CYBER RISK IN THE MARINE INDUSTRY

Marcus Baker, Marsh JLT Specialty leader for Global Marine and Cargo Practice, London, UK

Cyber-attacks and data theft are the threats considered most likely to occur in the marine industry within the next 10 years. They are also considered to be the third-most impactful issue, according to the Global Maritime Issues Monitor 2018 . Worryingly, it is also the issue the industry is least well prepared for. Given these concerns, cyber risk has become a board-level issue, with greater importance placed on mitigating the effects that cyber events could have on a company's safety, finances and reputation. The cyber threat landscape is constantly evolving, however. Attack surfaces are broadening, as companies throughout the value chain take increasing advantage of opportunities based on interconnectivity and automation. Constant vigilance is essential.

By 2020, 60% of all businesses with digital operations will have suffered major service failure related to breaches of security, Gartner estimates . Hacks are often not detected for several months from first inception: IBM calculated the mean time to identify a breach as 197 days, and the mean time to contain it a further 69 days . Companies that contained a break in security in less than 30 days saved more than US$1 million, compared with those that took more than 30 days to resolve the issue, IBM estimated.

Facing this complex, ever-changing cyber threat landscape requires a shift in mind-set. The maritime industry needs to take a strategic approach to protecting critical assets and business drivers. Once an organisation has sufficient knowledge of the most likely cyber risks, they can build a scalable security posture that can be continuously adapted to meet the changing risks. Let's look at some of these cyber risks in turn.

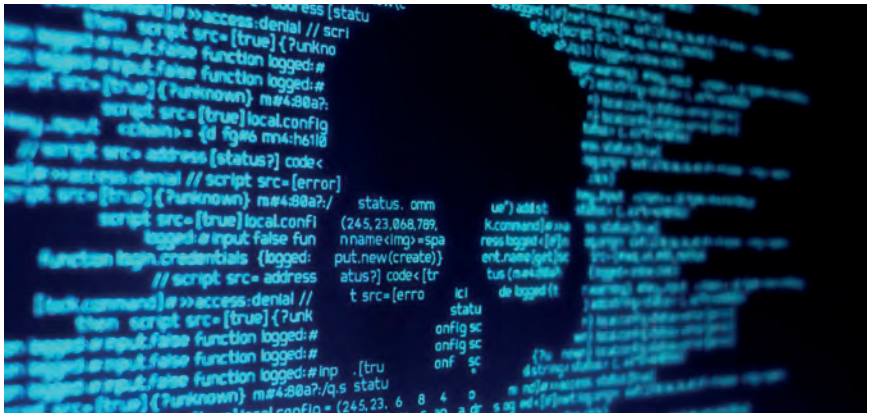
EVERYTHING CONNECTS

While the marine industry's use of interconnected systems has brought tremendous benefits – such as greater efficiency, cost savings, and monitoring of systems- it has also brought considerable risk.

Significant weaknesses have been identified in the cyber security of critical technology used for the operation of modern commercial cargo vessels. Global positioning systems (GPS), automatic identification systems (AIS) and electronic chart displays and information systems (ECDIS), are all essential aids to navigation in today's modern ships, but each has been identified as potentially vulnerable to a cyber-attack – potentially giving pirates the ability to monitor sources of sensitive information.

Meanwhile, wider internet connectivity is driving increased use of cheaper and more portable smartphone devices in the industry, which may expose users to increasingly sophisticated criminal groups. Criminals might manage to monitor communications between individuals, gaining hugely valuable information about goods, locations, and digital protection processes and could compromise expensive security systems. For example, a breach could occur if criminals learn that physical barriers are going to be undermanned at a particular time and location.

Vessels are particularly vulnerable to cyber security threats when third-party personnel gain remote access to undertake maintenance and security checks, or when crew connect directly to a ship's system



with devices such as tablets and memory sticks. Shipping companies also need to be aware of cyber threats from their own employees, who could strike back at the company if they are made redundant or bear a grudge against their employers.

In addition, employees could unknowingly expose the company to a cyber-attack and steps should be taken to train employees to recognise where cyber risks may stem from and how to prevent them. For example, phishing (also known as social engineering fraud) is a constant threat to the industry and refers to a variety of techniques used by fraudsters to deceive and manipulate victims into voluntarily performing actions which result in them giving out confidential information or transferring funds.

