INTERNATIONAL MARITIME ORGANIZATION

E

MARITIME SAFETY COMMITTEE
109th session
Agenda item 7

MSC 109/7
16 September 2024
Original: ENGLISH
Pre-session public release: ☒

REVISION OF THE GUIDELINES ON MARITIME CYBER RISK MANAGEMENT (MSC-FAL.1/CIRC.3/REV.2) AND IDENTIFICATION OF NEXT STEPS TO ENHANCE MARITIME CYBERSECURITY

Cyber incident response planning

Submitted by INTERPORTPOLICE

SUMMARY

Executive summary:	Cyber incident response planning is an important aspect of cybersecurity. This document provides background information on cyber incident response planning and gives details of recently developed tools that will complement the recently updated maritime cyber risk management guidelines.
Strategic direction, if applicable:	2
Output:	2.8
Action to be taken:	Paragraph 14
Related documents:	MSC 108/20, MSC 108/WP.10 and MSC-FAL.1/Circ.3/Rev.2

Introduction

1 MSC 108 approved the draft revised *Guidelines on maritime cyber risk management* (MSC-FAL.1/Circ.3/Rev.3), ("the revised Guidelines") as set out in annex 1 to document MSC 108/WP.10 and agreed to forward them to the Facilitation Committee for its concurrent approval. The revised Guidelines contain high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The revised Guidelines also include functional elements that support effective cyber risk management[1].

2 The Guidelines refer to "maritime cyber risk" as "a measure of the extent to which Computer Based Systems (CBS) are 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.".

[1] See also https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

3 While the protective element of maritime cyber risk management is clearly of vital importance, it is only one part of the cybersecurity system. Once that protection has failed and a cyber attack or a cyber incident has taken place, the next key element is the response. From a technical viewpoint, this response will be focussed on fixing the problem, i.e. addressing the cause and getting the system back up and running.

4 However, there is also an operational element. Irrespective of what caused the failure to the cyber system, whether it was malicious, accidental or of unknown origin, the core operational work of the port, ship or system needs to continue while the problem is identified and potential solutions defined and where possible implemented.

Cybersecurity and Cyber Incident Response

5 Keeping operations running is part of the "cyber incident response". To support this, all personnel involved in the safety, security and emergency management of the port have a role to play in maintaining the ports' business as usual (BAU) operations. This includes port safety, security and emergency management personnel, port management and associated port facility security officers (PFSOs), law enforcement agencies as well as private security agencies. Potentially, all these personnel and their agencies have a role in preparing for, responding to and managing cyber incidents in their ports.

6 Identification and designation of port and ship "cyber response" personnel is vital. They should have clearly defined roles and responsibilities. This cadre of personnel should have appropriate cyber awareness training and, whilst these personnel are not expected to be experts on cyber incidents, per se, they do need to understand and manage the potential impacts of an incident on their communities and port operations. Knowing whom to engage when a cyber incident occurs and having plans in place to effectively address the impacts of an incident is central to the role of a designated cyber incident manager or team, regardless of hazard type.

7 It is important to understand the difference and relationship between "cybersecurity" and "cyber incident response". The United States Cybersecurity and Infrastructure Security Agency (CISA) defines cybersecurity as "the art of protecting networks, devices and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity and availability of information". The goal of cybersecurity is to stop or minimize disruptions. A cybersecurity programme is designed to both understand and address cyber risks across an enterprise and is composed of people and technologies that monitor, detect and, ideally, prevent incidents on an ongoing basis.

8 Even with the best cybersecurity programme in place, cyber incidents are always a risk. Therefore, it is imperative to have a cyber incident response plan (or annex to an existing plan) that enables organizations to act quickly. An effective and efficient response helps mitigate impacts and return services as soon as possible. Much of cyber incident response planning occurs before an incident occurs and in conjunction with a cybersecurity programme.

9 A cyber incident response plan may include measures to:

.1 ensure continuity of critical services;

.2 disseminate timely information to affected stakeholders regarding impacted services, restoration expectations and available support;

.3 efficiently exchange information with service owners/operators to enable rapid response and recovery efforts;

.4 mitigate additional cascading impacts by isolating the impacted system(s), if possible; and

.5 identify how the system was compromised and make the immediate changes to ensure vulnerabilities cannot continue to be exploited while containment and recovery efforts are ongoing.

The Federal Emergency Management Agency (FEMA) guidance

10 In November 2023, the United States Federal Emergency Management Agency (FEMA) in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), published their Planning Considerations for Cyber Incidents - Guidance for Emergency Managers ("the FEMA guidance").[2]

11 The FEMA guidance complements the National Institute of Standards and Technologies (NIST) Cybersecurity Framework, cited in paragraph 4.2.4 of MSC-FAL.1/Circ.3/Rev.2. The FEMA guidance addresses, inter alia, types of cyber incident, assessing cyber risks to inform prioritization and planning, emergency management roles and responsibilities, communication considerations, and offers conclusions. Its annexes provide:

.1 A six-step planning process for cyber incident response planning:

Step One: Form a Collaborative Planning Team
Step Two: Understand the Situation
Step Three: Determine Goals and Objectives
Step Four: Develop the Plan
Step Five: Prepare and Review the Plan
Step Six: Implement and Maintain the Plan;

.2 cyber incident identification and closing processes; and

.3 links to a wide range of information resources on cyber incident management, references, and training.

Recent guidance on cyber security

12 On 16 December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy.[3]

13 The United Kingdom's National Cyber Security Centre[4] and National Protective Security Agency have both issued recent guidance on aspects of cybersecurity, including guidance on network-connected security technologies, issued in July 2024.[5]

2 The FEMA guidance may be downloaded from: https://www.fema.gov/sites/default/files/documents/fema_planning-considerations-cyber-incidents_2023.pdf

3 For further details visit https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

4 For further details visit https://www.ncsc.gov.uk/

5 For further details visit https://www.npsa.gov.uk/network-connected-security-technologies-ncst-guidance

Action requested of the Committee

14 The Committee is requested to:

.1 note the information provided;

.2 recall that in approving the draft Guidelines, MSC 108 "authorized the Secretariat to effect any minor editorial corrections that may be required";

.3 consider including references to the EU and UK guidance in the revised Guidelines as an editorial correction;

.4 invite Member Governments and organizations in consultative status to bring the FEMA guidance to the attention of all stakeholders concerned; and

.5 request the Secretariat to include suitable guidance on cyber incident response and its management in future revisions to the *IMO Guide to Maritime Security and the ISPS Code*.