Maritime Cyber Security

- Preparation for the (cyber) emergency
- Effective cyber risk management is necessary
- German flag supports shipping companies
- FAQs

Preparation for the (cyber) emergency Cyber security becomes increasingly important for maritime shipping as an important part of the logistics chain. At the latest since the attack with the malware "NotPetya" in 2017 – which alone caused damage of several hundred million euros to the Maersk shipping company – it has become clear that the extent of cyber attacks in maritime shipping could be immense. Such attacks, for example on the electronic navigation system or the propulsion system on board, could even lead to the total loss of ships.

The International Maritime Organization IMO has recognized the importance of cyber security and calls on shipping companies to protect themselves against cyber risks (IMO resolution MSC.428(98)). The companies need to develop effective measures to protect against cyber attacks and integrate these into their existing ISM systems.

Effective cyber risk management is necessary How can shipping companies effectively protect themselves against cyber attacks? By first identifying, analyzing and evaluating possible cyber risks in order to take subsequent concrete measures to reduce these risks on board and on shore. The aim of this cyber risk management is to make ship operations more resilient and to provide comprehensive protection against cyber attacks.

In practice, the four-stage model for cyber risk management has proven itself for shipping companies:

- Check
Which cyber risks are associated with my ship operations?

- Evaluate
Are my current measures sufficient or are further measures necessary?

- Implement
Determine and implement further appropriate technical, organizational or personal measures

- Analyze
Measures to avoid or reduce cyber risks are to be checked for effectiveness on a regular basis.

From the first ISM office audit after 1 January 2021 at the latest, shipping companies must prove to their flag state administration that they have assessed cyber risks and have implemented suitable protective measures.

(back to top)

German flag supports shipping companies The German Flag State Administration supports the shipping companies in developing holistic approaches to cyber risk management on shore and on board their German-flagged ships. BG Verkehr, the BSH and the Federal Office for Information Security (BSI) provide practical tips on cyber security in their "ISM Cyber Security" circular. As a minimum, they recommend the so-called IT-Grundschutz Profiles of the BSI for shore operations and ship operations. These sample protection profiles contain specific recommendations for protective IT measures on board and ashore.

(back to top)

FAQ Maritime Cyber Security

Do shipping companies have to submit cyber risk documents to BG Verkehr for review?

No, the implementation of cyber risk management in a shipping company is part of the external ISM audits.

What do the two terms "IT" and "OT" mean?

The term "IT" includes information technology and networks on board such as personal computer, server, wifi, internet, telephone.
The term "OT" (Operational Technology) refers to systems on board such as radar, ECDIS, GNSS, engine control, sensors and alarms.

Does the company's internal auditor have to be an IT specialist?

No, the company's internal auditor checks the implementation of the Safety Management System (SMS) and not the functionality of IT and OT systems.

Do shipping companies have to introduce a stand-alone ISO management system for cyber protection?

No, an independent cyber management system (such as ISO 27000) is not absolutely necessary. Implementation within the shipping company's Safety Management System (SMS) is sufficient. However, depending on their type and size, shipping companies can decide to introduce a separate certification such as ISO 27000. The latter meets the IMO requirements for cyber risk management (IMO Resolution MSC.428(98)) if the certified system is integrated into the shipping company's safety management system.

What is the minimum content of a cyber emergency plan?

A cyber emergency plan includes:

- tasks to be initiated from the moment an incident is detected (reacting to cyber incidents and their consequences - no preventive tasks),
- measures to restore (backup & restore),
- emergency contacts, and
- reporting chains including the "shore" emergency response team.