INTERNATIONAL MARITIME ORGANIZATION

E

MARITIME SAFETY COMMITTEE
110th session
Agenda item 7

MSC 110/7/3
11 April 2025
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

The need for specialized and stand-alone model courses

Submitted by Türkiye

SUMMARY

Executive summary:	This document provides information on the need for development of a specialized and stand-alone cybersecurity training as an IMO model course for designated officers who would be responsible in shipping companies, fleets, and ports for maritime cyber risk management based on existing and forthcoming IMO circulars/regulations/codes on cybersecurity. It particularly incorporates new considerations and updates in the revised *Guidelines on maritime cyber risk management* (MSC-FAL.1/Circ.3/Rev.3), emphasizing the introduction of new cybersecurity governance functions and enhanced definitions, such as Computer Based Systems (CBS).
Strategic direction, if applicable:	6
Output:	6.2
Action to be taken:	Paragraph 13
Related documents:	MSC 108/WP.10; MSC 109/22; HTW 11/3/1/Add.1; HTW 8/3/3/Add.1, HTW 8/3/4/Add.1; HTW 9/15 and MSC-FAL.1/Circ.3/Rev.3

Introduction

1 This document is submitted in accordance with the provisions of *Organization and method of work of the Maritime Safety Committee and the Marine Environment Protection Committee and their subsidiary bodies* (MSC-MEPC.1/Circ.5/Rev.5) and proposes a new model course in line with the invitation in paragraph 7.7.2 of document MSC 109/22 in order to enhance maritime cybersecurity and latest updates proposed in MSC-FAL.1/Circ.3/Rev.3 which has been approved by both Maritime Safety and Facilitation Committees, to address emerging cybersecurity challenges.

2 Existing IMO Model Courses for Company Security Officers (CSO), Port Facility Security Officers (PFSO), and Ship Security Officers (SSO) in HTW 9/15 represent a significant step toward aligning traditional security practices with emerging maritime threats. These efforts emphasize the growing importance of integrating modern security challenges, particularly in the realm of cyber risk management. A key focus is placed on safeguarding shipping and port operations against evolving cyber threats through a structured approach that includes identifying risks, implementing protective measures, detecting vulnerabilities, responding effectively, and ensuring recovery. However, the evolving complexity of cyber threats necessitates a separate specialized framework that addresses newly defined areas, particularly "Computer Based Systems (CBS)" and "Govern" function of cybersecurity outlined in MSC-FAL.1/Circ.3/Rev.3.

3 Integrating cybersecurity into ISPS model courses also has challenges in aligning with the foundational principles of the ISPS Code, which is primarily based on physical security measures and assessments. The ISPS framework aims to deter unauthorized access and physical sabotage through security surveys, inspections, and procedural safeguards. In contrast, cybersecurity focuses on the protection of CBS including IT and OT systems, data integrity, and the prevention of digital sabotage.

4 Simply incorporating cybersecurity elements into existing ISPS model courses for CSO (Model course 3.20), SSO (Model course 3.19) and PFSO (Model course 3.21) would not fully equip officers with the necessary skills to effectively manage cyber risks across shipping companies, ship fleets and ports. A more holistic, practical, specialized and separated training framework is needed to bridge this gap and enhance resilience against evolving digital threats.

Discussion

5 The CSO, SSO, PFSO training frameworks in Model course 3.20, Model course 3.19, and Model course 3.21, respectively, are primarily designed to address physical and procedural maritime security challenges under the ISPS Code. It lacks the technical depth and specialization needed to manage the complexities of cyber risks. Incorporating advanced cybersecurity concepts, such as those outlined in MSC-FAL.1/Circ.3/Rev.3, alongside traditional security subjects' risks overwhelming the ISPS model courses, diluting its effectiveness, and providing inadequate coverage of both areas. Moreover, MSC-FAL.1/Circ.3/Rev.3 specifically introduces the "Govern" function, enhancing existing risk management processes by clearly defining roles, responsibilities, and strategies. Effective governance practices require specialized cybersecurity knowledge and competencies significantly beyond traditional ISPS security training.

6 Stand-alone cybersecurity training programmes are essential to equip officers with the technical expertise and focused knowledge necessary in the functional elements of cyber risk management – Identify, Protect, Detect, Respond, and Recover, as defined in MSC-FAL.1/Circ.3/Rev.3 – and additionally Govern as newly defined by MSC-FAL.1/Circ.3/Rev.3, to address evolving cyber threats for both shipping and port operations. These stand-alone programmes would complement the ISPS Model courses by set forth common training framework for managing cyber risks for enhancing maritime security.

