Cyber hijack

by Henry Clack, *Associate, HFW*

As for all businesses, ransomware is a significant issue for the shipping industry. There have been a series of high-profile attacks on the sector in recent years. In 2021, Swire Pacific Offshore was reportedly the victim of a cyber attack. Whilst its fleet of roughly 50 vessels was not materially affected, the attack is understood to have caused a significant loss to the company. Historically, shipowners have viewed their ships as being relatively immune to these sorts of attacks as, due to their very nature, they have been 'air-gapped' from the rest of the owners' IT network. This is, however, no longer the case.

The software and hardware on board that monitors or controls the vessel's physical equipment (known as operational technology or OT) have increasingly been connected with the outside world. This equipment, which generally comprises computer systems that control engines, steering gear, pumps or valves, is now regularly linked to the outside world to allow for external monitoring by head office or third-party suppliers/manufacturers. Cybercriminals can exploit this vulnerability.

An increasingly attractive form of cyber crime

Ransomware exploits are relatively straightforward to execute. They can either be purchased on the dark web as software packages or be of a bespoke design for a unique target. The code can infiltrate and encrypt computer networks, locking employees and IT teams out of the system until a fee has been paid in exchange for its release. The recent growth in cryptocurrencies has provided perpetrators with an anonymous payment system, making it an increasingly attractive form of cybercrime.

Regarding the payment of ransoms, it is important to note that the victim may face legal issues if it makes payment without carrying out due diligence. Whilst the payment of ransoms is legal as a matter of English law, this is not always the case in other jurisdictions. Similarly, it should be borne in mind that transferring funds to terrorist organisations is illegal, and this is particularly problematic given that some groups are arguably politically motivated and/or state-sponsored. Insurers should also exercise caution as UK law includes a specific offence for insurers who fund ransom payments to a terrorist organisation.

Finally, ransomware victims could fall foul of sanction rules. In September 2021, the Office of Foreign Assets Control (OFAC; a financial intelligence and enforcement agency of the U.S. Treasury Department) issued an advisory notice with specific information relating to ransomware. The memo states that individuals may be "held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC."

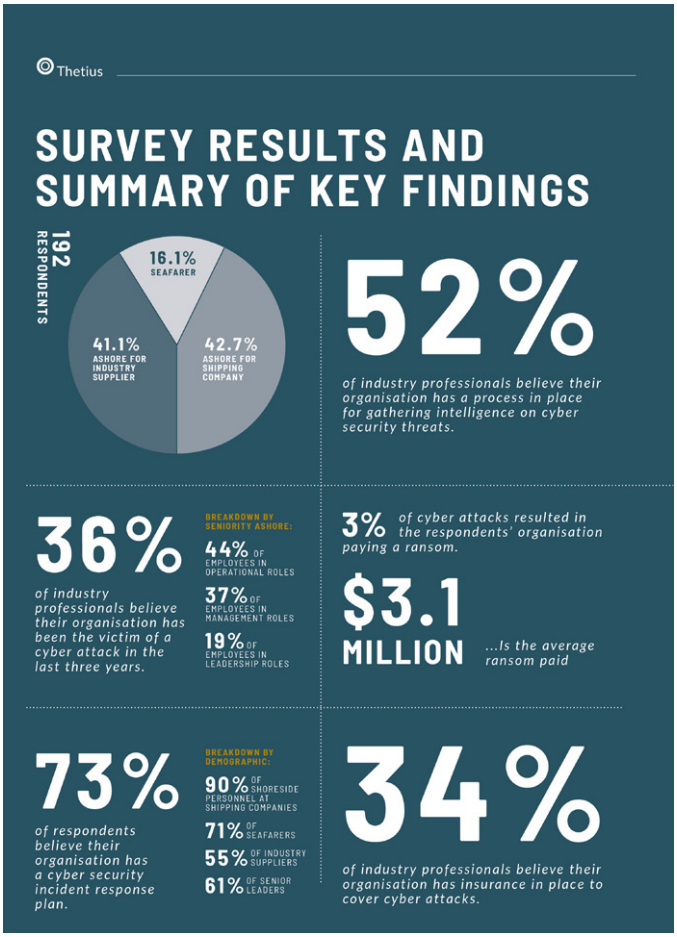
Reconnecting

HFW, CyberOwl and the maritime innovation agency Thetius have released ***The Great Disconnect***, a report which attempts to shed light on the cyber security readiness of shipping based on surveys and research interviews of more than 200 industry professionals.

Whilst the report deals with several cyber issues facing the shipping industry, the survey results were striking when it came to ransomware: 44% of industry professionals reported that their organisation had been the subject of a cyberattack in the last three years. Of those, 3% resulted in paying a ransom by the victim to the attacker, at an average cost of $3.1m.

The report makes four recommendations of practical measures for ship operators, industry suppliers, and wider stakeholders to take to reduce the risk of falling victim to these attacks.

First: set up a dedicated cyber security directorate within fleet operations that covers both IT and OT security. One of the most significant vulnerabilities uncovered during the research was the serious disconnect between senior leaders in organisations that operate ships, those responsible for the



security of IT systems, and those responsible for protecting OT systems. Taking a holistic approach to cyber security that includes both IT and OT systems alongside physical security is therefore critical.

Second: implement a comprehensive cyber incident training and drill programme. Everyone in an organisation, whether at sea or ashore, must understand what actions are required of them during a live cyber incident. The programme should be based on practical scenarios that reflect the actual setup and security posture of the organisation, its people, processes, and technology. Senior leaders in organisations should understand the decisions they will need to make during a cyberattack to enable their organisation to deliver the best response to minimise losses and disruption. They should have confidence that systems and processes have been put in place to ensure that the right information gets to the right people to make the right decisions quickly.

Third: develop minimum security standards for suppliers and partners. It was clear from the survey and research interviews that maritime suppliers work to a much less stringent cyber security standard than the ship operators they serve. On average, industry suppliers reported a 10% lower score than those who work for ship operators across all of the self-assessment questions asked in the survey. We recommend that all shipowners and operators create a cyber security standard that is incorporated into the procurement or counterparty due diligence processes. This can be designed as a supplier code of connection which sets a minimum cyber security standard for the supplier before they are permitted to connect to vessel systems or access ship data.

Lastly: conduct an urgent review of insurance policies and seek guidance on ransom payments. Only 35% of respondents to our industry survey confirmed that their organisation has insurance in place to cover cyber risks. Though many organisations may believe they are covered under existing policies, for many policies, there are blanketing exemptions they should be aware of. Further, even if cyber threats are not specifically exempted, the circumstances of an attack and the failures of organisations to address earlier failures and vulnerabilities identified in cyber security systems and processes could lead to denied claims.

These recommendations should go some way to reduce the risks facing the shipping industry. ■