cyber into established risk assessment and training procedures. ▪ Identify any applicable legal and regulatory requirements regarding cybersecurity.

PROTECT	▪ Ensure all system users are appropriately trained and understand their responsibilities. Integrate cyber training into established training procedures in the PFSP. Training should include how to identify malicious phishing emails and the importance of protecting the integrity of physical controls and operational systems. Users should know where to report any possible cyber incident and understand their importance in the cyber risk posture of the port facility. ▪ Evaluate 3rd party access to port operation systems. Minimize or avoid any unattended 3rd party access, and if possible, have remote access initiated by port personnel. Change any default passwords from 3rd party supplied equipment. ▪ Ensure that all physical control systems are isolated. If physical control systems must be networked, enforce network segmentation and strictly control local network and internet traffic. ▪ Physically block access to OT access points not protected by logical means (i.e., software safeguards). ▪ Use unique usernames and passwords for accounts to access computer systems. ▪ Apply system, security and application updates on the systems regularly, including procedure for verifying and applying updates. ▪ Apply protective technical security controls where applicable to computer systems. Consider a "defense-in-depth" approach whereby multiple layers of security controls are in place to reduce the risk when individual controls fail.
DETECT	▪ Myanmar Computer Emergency Response Team (MMCERT) has been established to receive information and reports about current cyber threats. Consult with Myanma Port Authority. ▪ Monitor and log network egress points and user logons for computer systems. Periodically audit computer system logs to look for unauthorized access or suspicious activity. ▪ Encourage port personnel to report any suspicious behavior or activity, as well as any unauthorized access to critical OT and IT systems and functions. ▪ Periodically scan critical computer systems for vulnerabilities.
RESPOND	▪ Assign a person responsible for responding to cyber incidents. Develop a response plan for critical OT and IT systems, indicating who inside the port facility and external to the port facility should be communicated with, and how that communication will occur. ▪ Incorporate lessons learned from post-incident evaluations into risk mitigation activities and updates to the response plan. ▪ Periodically test response plans using tabletop exercises.

RECOVER	▪ Assign a person responsible for system and data recovery planning. Identify and document data losses and how much downtime are tolerable by the systems. Identify any legal or regulatory requirements for reporting cyber incidents. ▪ Periodically test recovery plans using tabletop exercises. ▪ Identify any external assistance required for recovery efforts. Rely on subject matter experts, industry peers and the DA as needed. ▪ Consider to have an insurance plan to cover cyber risk incidents. Consult with insurance companies who can provide resources for both responding to and recovering from cyber incidents as part of their policies. ▪ Incorporate lessons learned from post-recovery evaluations into the recovery plan. ▪ Share information and lessons learned with counter-parts and industry peers.

18. Port Facilities are encouraged to develop strategies and standards against cyber-threats, to review the identified risks to its ports, personnel and the environment and to establish appropriate safeguards to ensure that maritime cyber risks are appropriately addressed, and that the five functional elements stated in para 17 have been incorporated into their risk management framework.

MARITIME CYBER RISK MANAGEMENT TRAINING

19. The following trainings are required for shore-based personnel:

    (a) Security training for port facility security officers (IMO Model Course 3.21)

    (b) Security Awareness Training for port security personnel with designated security duties (IMO Model Course 3.24); and

    (c) Security Awareness Training for all port facility personnel (IMO Model Course 3.25).

20. The DA also considers that cybersecurity trainings are specialized components of overall security training. The following cybersecurity training programme may be available upon request:

    (a) Maritime Cybersecurity Awareness Training

    (b) Maritime Cybersecurity Training for port operators

    (c) Advanced Cybersecurity Training for Administrators

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

ADDITIONAL GUIDANCE

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

(a) 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).

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

(c) Good Practice Guide Cyber Security for Ports and Port Systems. Published by Institution of Engineering and Technology, London, United Kingdom.

(d) Port Cybersecurity: Good practices for cybersecurity in the maritime sector. Published by European Union Agency for Cybersecurity (ENISA).

CONTACT

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

Email: sse@dma.gov.mm

24. 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/

9/10/20

Soe Naing
Director General