Cyber risk on managed ships - IMO 2021 – be prepared!

By Robert Hodge, Director, ITIC

Earlier this year we wrote an article for *Ship Management International* on the low sulphur rules with the introduction of the International Maritime Organization (IMO) 2020. Now ship managers have yet another date to focus their attention on which is IMO 2021, cyber risk management.

Technologies are essential to the operation and management of a ship, there are numerous systems onboard and ashore that are critical to its safety and security. The IMO has recognised these technologies as being vulnerable to cyber risks and threats. Rather embarrassingly in October 2020 the IMO itself suffered what it called "a sophisticated cyberattack against the organisation's IT systems that overcame robust security measures" which took down their website and web-based services. Nonetheless they require, no later than a ship's first annual Document of Compliance (DOC) audit after 1st January 2021, that every Safety Management System (SMS) must include cyber risk management.

The DOC holder is the party who is ultimately responsible for ensuring the management of the cyber risks. As most ship managers are the DOC holder, they must carry out this role. One description of cyber risk management used by the IMO sees it as "the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders". So, it is no small task! Yet non-compliance may lead to the detainment of the ship.

The manager will have to carry out assessments to identify the risks on each vessel. There is no "one size fits all" assessment, as each vessel will have different systems and technology onboard. If an assessment is not carried out and a cyber-loss arises, the manager could be left exposed to a claim from the owner.

It is not just onboard risks that need to be assessed. The interface between the ship and shore is vital as many systems are linked. It is necessary, therefore, that the manager considers the cyber risks in their office, systems and employees, as this could be the route a hacker uses to penetrate the onboard systems. You must also think about how secure your physical office space is as well. Cyber criminals have been known to break into buildings to access IT systems from the "inside".

The manager should consider the cyber security arrangements of third parties appointed on behalf of the owner. It could be the ship agent who is employed to carry out the complex tasks of coordinating information with various parties at the port. The service providers and suppliers of products and equipment to the vessel should also be evaluated. It is clearly not possible to carry out detailed assessments on each, but the manager could ask to see if the ship agent has, for example, the FONASBA quality standard or a ship supplier has the Lloyd's Register cyber security certification ISO 27032.

ITIC insures ship managers on terms no more onerous than BIMCO Shipman 2009. As part of the effort to address cyber security risks, BIMCO has developed the Cyber Security Clause 2019 to be used in their agreements. This clause is intended to further raise awareness of the risk and to ensure there is a mechanism to have in place procedures and systems to minimise it. Managers may wish to consider including such a clause in their management agreement.

In the article on IMO 2020, we advised that is critical you have in place the plans, processes and documentation in the event the owner seeks to recover a loss from you. The exact same advice is again relevant for the upcoming IMO 2021 - you must be prepared. ●