BERMUDA MERCHANT SHIPPING GUIDANCE NOTICE

Cyber Security on Board Ships 2020-14

Application

Recognised Organisations, Ship Owners, Managers, Masters and IT Officers of Bermuda Registered ships to which the ISM Code applies

Summary

This notice is to inform Owners and Managers of Bermuda registered ships of the need to raise awareness of cyber risk threats and vulnerabilities in the shipping industry.

Cyber risks should be appropriately addressed within the Safety Management System no later than the first annual verification of the Document of Compliance after **1st January 2021**.

References

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

MSC-FAL.1/Circ.3 – Guidelines on Maritime Cyber Risk Management

MSC.1/Circ.1526 – Interim Guidelines on Maritime Cyber Risk Management [*Superseded by FAL.1/Circ.3*]

UK Department for Transport – Code of Practice Cyber Security for Ships

This Notice was issued on 27th October 2020.

1. Introduction

(1) Ships are becoming more and more complex and increasingly dependent on the extensive use of digital and communications technologies, even in equipment which would not normally be considered to be 'connected', such as switchboards and access control technologies.

(2) Poor cyber security has the potential to lead to significant reputational damage and financial losses or penalties, as well as undesired outcomes such as:

a. Physical harm to the system or the shipboard personnel or cargo – in the worst case scenario this could lead to a risk to life and/or the loss of the ship.

b. Disruptions caused by the ship no longer functioning or sailing as intended.

c. Loss of sensitive information, including commercially sensitive or personal data.

d. Permitting criminal activity, including kidnap, piracy, fraud, theft of cargo, imposition of ransomware.

2. Relevant Guidance

(1) Being mindful of the above, Resolution MSC.428(98) requires cyber risk management to be undertaken in accordance with the objectives and requirements of the ISM Code.

(2)Cyber risks should be appropriately identified, analysed and addressed within the Safety Management System no later than the first annual verification of the Document of Compliance after **1st January 2021**.

(3)It is recognised that no two companies are the same and ships with limited cyber-related systems may, after review of their systems and vulnerabilities, find simple application of the published recommendations sufficient, while ships with complex system requirements may require substantially increased mitigation of the identified risks.

(4) 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 and the UK Department of Transport issued Code of Practice "Cyber Security for Ships".

a. These provide actionable advice on:

i. Developing a cyber security assessment and plan to manage risk.

ii. Handling security breaches and incidents.

iii. Highlighting national and international standards used.

iv. The relationship to existing regulation.

b. These guidance documents are to be used with the Company's SMS and SSP for:

i. Risk management systems.

ii. Subsequent business planning.

3. Implementation

(1) Resolution MSC.428(98) requires cyber risks to be considered and anticipated through the ISM Code and for such an assessment to be completed and documented within the SMS by the first Document of Compliance verification after 1st January 2021.

(2) However the ISPS Code Part B, Paragraphs 8.3 and 8.4 also states that the Ship Security Assessment should address '*radio and communication systems, including computer systems and networks*'.

(3) It is recommended that review and assessment of a ship's cyber security risks be conducted in a similar manner as stipulated by the ISPS Code, as follows:

a. Companies perform a Cyber Security Assessment alongside and in conjunction with, the Ship's Security Assessment and this is incorporated into the Ship's Security Plan, or;

b. Companies perform a Cyber Security Assessment and use this as the basis for production of a separate Cyber Security Plan to stand alongside the Ship's Security Plan.

Note: In both situations the Safety Management System would need to make reference to cyber security being addressed in either the Cyber Security Plan or updated Ship's Security Plan to meet the requirements of Resolution MSC428(98).

Note: Any such document would be within the scope of the ISM Code and could be audited as part of the DOC and SMC audit.

Note: There is currently no requirement for the Cyber Security Assessment or CSP to be reviewed by this Administration, however, if the exercise resulted in large scale changes to the SSP this may need to be resubmitted to BSMA for review.

(4) The UK Department for Transport – Code of Practice Cyber Security for Ships provides detailed guidance on the content and format of the Cyber Security Plan and Cyber Security Assessment.

(5) When conducting the Cyber Security Assessment companies should be aware of the data collection, diagnostic and transmission arrangements that may be fitted to essential equipment by the manufacturer.

a. It is recommended that the Company begin a dialogue with engine, propulsion motor, switchboard, VDR and navigation equipment manufacturers as well as the manufacturers of other safety critical equipment to find out the potential for remote access to their equipment.

Note: Some equipment manufacturers may maintain remote access to their equipment to allow for diagnostics, fault finding and periodic upgrade capability. Such vulnerabilities, if not suitably protected could potentially lead to malicious control or damage.

(6) The requirements of Resolution MSC.428(98) are deliberately not prescriptive for the reasons detailed in 2.3 above, however, it is likely that these requirements will be further defined in the future as the industry and IMO better come to understand the risks.

4. Assessment

(1) At each DOC audit and each SMC audit after implementation of the requirements of Resolution MSC.428(98) the company and ship will need to demonstrate that *'cyber risks are appropriately addressed in safety management systems'.*

(2) The attending Bermuda auditor will look to ensure that the subject has been addressed and relevant cyber security risks considered and documented in some manner.

(3) Any mitigating measures defined by the company would be within scope of the ISM audit and could be reviewed by the attending auditor, with the potential for Observations or Non-Conformities to be awarded should non-compliance with company requirements be detected.