ISM - Cyber security

Maritime Safety Committee

In June 2017 the 98th session of the Maritime Safety Committee (MSC) approved MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management. This circular to ship owners still remains non-mandatory. The MSC 98 also adopted Resolution MSC.428 (98) Maritime Cyber Risk Management in Safety Management Systems (SMS).

Resolution MSC.428 (98) affirms that an approved SMS should take into account cyber risk management in accordance with the objectives and functional requirements of the International Safety Management (ISM) Code. The objectives of the ISM Code include the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment. Cyber risks should be appropriately addressed in a SMS no later than the first annual verification of the company's *Document of Compliance* that occurs after 1 January 2021.

What is cyber risk?

Cyber risk can be represented as a threat or vulnerability resulting from either a computer or software hack for the purpose of theft, disruption or damage. For example out of date software on a computer or website may leave it vulnerable to intrusion or exploitation. A further example would be a victim responding to fraudulent emails that request for unauthorised payments and/or changes in payment details.

If a company becomes a victim of cyber-crime it could be affected financially both with the cost of fixing the issue and the theft of funds. Both issues could result in operational disruption and reputational damage impacting specifically on consumer confidence.

Limiting the chances of a cyber attack

Companies should not only be aware of external cyber threats but also those that can occur internally. Procedures, rules and training should be put into place to limit the opportunity for cyber-attacks to occur. These could be, but are not limited to:

- Ensuring virus protection is up to date and appropriate software updates applied.
- Ensure password protection is in place and updated regularly.
- Ensure there is a procedure in place to check files on external media such as USB sticks and drives, DVD's and CD's before connecting to electronic devices. In addition, emails must be scanned for suspicious attachments.

- Staff must be trained and routinely assessed on how to identify report and, if appropriate, manage a cyber risk incident.
- If it looks suspicious, STOP and check.

Maritime Cyber Security – webinar

The true extent of shipping’s cyber vulnerabilities remains uncertain and a ship owner’s readiness for cyber threats is of huge importance to keeping ships safe, secure and operable. It is with this in mind that the Shipowners' P&I Club hosted a webinar to assist Members in the mitigation of these risks, the aim being to help keep ships safe, secure and operable.

A recording of this webinar is available upon request.