7 Unlike physical threats, cyber risks require knowledge in network architecture, software vulnerabilities, and response protocols areas that are fundamentally distinct from the ISPS operational framework. Therefore, there is a clear need for a stand-alone cybersecurity training programme.

Rationale for retaining separate cybersecurity training rather than revision of the ISPS model courses

8 The following provides a summary of the reasons why a stand-alone cybersecurity training programme should be established instead of revising ISPS Model Courses for CSO (Model course 3.20), SSO (Model course 3.19) and PFSO (Model course 3.21).

.1 Scope and depth of the cybersecurity challenges

The IMO *Guidelines on Maritime Cyber Risk Management* (MSC-FAL.1/Circ.3/Rev.3) put into focus those cyber threats and vulnerabilities go far beyond traditional security regimes. These threats target IT/OT systems defined in MSC-FAL.1/Circ.3/Rev.3 and newly defined Computer Based System (CBS) utilized by bridge systems, navigational systems, cargo handling systems, propulsion systems which are the main elements of critical operations on board ships and at ports. Being able to put into practice the high-level recommendations and functional elements of MSC-FAL.1/Circ.3/Rev.3 effectively could not be done by only being embedded cybersecurity themes to syllabus of ISPS Model Courses.

.2 Specialized knowledge requirements

Cybersecurity risk management involves intricate technical, procedural, and human factor considerations. Functional elements of effective cyber risk management – Govern, Identify, Protect, Detect, Respond and Recover (MSC-FAL.1/Circ.3/Rev.3) – require specialized training in the areas of risk assessments, network segmentation, access controls, incident response protocols, cybersecurity strategies and business continuity. These are very specialized skills well beyond the remit of conventional CSO, SSO and PFSO responsibilities, which focus on physical security and compliance with the ISPS Code.

.3 Maritime cyber risk management complexity

The dynamic and evolving nature of cyber threats would probably require continual updating of the training programmes, in keeping with international standards such as ISO/IEC 27001, the NIST Cybersecurity Framework 2.0, and the IACS Recommendations on cyber resilience explicitly mentioned in MSC-FAL.1/Circ.3/Rev.3. Incorporating all these standards into CSO, SSO and PFSO Model Courses curriculum which have already been comprehensive and make it dynamic for cybersecurity risk management, poses the risk of undermining both cybersecurity and traditional security training.

.4 Alignment with international standards

The guidelines on cyber risk by IMO and industry recognition of cybersecurity as a stand-alone risk domain underline the need for a dedicated course ensuring at least alignment with these international standards, so maritime organizations are compliant and resilient against ever-evolving cyberattacks.

.5 Impact on operational resilience

Increasing dependence on digitalization and automation in shipping operations means proactive protection of systems against cyber incidents, as indicated in MSC-FAL.1/Circ.3/Rev.3. Specialized training programmes could more effectively prepare the maritime personnel to devise and implement robust strategies on cybersecurity customized for their unique operational contexts.

.6 Software and hardware supply chain security

MSC-FAL.1/Circ.3/Rev.3 emphasizes security-by-design principles and robust vulnerability handling throughout the lifecycle of CBS products. Specialized training must therefore cover management of cybersecurity risks related to procurement, maintenance and lifecycle of maritime equipment and software.

.7 Incident reporting and information sharing

Training should include systematic cyber incident reporting and communication strategies as critical components for enhancing maritime domain awareness and collective resilience.

.8 Integration into business continuity plans

Cybersecurity training should explicitly include modules to ensure effective integration of cyber risk management into existing business continuity and disaster recovery frameworks.

.9 Regular cybersecurity drills and exercises

Hands-on cybersecurity drills and exercises must be an essential element of practical training, differentiating clearly from ISPS physical security training methods.

.10 Continuous updating and adaptation

The training framework should be inherently flexible and regularly updated, reflecting the evolving nature of cyber threats, technological advances, and industry best practices.

