ISM Technical Notice NO 30/2020

Dated: 11.11.2020

SUBJECT:

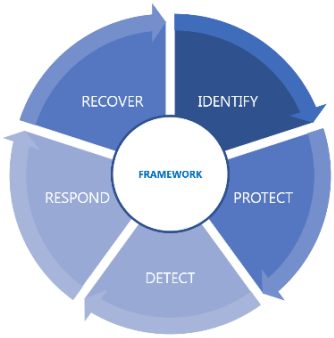
ISM CYBER SECURITY: BE PREPARED

The IMO has identified **cyber security as a risk to be addressed in safety management systems** and the handling of the risks are to be **verified in audits from 1 January 2021 onwards**.

Company plans and procedures for cyber risk management must be aligned with existing security and safety risk management requirements contained in the ISPS and ISM Codes as included in company policies. Requirements related to training, operations and maintenance of critical cyber systems should also be included in relevant documentation on-board.

The IMO Maritime Safety Committee (MSC) adopted Resolution MSC.428(98) on *Maritime Cyber Risk Management in Safety Management Systems* in June 2017. The resolution states that an approved safety management system should include cyber risk management in accordance with the objectives and requirements of the ISM Code, **no later than the first annual verification** of a **company's Document of Compliance** after **1 January 2021.**

Based on the recommendations in MSC-FAL.1/Circ.3, *Guidelines on maritime cyber risk management*, the resolution confirms that existing risk management practices should be used to address the operational risks arising from the increased dependence on cyber enabled systems. The guidelines set out the following PDCA process that can be taken to support effective cyber risk management:



1. **Identify**: Define the roles responsible for cyber risk management and identify the systems, assets, data and capabilities that, if disrupted, pose a risk to ship operations.
2. **Protect**: Implement risk control processes and measures, together with contingency planning to protect against a cyber incident and to ensure continuity of shipping operations.
3. **Detect**: Develop and implement processes and defences necessary to detect a cyber incident in a timely manner.
4. **Respond**: Develop and implement activities and plans to provide resilience and to restore the systems necessary for shipping operations or services which have been halted due to a cyber incident.
5. **Recover**: Identify how to back-up and restore the cyber systems necessary for shipping operations which have been affected by a cyber incident.

Cyber Risk Management (CRM) means the process of identifying, analyzing, assessing and communicating cyber-related risk and avoiding, transferring or mitigating this risk to an acceptable level.

IMO specifies that effective CRM should consider the safety and security impacts resulting from the exposure or exploitation of cyber vulnerabilities in both information technology (IT) and operational technology (OT) systems.

Operators should proceed with the following:

First, ship owners must define the high-level structure of their cyber security policy by developing a complete inventory of at-risk systems. This should include onboard and offshore systems, Operation Technology (OT) and Information Technology (IT) and equipment. This allows owners to gain a comprehensive understanding of all systems, in order to assess their risk criticality.

Ships should then undergo a cyber risk analysis that assesses threats and vulnerability, as well as the impact of exploitation of IT and OT systems on cyber security. Experts can then determine relevant risk, evaluate equipment surface of attack and consider mitigation measures that have been or should be applied onboard.

Once this is done, owners can develop a set of policies and procedures for cyber risk management that is tailored to their vessel and its equipment. This policy should address onboard cyber safety management rules, define the roles and responsibilities of personnel, include crew training activities and provide crisis management strategies.

Other guidance and standards

Guidelines on Cyber Security on board Ships issued by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, OCIMF, IUMI and WORLD SHIPPING COUNCIL.

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 Electrotechnical Commission (IEC).

United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).

Operators should also consult the flag states for any cyber security information on their web sites.