INTLREG

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

2021

4770 Biscayne Boulevard 800
Miami, Florida 33137, USA

CONTENTS

1. **INTRODUCTION**.....3
2. **GENERAL**.....4
3. **ELEMENTS OF CYBER RISK MANAGEMENT** 7
4. **BEST PRACTICES FOR IMPLEMENTATION OF CYBER RISK MANAGEMENT** 8
5. **CYBER RISK MANAGEMENT APPROACH AS IN THE GUIDELINES**. 9

1. INTRODUCTION

Maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, resulting in shipping – related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised. The purpose of these guidelines is to improve the safety & security of seafarers, the environment, the cargo and the ships.

Shipping is relying increasingly on digital solutions for the completion of everyday tasks. The rapid developments within information technology, data availability, the speed of processing and data transfer present Ship-owners and other players in the maritime industry with increased possibilities for operational optimization, cost saving, safety improvements and a more sustainable business. However, these developments to a large extent rely on increased connectivity often via internet between servers, IT systems and OT systems, which increases the potential cyber vulnerabilities and risks.

Risk management is fundamental to safe and secure shipping operations.

Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitization, integration, automation and network-based systems has created an increasing need for cyber risk management in the shipping industry. Approaches to cyber risk management will be company & ship specific but should be guided by relevant national, International, flag state regulations and guidelines.

Recognizing the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, IMO Resolution MSC.428(98) and guidelines on Maritime Risk Management (MSC-FAL.1/Circ.3) was approved.

The Resolution stated that an approved SMS should address Cyber Risk Management in accordance with the objectives and functional requirements of the ISM Code. All stakeholders to ensure that cyber risks are appropriately addressed in SMS no later than the first than the first annual verification of the companies DOC after 01-01-2021.

2. GENERAL

1.1 Background

1.1.1 Cyber technologies have become essential to the operation and management of numerous systems critical to the safety & security of shipping and protection of the marine environment. vulnerabilities created by accessing, interconnecting or networking these systems can lead to cyber risks which should be addressed. Vulnerable systems could include, but are not limited to:

Bridge systems:

- integrated navigation system
- Positioning systems (GPS, etc.)
- Electronic Chart Display Information System (ECDIS)
- Dynamic Positioning (DP) systems
- Systems that interface with electronic navigation Systems and propulsion/maneuvering systems
- Automatic Identification System (AIS)
- Global Maritime Distress and Safety System (GMDSS)
- Radar equipment
- Voyage Data Recorders (VDRs)
- Bridge Navigational Watch Alarm System (BNWAS)
- Shipboard Security Alarm Systems (SSAS).

Propulsion and machinery management and power control systems:

- Engine governor
- Power management
- Integrated control system
- Alarm system
- Bilge water control system
- Water treatment system
- Emissions monitoring
- heating, ventilation and air-conditioning monitoring
- damage control systems
- Other monitoring and data collection systems e.g. fire alarms.

Cargo Management system:

- Cargo Control Room (CCR) and its equipment
- Onboard loading computers and computers used for exchange of loading information and load plan updates with the marine terminal and stevedoring company
- Remote cargo and container tracking and sensing systems
- Level indication system
- Valve remote control system
- Ballast water systems
- Reefer monitoring systems
- Water ingress alarm system.

Communication systems

- Integrated communication systems
- Satellite communication equipment
- Voice Over Internet Protocols (VOIP) equipment
- Wireless networks (WLANs)
- Public address and general alarm systems
- Systems used for reporting mandatory information to public authorities.

Access Control Systems

- Surveillance systems such as CCTV network
- Electronic “personnel-on-board” systems

Passenger or visitor servicing and management systems

- Property Management System (PMS)
- Ship management systems (often including electronic health records)
- Financial related systems
- Ship passenger/visitor/seafarer boarding access systems
- Infrastructure support systems like domain naming system (DNS) and user authentication/ authorization systems.
- Incident management systems.

Passenger facing networks

- Passenger Wi-Fi or Local Area Network (LAN) internet access, for example where onboard personnel can connect their own devices22
- Guest entertainment systems.

Core infrastructure systems

- Security gateways
- Routers
- Switches
- Firewalls
- Virtual Private Network(s) (VPN)
- Virtual LAN(s) (VLAN)
- Intrusion prevention systems
- Security event logging systems.

Administrative and crew welfare systems

- Administrative systems
- Crew Wi-Fi or LAN internet access, for example where onboard personnel can connect their own devices.

1.1.2 The distinction between Information Technology (IT) and Operational Technology (OT) should be considered. IT is focusing on use of data as information and OT focusing on the use of data to control or monitor physical processes. The protection of information and data exchange to be considered.