.11 Course duration

This initiative, however, brings forth significant challenges related to the practicalities of course delivery and engagement by participants, specifically given the increased training duration that these updates have necessitated. Currently, the majority of CSO, SSO and PFSO model course training addresses physical and procedural security measures under the ISPS Code and is generally provided over a period of three to five days. Incorporating comprehensive cybersecurity subjects as outlined in MSC-FAL.1/Circ.3/Rev.3 would require coverage of the following areas and should be integrated into "Knowledge, Understanding and Proficiency" of CSO, SSO and PFSO Model Courses. The proposed integration would extend the courses' duration by approximately 3.5 to 4.5 days, resulting in an overall courses' length of eight to ten days. This substantial increase presents several operational and logistical challenges, including:

.1 Increased costs

Extended use of training facilities, additional resources, and longer instructor fees would raise costs for both the training providers and trainees.

.2 Participant availability

Senior officers, who are often the course participants, may struggle to arrange extended absences from their operational duties.

.3 Reduced focus

Incorporating cybersecurity into the CSO, SSO and PSFO's traditional responsibilities could dilute the depth and quality of coverage for both domains.

.12 The qualifications of instructors

According to staff requirements in SSO Model Course 3.19, the instructor in charge of the course should have adequate experience in maritime security matters and should have knowledge of the requirements of chapter XI-2 of the 1974 SOLAS Convention, as amended, the ISPS Code, and security-related provisions of the STCW Code, as amended. It is also recommended that instructors should either have appropriate training in or be familiar with instructional techniques and training methods. According to the CSO Model Course 3.20 staff requirements, instructors should have completed the CSO Model Course 3.20 or, alternatively, possess adequate experience in maritime security matters. Additionally, it is recommended that instructors either have appropriate training in or be familiar with instructional techniques and training methods. According to PFSO Model Course 3.21 staff requirements, instructors should be an experienced PFSO who has successfully completed the PFSO course or, alternatively, have substantial experience in port security operations and sound knowledge of the requirements of SOLAS chapter XI-2 and ISPS Code. However, most current CSO, SSO and PFSO instructors are trained primarily in ISPS Code-related physical security and lack the necessary depth of knowledge and hands-on experience to effectively teach cyber risk management content. When incorporating cybersecurity risk management frameworks and functional requirements into the curriculum for all three model courses, the qualifications of existing instructors fall short of meeting the unique demands of this specialized and rapidly evolving field. Instructors that are defined in these model courses' frameworks would not be able to provide the required expertise, as their training and experience are based on traditional maritime security under the ISPS Code, which does not encompass the technical and dynamic aspects of cybersecurity Accordingly, the qualifications of instructors, who are able to transfer the requirements of MSC-FAL.1/Circ.3/Rev.3 to their audience, should have a maritime related background with expertise on both the ISPS Code and specialized technical knowledge of cyber risk management frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, and IACS Recommendations, along with experience in cybersecurity tools and practices, including threat modelling, penetration testing, and incident response, to adequately address the potential threats and vulnerabilities associated with CBS systems including IT/OT systems, integration, and automation.

.13 Furthermore, cybersecurity is a highly technical and rapidly evolving field, requiring instructors to possess specialized qualifications and experience in cyber risk management. As such, it would be impractical to attempt to revise the CSO (Model course 3.20), SSO (Model course 3.19) and PFSO (Model course 3.21) model courses without it compromising the quality and effectiveness of both security areas. The only way to bridge this skills gap is by establishing a comprehensive stand-alone cybersecurity training programme led by certified instructors.

Proposals

9 As expressed in paragraphs 5 to 7 of this document, Türkiye advocates for the development of a specialized and stand-alone cybersecurity training as an IMO model course to designated officers, who can also be a new defined officer such as digitalization officer. The designated officer would be responsible in shipping companies, fleets and ports for maritime cyber risk management based on existing and forthcoming IMO circulars/regulations/codes about cybersecurity and aligning with IACS UR E26 and E27 standards and other related developments on the maritime cyber risk management for ships, shipping companies and ports.

10 By adopting this approach, IMO would ensure that cybersecurity measures are not only integrated into existing security structures but are also tailored to address the unique challenges posed by cyber threats in maritime operations. This comprehensive strategy will better prepare the industry to manage cyber risks and protect global maritime assets effectively.

11 Türkiye invites the Committee to consider this proposal for a differentiated approach to cybersecurity training, which will significantly enhance the industry's preparedness and response capabilities in the face of evolving cyber threats.

12 Türkiye proposes to set up a review and course developer group for the development of the stand-alone cybersecurity model course in alignment with IMO's framework.

Action requested of the Committee

13 The Committee is invited to consider the proposal in paragraph 12 and take action, as appropriate.