SHIP MANAGEMENT INTERNATIONAL

Issue No 91 May/June 2021

Support. Our. Seafarers.

MARITIME Safety

The opportunity to build cyber resilience beyond regulation

By Julian Clark, Global Senior Partner at Ince

Cyber security has for some time now been viewed as one of the shipping industry's greatest challenges alongside other pressing topics such as decarbonisation and digitalisation. With cyber attacks and hackers becoming increasingly sophisticated by the day, the level of threat to the maritime industry is at an all-time high. Alarmingly, the ISP Association states that 92% of the estimated costs arising from a cyberattack are uninsured, which has serious risk management implications for maritime companies.

Given the complexity of the issue, however, many companies are struggling to keep up with the challenge and to fully appreciate its seriousness and the potential commercial, operational, reputational and legal risks that they face. Additionally, while the latest IMO cyber security regulations are absolutely necessary and a welcome step in the right direction, they do not go far enough and shipping companies remain increasingly exposed to cyber attacks and legal liability even when within adequate compliance levels.

The legal implications of cyber reguation and risk exposure

Beyond the financial and reputational damage that can result from cyber-attacks, the maritime community must be aware that legal consequences will be a key part of the aftermath of a cyber incident. If a vessel is cyber compromised, the companies involved will be forced to show the exercise of due diligence in order to protect themselves legally.

We can expect third parties to bring claims against vessel owners and operators arguing that there was a failure to make use of the cyber security protection systems available in the market. Discovery will be used to assess what real steps these companies had engaged in to ensure they were adequately protected. In the case of failure to have proper cyber protections in place, such fault will be directed against the actual owning entity rather than those directly responsible for the operation of the vessel.

If ship owners do not afford themselves of the systems available on the market that can provide the right protection against a cyber attack, this will expose them to the risk of significant damages claims. Additionally, if they have failed to adequately check and mitigate against the level of their vessels' exposure to cyber compromise, these omissions could amount to recklessness and give rise to a possibility to break the right to limitation, and even amount to unseaworthiness.

An opportunity for the shipping industry

While important for compliance and risk awareness purposes, the current IMO cyber security regulations only deliver a level one solution to a level four threat, so the risk for shipping companies is still too high even if they are compliant. Regulation can therefore be seen as an opportunity and an incentive to carry out a more ambitious and critically needed wider implementation of cyber protection mechanisms.

In tackling the issues that can arise from cyber attacks, there are a number of separate service elements available in the industry available for this purpose, but the shipping sector has long lacked an integrated, combined offering that brings together all the essential elements that an organisation needs to fully protect itself from cyber threats. In order to achieve this level of protection, the best option for maritime organisations is an integrated, fully comprehensive approach to cyber security.

In addressing this market need, we recently joined forces with Mission Secure - who are leaders in providing military grade cyber security for OT systems - to launch an industry-first integrated legal advisory, consultancy and technology implementation cyber security solution. This partnership allows us to provide both advisory and action to fully help protect companies beyond the current regulatory guidelines.

In order to successfully address the cyber security challenge, the shipping industry must understand the need to exceed compliance requirements and embrace the opportunity to buid more resilient, robust and effective cyber protection.

If ship owners do not afford themselves of the systems available on the market that can provide the right protection against a cyber attack this will expose them to the risk of significant damages claims

Julian Clark, Global Senior Partner at Ince