Cyber security

Modern technology has changed the way ships are operated. Whilst this technology has generally improved the efficiency and safety of ships, these improvements come at a price in the form of an increased vulnerability to cyber attack.

Richard Bell
Loss Prevention Executive
T +44 20 7680 5635
E richard.bell@ctplc.com

Introduction

The Standard Club, like many other maritime stakeholders, has paid close attention to cyber-related incidents in the industry in the past year and 2017 proved to be a significant year for cyber-related issues.

One of The Standard Club's recent initiatives was its joint sponsorship of FIDRA's Be Cyber Aware At Sea – Maritime Cyber Security film. This free film is designed to educate seafarers about the dangers associated with internet usage on board. At the time of writing, the Fidra film had received well over 100,000 views on Facebook and YouTube.

Probably the most famous maritime cyber event in 2017 was the 'NotPetya' ransomware attack. NotPetya caused disruption to many companies including AP Moller-Maersk. AP Moller-Maersk's commercial operations were interrupted, revenue was lost and the company was forced to overhaul its existing cyber security infrastructure. Another well-publicised event was the apparent Global Navigation Satellite System (GNSS) spoofing, which occurred in the Black Sea. The Standard Club has previously discussed this issue, whereby a GNSS is made to display false information deliberately without the knowledge of the user.

Fortunately, in this case, the GNSS position discrepancies were so large as to be obvious to the user.

Legislative developments

The International Maritime Organization's (IMO) Maritime Safety Committee has produced resolution MSC. 428(98) which was adopted on 16 June 2017. This resolution contains a recommendation for cyber risks to be addressed within safety management systems (SMS) no later than the first annual verification of the company's Document of Compliance after 1 January 2021. It encourages flag states to ensure that this is the case.

Key points of the resolution are:

- the need to raise awareness of cyber risk threats
- the need for stakeholders to expedite work towards safeguarding shipping for current and emerging threats
- a reference to the 'Guidelines on maritime cyber risk management' as providing high-level recommendations for maritime cyber risk management.

The IMO has released MSC FAL.1/Circ.3 'Guidelines on maritime cyber risk management'. These guidelines are intended to provide high-level recommendations to help safeguard shipping from existing and emerging cyber threats. The recommendations are designed to complement existing IMO safety and security management practices. Further information can be obtained from the 'maritime cyber risk' page of the IMO's website. In addition to the IMO's guidelines, Cyber Security on board Ships is another resource which is available for use. This publication was produced by a group of organisations, including BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.

Conclusion

2021 is still far away and shipowners/managers may think they have plenty of time to address cyber risks and comply with the new IMO resolution, but there is no room for complacency. Ship owners/managers should act now to develop and establish their cyber security infrastructure. This should not be just for compliance purposes but to protect their crews and assets from the very real threat of cyber interference. Effective action now could prevent an organisation from becoming another high-profile victim of a future cyber attack.