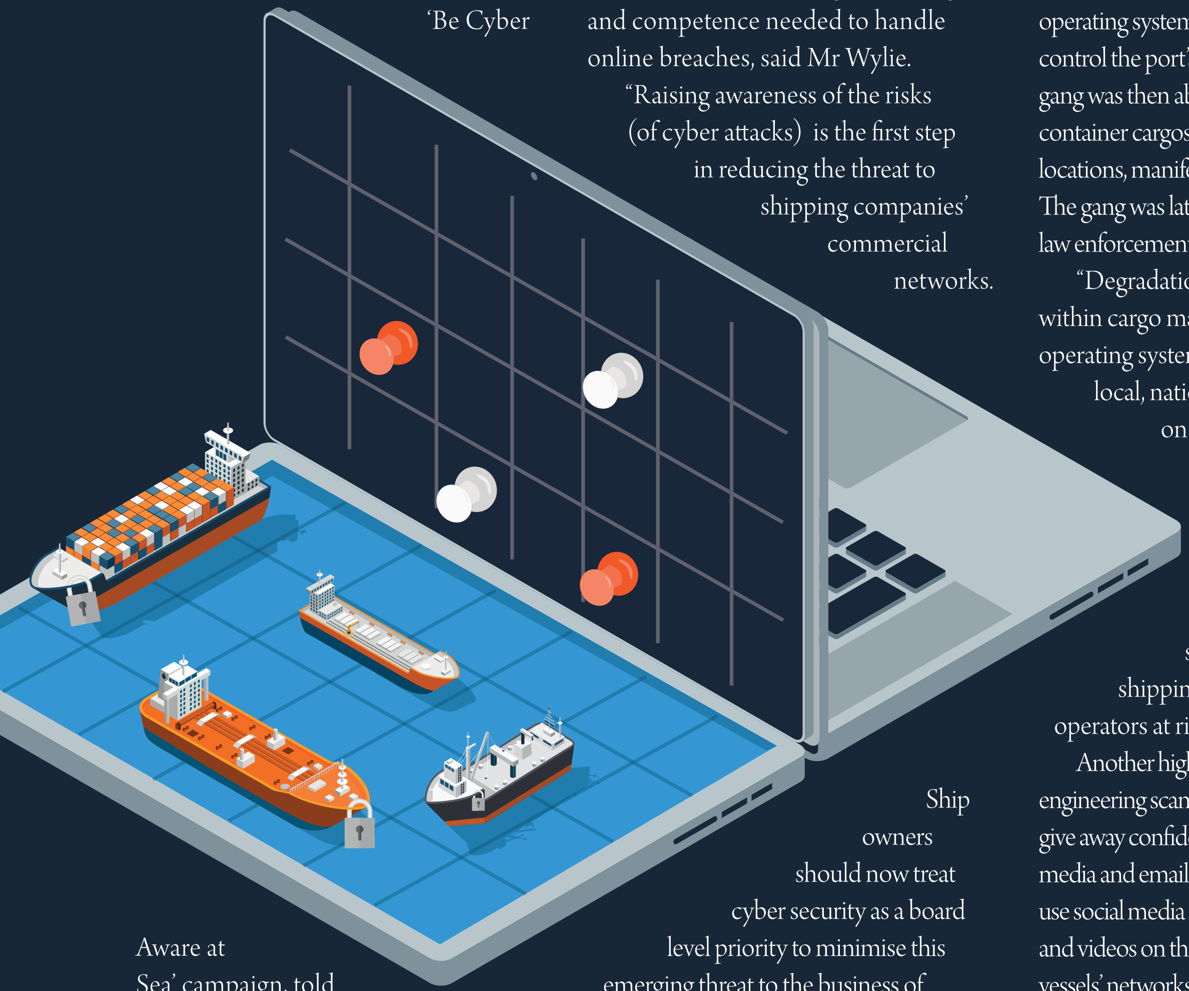
Notebook

Hackers wage a cyber war at sea

Complacency, poor training and a worrying gap in security knowledge are the key reasons for the disturbingly high number of cyber security breaches at sea, a press round-table event at London's Baltic Exchange heard recently.



