20 ESSEX STREET

BULLETIN

April 2018

Cyber-seaworthiness: the calm before the storm?

Karen Maxwell

Will we soon see claims for compensation resulting from cyber-attacks in the maritime sector? 2017 saw a significant stepping up of global cyber-crime; and there appears to be a growing understanding that the shipping industry is particularly vulnerable to attack. One of the most renowned cases occurred last June when the NotPetya ransomware closed down AP Moeller Maersk operations in LA, reportedly costing the company over USD300m in lost revenues, as well as requiring the company to rebuild or reinstall 4,000 servers, 45,000 laptops and 2,500 apps.

Any shipping transaction, and indeed any voyage, is dependent for its performance upon connected technologies which may be disrupted in any number of ways, ranging from fraudulent diversion of payments to attacks on vessel navigation systems or shore facilities. The risk is amplified by the fact that the transaction is likely to involve several parties and disparate systems, all situated in different jurisdictions. Add to this the increasingly sophisticated tools used by cyber-criminals, and the lack of any unified or harmonized regulatory system, and the potential for civil claims appears high.

Could failures in cyber-security render a ship unseaworthy? Modern ships, designed for efficiency, are vulnerable to attack. The increasing integration of IT and OT systems across vessel plant, cargo operations and navigation tools creates particular security risks. Although the more serious recent attacks have mainly involved shore facilities (usually as collateral damage in a wider attack, as was the case with Maersk and NotPetya), the possibility of attacks directed at or affecting vessels must be taken seriously. For example, vessels' navigational GPS, ECDIS and AIS systems are vulnerable to spoofing and jamming attacks: in 2017, it was reported that around 20 vessels in the Black Sea were showing incorrect GPS readings, probably as a result of a Russian cyber attack. In other incidents, the switchboard of a vessel calling at an Asian port was shut down by malware, meaning that there was no means of powering or controlling the propeller. The vessel was forced to remain in port until the situation could be remedied. Once a hacker has gained access to the network, the scope for disruption and damage may be significant.

One might imagine that unmanned vessels would be still more vulnerable – but, in fact, anecdotal evidence suggests that human error is very often the weak link. Crew members will usually bring on board their own mobile phones or other devices which are then connected to the vessel's network, providing an avenue by which malware can infect the entire vessel system. One reported example concerned a crew member's USB stick, which had been brought on board so that documents could be printed, but which resulted in the vessel's network becoming infected. Perhaps the only surprise is that there have not been more cyber attacks in the shipping sector – though, of course, the potential for reputational damage means that such attacks are almost certainly under-reported.

Unsurprisingly, the growth of cyber-crime and associated risks has spawned a fast-growing risk management industry, with the players vying to provide the most up to date and effective solutions. The industry itself has also sought to address the situation. The IMO has issued guidelines on maritime cyber risk management, and resolved in June 2017 to "encourage" administrations to ensure that cyber risks are appropriately addressed in existing safety management systems no later than 2021. However, the IMO guidelines are very high level. More detailed practical guidance is contained in the Guidelines on Cyber Security on board Ships, issued by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI, the United States National Institute of Standards and

Technology's Framework for Improving Critical Infrastructure Cybersecurity, and the British Department of Transport Cyber Security Code of practice for ships. Such documents provide at least a framework for managing the risk posed by cyber-attacks. Other related projects include the cyber incident information sharing platform established by CSO Alliance and Airbus; and the Liberian flag registry's cyber-security training programme.

Despite such efforts, it can only be a matter of time before cyber risks translate into actual claims against, and perhaps liability on the part of shipowners. Even though most standard form charterparties and bills of lading were drafted long before cyber-crime was even heard of, there is potential for a breach of contract. Failure to have in place adequate systems (including crew training) to address cyber-risks could certainly render a vessel unseaworthy. (Similar factors on the shore side could give rise to a finding that a particular port was unsafe for a vessel to call.) The problem faced by owners is that this is a relatively new, and rapidly developing, issue: there are no harmonized standards and no clearly established "best practice". Anecdotal evidence suggests, however, that lack of training or awareness may be key areas to consider: a 2017 IHS Fairplay survey identified lack of training as a key issue in this area, and the 2018 Futurenautics crew connectivity survey found that only 15% of crew members had received training, and only 49% were aware of cyber security guidelines. As against that, 47% had been on board a vessel that was infected with virus or malware. Such figures suggest that in any future claims, crew training may well form a significant area of inquiry. In the meantime, parties may wish to consider negotiating exclusions of liability into their contracts, where possible, and/or ensuring that their insurance sufficiently covers any potential liability.

Karen Maxwell

Karen practises in shipping, sale of goods, international trade, banking, private international law, arbitration and insurance. Recent advisory and arbitration work includes challenges to arbitration awards, shipbuilding disputes and guarantee claims. She writes and lectures widely on arbitration and private international law topics and is also a co-author of London Maritime Arbitration, published by Informa and now in its fourth edition.

For further information about this bulletin contact tmccombe@20essexst.com

LONDON
20 Essex Street London WC2R 3AL
Tel +44 (0)20 7842 1200
Fax +44 (0)20 7842 6770

SINGAPORE
Maxwell Chambers, #02-09
32 Maxwell Road, Singapore 069115
Tel (+65) 62257230
Fax (+65) 62249462

clerks@20essexst.com