VULNERABLE SYSTEMS

Propulsion monitoring systems, cargo handling, container tracking systems and shipyard inventories are now all controlled using software to reduce costs and improve efficiency. However, the accessing, interconnecting, monitoring and networking of numerous shipping systems have created new cyber risks and previous events suggest these systems might be vulnerable to attacks or disruption.

For example, cyber-attacks on routing systems allow for the potential re-routing of cargo, enabling targeted trafficking and theft, causing considerable operational delays for ports and third-party logistics companies. Aside from disruption to services, there are inherent safety risks associated with cyber security through the compromise of computerised navigation and stability systems.

Pirates could hack a marine company's system, enabling them to target, track, board, and take specific cargo ships, offload the cargo and vanish before authorities can respond. For example, hackers working with a drug-smuggling gang infiltrated the computerised cargo tracking system of the Port of Antwerp to identify the shipping containers in which consignments of drugs had been hidden . The gang then drove the containers from the port, retrieved the drugs, and covered their tracks. This criminal activity continued for a two-year period, until it was stopped by police.

LOOKING AHEAD

While crewless, fully autonomous ships are yet to navigate global waters, but interest in the potential of this technology is growing due to a combination of rising transport volumes, growing environmental concerns and a shortage of experienced and qualified seafarers. Autonomous technology in shipping could possibly provide greater monitoring of vessel performance, plus cost reductions and reduced risk to human life.

If the relevant regulatory approvals are achieved and autonomous technology is successfully introduced, however, the traditional and emerging risks these vessels pose will need to be carefully considered and mitigated by ship operators.

Relying on automated systems could result in errors or system failure following an electrical or cyber derangement, which could have severe consequences. The system may detect an issue on board the ship, or an error or failure could cause sensors not to pick up on a danger or obstacle in the water. Safeguards and backup systems would need to be part of the overall design, in case primary systems fail or communications with the ship are interrupted.

Successful cyber-attacks against a ship operator or any party in the shipping industry inevitably lead to reputational damage for the victim and, potentially, the industry as a whole. In the current commercial climate of ferocious competition among maritime operators, a good reputation for prudent operations must be protected. Although many questions remain, it appears certain that cyber issues will stay at the forefront of the industry for the foreseeable future.

REFERENCES

i Global Maritime Issues Monitor 2018, produced by Global Maritime Forum, Marsh and IUMI, surveyed opinions of senior maritime stakeholders from more than 50 countries.

ii Gartner, "Gartner Says By 2020, 60 Percent of Digital Businesses Will Suffer Major Service Failures Due to the Inability of IT Security Teams to Manage Digital Risk", https://www.gartner.com/en/newsroom/press-releases/2016-06-06-gartner-says-by-2020-60-percent-of-digital-businesses-will-suffer-major-service-failures-due-to-the-inability-of-it-security-teams-to-manage-digital-risk

iii IBM Security, "IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses", https://newsroom.ibm.com/IBM-security?item=30567

iv BBC News. "Police warning after drug traffickers' cyber-attack," available at: http://www.bbc.com/news/worldeurope-24539417

ABOUT THE AUTHOR

Marcus Baker is Marsh JLT Specialty's leader for Global Marine and Cargo Practice and is responsible for the marine business lines globally, comprising marine cargo, marine hull, P&I, and liabilities. He was formally the Chairman of Marsh's Global Marine Practice and before that CEO for Marsh's Marine and Energy practice in EMEA. He has over 35 years' experience in the industry, travelling extensively globally, and has been involved in all aspects of global marine and energy insurance. As well as Head of the Global Marine and Cargo Practice, Marcus is a member of the Advisory Board for the Global Maritime Forum and also a member of Marsh's Leadership Council.

ABOUT THE ORGANIZATION

Marsh is the world's leading insurance broker and risk adviser. With over 35,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data driven risk solutions and advisory services. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy and people. With annual revenue over US$15 billion and 75,000 colleagues worldwide, MMC helps clients navigate an increasingly dynamic and complex environment through four market-leading firms: Marsh, Guy Carpenter, Mercer, and Oliver Wyman.

ENQUIRIES

Tel: +44 (0)20 7357 1780
Fax: +44 (0)20 7929 2705
Email: marcus.baker@marsh.com