THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

Produced and supported by

BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC)

BIMCO

CHAMBER OF SHIPPING OF AMERICA

dcsa

INTERCARGO
International Association of Dry Cargo Shipowners

InterManager

INTERTANKO

International Chamber of Shipping
Shaping the Future of Shipping

IUMI
International Union of Marine Insurance

OCIMF

SYBASS
SUPERYACHT BUILDERS ASSOCIATION

WORLD SHIPPING COUNCIL
PARTNERS IN TRADE

The Guidelines on Cyber Security Onboard Ships

Version 4

Contents

Introduction

The purpose of these guidelines is to improve the safety and security of seafarers, the environment, the cargo, and the ships. The guidelines aim to assist in the development of a proper cyber risk management strategy in accordance with relevant regulations and best practises on board a ship with a focus on work processes, equipment, training, incident response and recovery management.

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 shipowners and other players in the maritime industry with increased possibilities for operational optimisation, cost savings, 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[1], which increases the potential cyber vulnerabilities and risks.

The guidelines explain why and how cyber risks should be managed in a shipping context. The supporting documentation required to conduct a risk assessment is listed and the risk assessment process is outlined with an explanation of the part played by each component of cyber risk. This publication highlights the importance of evaluating the likelihood and threat in addition to the impact and vulnerabilities when conducting a cyber risk assessment. Finally, this publication offers advice on how to respond to and recover from cyber incidents.

Approaches to cyber risk management will be company and ship specific but should be guided by the requirements of relevant national, international and flag state regulations and guidelines. In 2017, the International Maritime Organization (IMO) adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management System (SMS). The resolution stated that an approved SMS should consider cyber risk management in accordance with the objectives and functional requirements of the (International Safety Management) ISM Code. It further encourages administrations to ensure that cyber risks are appropriately addressed in SMS no later than the first annual verification of the company's Document of Compliance (DoC) after 1 January 2021. The same year, IMO developed guidelines[2] that provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. As also highlighted in the IMO guidelines, effective cyber risk management should start at the senior management level. Senior management should embed a culture of cyber risk management into all levels and departments of an organisation and ensure a holistic and flexible cyber risk governance regime, which is in continuous operation and constantly evaluated through effective feedback mechanisms.

In addition to the IMO resolution, the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework Version 1.1 (April 2018) has also been taken into account in the development of these guidelines. The NIST Cybersecurity Framework assists companies with their approach to risk assessments by helping them understand an effective approach to manage potential cyber risks both internally and externally. As a result of applying the Framework, a "profile" is developed, which can help to identify and prioritise actions for reducing cyber risks. The profile can also be used as a tool for aligning policy, business and technological decisions to manage the risks. Sample framework profiles are publicly available for maritime bulk liquid transfer, offshore, and

1 Operational Technology (OT) systems include hardware and software which monitor and/or control physical devices, processes, and events. Information Technology (IT) systems include hardware and software which manages data (ie IT systems do not control physical devices, processes, or events).

2 MSC-FAL.1/Circ.3 on Guidelines on maritime cyber risk management.

passenger ship operations[3]. These profiles were created by the United States Coast Guard and NIST's National Cybersecurity Center of Excellence with input from industry stakeholders. The NIST's profiles can be used together with these guidelines to assist industry in assessing, prioritizing, and mitigating their cyber risks.

Guidelines are also available from other associations, such as the Digital Container Shipping Association's (DCSA) "DCSA Implementation Guide for Cyber Security on Vessels v1.0". The DCSA's guidelines are based on an analysis of version 3 of these guidelines and the NIST framework. While the target audience for DCSA's guidelines is the container industry, other segments of shipping may also find them worthwhile to read.

The International Association for Classification Societies (IACS) has issued a "Recommendation on Cyber Resilience (No. 166)". This recommendation consolidates IACS' previous 12 recommendations related to cyber resilience (Nos. 153 to 164) and applies to the use of computer-based systems, which provide control, alarm, monitoring, safety or internal communication functions that are subject to the requirements of a classification society. The IACS recommendation applies to newbuild ships only but can also serve as guidance for existing ships. In due course, IACS is expected to develop Unified Requirements, which will also apply to newbuilds only. This publication is not intended to provide a basis for, and should not be interpreted as, calling for external auditing or vetting the individual company's and ship's approach to cyber risk management.

3 The NIST Framework Profiles for maritime bulk liquid transfer, offshore, and passenger operations can be accessed here: **https://www.nist.gov/cyberframework**.