Jordan Wylie, Director of the 'Be Cyber Aware at Sea' campaign, told 40 journalists and security specialists that criminals are playing a "dangerous and high-stakes game of cat-and-mouse" with ships' seafarers and officers. Yet a remarkable 80% of marine and offshore cyber attacks and breaches were due to human error, 67% of Company Security Officers believed cyber threats were not serious, 100% of Chief Information Officers did not provide cyber security training onboard for crews and 91% of Ship Security Officers believed they lacked the cyber training, knowledge and competence needed to handle online breaches, said Mr Wylie.

"Raising awareness of the risks (of cyber attacks) is the first step in reducing the threat to shipping companies' commercial networks. Ship owners should now treat cyber security as a board level priority to minimise this emerging threat to the business of shipping," said Mr Wylie.

One of the biggest recent breaches was when hackers obtained the personal data of 134,386 current and former seafarers in the US Navy via a contractor's laptop. In another incident, a criminal gang recruited a team of freelance hackers and targeted the networks of terminal operators in a large European port. Using malware (malicious software used to disrupt computer operations), the gang gained access to the seafarers' online systems and installed key-logging devices on to their individual networks.

The hackers then accessed the terminal operating systems used to manage and control the port's container movements. The gang was then able to smuggle narcotics into container cargos by exploiting the cargos' locations, manifest data and pick-up times. The gang was later caught and arrested by law enforcement officers.

"Degradation of data integrity within cargo management and terminal operating systems raises concerns around local, national and regional security on matters relating to narcotics, weapons and human trafficking. Persistent cyber vulnerabilities in cargo management systems leave both shipping companies and terminal operators at risk," warned the briefing.

Another high-risk area for ships is social engineering scams (manipulating seafarers to give away confidential information via social media and email networks). Seafarers often use social media sites to download images and videos on their mobile devices via their vessels' networks for personal entertainment and to help pass the time during long voyages. This makes them easy targets for phishing scammers who deviously try to trick them into giving away their private passwords, account numbers and credit card details.

It was a piece of social engineering that led to a HudsonAnalytix client suffering the loss of more than $250,000 when he was duped into a series of fraudulent payments to phishing criminals who often act in groups rather than as individuals to hoodwink and intimidate their victims. Another client had to pay out a significant sum of money to restore his business systems after a Ransomware attack – an online version of a ransom note and an increasingly popular scam – paralysed his headquarters' network.

Colin Gillespie, Deputy Director for Loss Prevention at the N of E P&I Club, told delegates that IT systems' functionality was responsible for 67% of cyber breaches. However the most vulnerable target for attacks by cyber criminals were ships' ECDIS systems. A total of 48% of maritime victims reported loss of corporate data while 21% suffered financial loss, he said.

"It is very difficult to legislate for cyber risks and the regulators are loath to issue rules and regulations," said Mr Gillespie. The root of the problem, he said, was that eventually virtually everything on a ship would be controlled by computer which makes vessels increasingly prone to hackers and cyber attacks.

It's the disturbing number of recent cyber-attacks that led to the launch of the 'Be Cyber Aware at Sea' campaign in October 2016. Pioneered by JWC International , the maritime and offshore cyber security training solutions provider, the campaign's aim is to help ship owners and managers, P&I Clubs, classification societies, maritime lawyers and flag states to protect ships and cargos and help seafarers understand the risks posed by the disturbing rise in cyber security breaches and the actions needed to combat incidents.

"All maritime risk management systems should now include some level of cyber security. There can be no excuses and no ignoring the threats," is one of the campaign's stark messages. A not-for-profit initiative, it is using posters, guidance booklets, seminars, a bespoke training maritime cyber training programme, a regular online magazine called *Phish and Ships* and educational videos to help 'normalise and simplify' maritime cyber threats, highlighting how risks of attack can be reduced significantly by adopting simple rules.

JWC, the pioneer of the campaign, has designed the first globally approved Maritime Cyber Security Awareness Course (MCSA) with GCHQ, the UK's intelligence and security organisation. The course which can be delivered onboard or onshore, is the first of its kind and has been developed for people working in both the maritime and offshore sectors.

Mr Wylie, who is JWC's Founder and Principal Consultant as well as the campaign director, said: "Shipping's evolution means its reliance on information and communications technology (ICT) is growing. The result is that more vessels are open to evermore cyber vulnerabilities. This is an unfortunate fact, but we can act to protect seafarers and ships." ●