1.1.3 While these technologies and systems provide significant efficiency gains for the Maritime Industry, they also present risks to critical systems and processes linked to the operation of systems integral to shipping. These risks may result from vulnerabilities arising from:

- Inadequate Operation
- Integration
- Maintenance & design of cyber-related systems
- Intentional and unintentional cyber threats.

1.1.4 Threats are presented by malicious actions (e.g., hacking or introduction of malware) or by Unintended consequences of benign actions (e.g. Software Maintenance or User Permissions). In general, these actions expose vulnerabilities (e.g. outdated software or ineffective fire walls) or exploit a vulnerability in Operational or Information Technology. Effective Cyber Risk Management should consider both kinds of threat.

1.1.5 Vulnerabilities can also result from inadequacies in design, integration and / or maintenance of systems, as well as lapses in cyber discipline. Where vulnerabilities in Operational and / or Information technology are exposed or exploited, either directly (e.g. Weak passwords leading to unauthorized access) or indirectly (e.g. the absence of network segregation), there can be implications for Security and the confidentiality, integrity and availability of information. In addition, where Operational and / or Information technology vulnerabilities are exposed or exploited,

there can be implications for safety, particularly where critical systems (e.g., Bridge Navigation, or main propulsion systems) are compromised.

1.1.6 Effective cyber risk management should also consider safety and security impacts resulting from the exposure or exploitation of vulnerabilities in information technology systems. This can happen from inappropriate connection to Operational technology systems or from procedural lapses by operational personnel or third parties, which may compromise these systems (e.g., inappropriate use of removal media such as a USB memory stick).

1.1.7 Vulnerabilities also due to Operational technology systems that are no longer supported and / or that rely on obsolete operating systems or Operational technology systems that cannot be patched or able to run anti-virus due to type approval issues.

1.1.8 Vulnerabilities to ship equipment that is remotely monitored and accessed e.g., by the manufacturers or support providers. Also ships that interface online with shore side parties and other parties of the global supply chain. Same with ships, sharing of business critical, data sensitive and commercially sensitive data with shore-based service providers, including marine terminals and stevedores and also, where applicable, public authorities.

1.1.9 Vulnerabilities also occur due to frequently the automation system comprises of multiple sub-systems from numerous vendors that are integrated by shipyards with minimal regard to cyber issues. These rapidly changing technologies and threats make it difficult to address these risks only through technical standards. As such, these guidelines recommend a risk management approach to cyber risks that is resilient and evolves as a natural extension of the existing safety and security management practices. In considering potential sources of threats and vulnerabilities and associated risk mitigation strategies, a number of potential control options for cyber risk management should also be taken into consideration, including amongst others, management, operational or procedural & technical controls.

This necessitates robust approaches to Cyber Risk Management.

1.2 **Application**

1.2.1 These guidelines are primarily intended for all organizations in the shipping industry and are designed to encourage safety and security management practices in the cyber domain.

1.2.2 Recognizing that no two organizations in the shipping industry are the same, these guidelines are expressed in broad terms in order to have a widespread application. Ships with limited cyber-related systems may find a simple application of these guidelines will be sufficient, however ships with complex cyber-related systems may require a greater level of care and should seek additional resources through reputable industry and Government partners.

1.2.3 These Guidelines and recommendatory.

3. ELEMENTS OF CYBER RISK MANAGEMENT

a. Cyber risk Management means 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 the stakeholders.

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

c. Effective Cyber risk management should start at the senior management level. Senior management should embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanism.

d. Once an approach has been accepted to achieve above is to comprehensively assess and compare an Organizations current, and desired, cyber risk management postures. Such a comparison may reveal gaps that can be addressed to achieve the risk management objectives through a prioritized cyber risk management plan. This risk-based approach will enable an organization to best apply its resources in the most effective manner.

e. These guidelines present the functional elements that support effective cyber risk management. These functional elements are not sequential. They all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management 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.

f. These functional elements encompass the activities and desired outcomes of effective cyber risk management across critical systems affecting maritime operations and information exchange and constitute an ongoing process with effective feedback mechanisms.

g. Effective cyber risk management should ensure an appropriate level of awareness of cyber risks at all levels of an organization. The levels of awareness and preparedness should be appropriate to roles and responsibilities in the cyber risk management system.

4. BEST PRACTICES FOR IMPLEMENTATION OF CYBER RISK MANAGEMENT

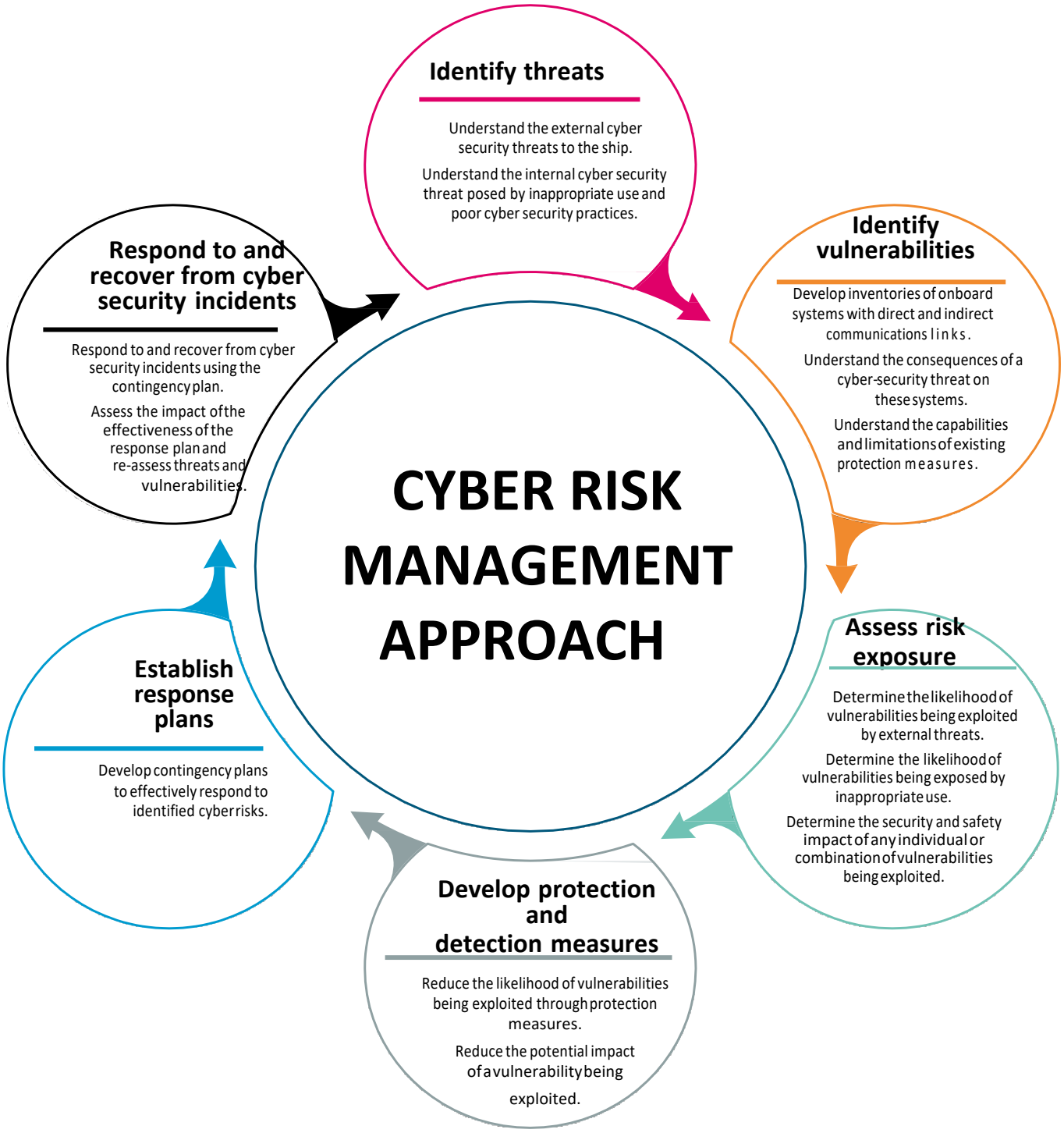
The approach to cyber risk management described herein provides a foundation for better understanding and managing cyber risks, thus enabling a risk management approach to address cyber threats and vulnerabilities. For detailed guidance on cyber risk management, users of these guidelines should also refer to member governments and flag administrations requirements, as well as relevant international and industry standards and best practices.

Additional guidance and standards may include, but not limited to below:

- The Guidelines on Cyber Security On board ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.
- 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 Electro Technical Commission (IEC).
- United States National Institute of Standards and Technology's Framework for improving Critical Infrastructure Cybersecurity (the NIST Framework).
- IMO Guidelines on Maritime Cyber Risk Management- MSC-FAL.1/Circ.3.
- IMO Resolution MSC.428(98) making clear that an approved SMS should take into account Cyber Risk Management when meeting the objectives and functional requirements of the ISM Code.

Reference should be made to the most current version of any guidance or standards utilized.

5. CYBER RISK MANAGEMENT APPROACH AS IN GUIDELINES



THANK YOU

For enquiries related to Maritime Cyber Security Management or implementation

or any other Intlreg Services contact us services@intlreg.org

4770 Biscayne Boulevard 800
Miami, Florida 33137, USA