LSLC
BUSINESS FORUM

It's full steam ahead for cyber crime unless the shipping industry and the authorities can keep it in check.

Cyber crime, directed against various parties within a transaction, was a fairly new type of offence but was already "rife," according to **Robert Hodge**, **a director of professional indemnity insurer ITIC**. Maritime executives needed to be very wary indeed about whom they are actually dealing with when communicating by email.

A recent IBM study into cyber breaches found that human error was involved in 95% of cases. Frauds might be fairly simple to spot "but its amazing how often they occur." Payments to third parties were sometimes activated by phishing emails which required the recipient to click on a link and open an attachment. Once the click was made, malware would be placed on that computer or server. "The hackers would be into your system."

Spear phishing was a relatively sophisticated form of attack. Organised gangs would co-ordinate a range of expertise to effect computer fraud. The criminals might take their time researching a company, checking published accounts, reviewing company profiles and identifying the right people to whom to send false emails. Having hacked into an email server, they might monitor the flow of traffic and learn the language of a particular trade so that eventual fraudulent emails looked the part.

They would wait for a worthwhile opportunity, such as a genuine email involving suppliers, banks or owners making requests for payment. The hackers would then set up a spoofed email address looking just like the real thing, in order to divert payment. Although a busy executive ought to check emails in minute detail, he might not. A single click and fraudulent accounts would be activated.

Mr Hodge cited a massive fraud on the Bangladeshi National Bank which involved diverting money to an account with a Philippines bank and which was stopped only after $100 million had gone to the hackers. The scam began with an email to the Bangladeshi Bank's HR department from a supposed job applicant. As requested, the HR dept clicked on a reference to bring up the supposed applicant's CV, entirely unaware that malware was thereby placed on the Bank's system. The hackers took time to work through to the SWIFT system where they started to redirect legitimate payments.

Shipbrokers have been known to phone numbers featured in the fraudulent emails, thinking they were speaking to the right people. "That's a sure way to pay the wrong person. When you get new bank account details from a party you've never paid before, advised Mr Hodge, phone the number you know to be correct—and not that featured

in a dodgy email—to verify details with the counter party. Phone someone you can trust."

Even if there has been some shipbroker liability, the weight of legal opinion and court cases has assigned real culpability to the parties making the payments because they should have checked fully.

Matthew McGhee, a barrister at Twenty Essex, surveyed the legal obligations of the parties after fraudsters had absconded with charterers' payments. Inevitably, owners and charterers would argue about who should bear the loss.

A charterer would assert strongly that, having been provided with apparently bona fide contact details by the owner or his agent, he had every reason to feel he was paying the owner. Why should he have to pay again?

Issues about contractual obligations were being teased out in new cases. In one, the court held that in the absence of something specific in the contract, the charterer must give the owner unfettered right to the immediate use of the funds. Yet where funds had already been diverted to a fraudster's bank account, this would not happen.

However, if a fraudster also happened to be an owner's employee, he would almost certainly be acting within his ostensible—although not actual—authority. The charterer might thereby argue that he had discharged his debt to the owner.

Normally, the fraudster would be an outsider. Nevertheless, might he be regarded as a de facto owner's agent, irrespective of whether the fraudster had proffered a false email address or taken over the genuine one? It might not matter that the fraudster is not actually an agent. Charterers might also argue that owners should bear the risk of a loss because a lack of care had enabled their own email systems to be compromised; or that owners let documents with charter details leak into the public domain, allowing access by a fraudster.

A court has held that if a party represented that a particular email address was secure with a very high level of password protection for the account, and that only someone authorised to have access to that email had done so, this might constitute an implicit representation. However, absent such a representation, a person is not entitled to assume that the sender of an email was the person who normally had control over the relevant address.

A couple of cases have involved discussion about owners according implicit representation about existing duties. Certainly, charterers would contend that there was an implied contractual duty for the owner to take reasonable care to maintain cyber security. However, expecting an owner to take on extra responsibility for security would be a high hurdle to cross.

In short, where a charterer pays according to a fraudster's "instructions," even if the fraudster's instructions have come from the owner's genuine email address, it is difficult for the charterer to shift payment obligation to the owner.

What other options are open to the charterer? The broking chain is important. If only the charterers' broker was fooled by the fraud, the charterer might have no recourse against the owner—-but he might have an action against his own broker.

The charterer would need to argue that the broker owed him a contractual duty to take care and guard against a type of fraud to which charterers were very obviously exposed. If, however, the owner's broker was fooled then he might be said to have bound the owner to the change in banking details.

Otherwise, brokers might be regarded essentially as intermediaries, just passing messages between the parties, not acting directly for any of them. Judges have upheld the view that an intermediary has no real agency function. It followed that although charterers had paid out once according to "instructions," they would have to pay again.

Charterers could accuse their own (paying) banks of a breach of care, contending that they should not have paid out because of the obvious nature of the fraud—very difficult to prove. They could go for the fraudster's own bank, contending that the receiving bank has been unjustly enriched by receiving the stolen money. Whether or not it had been so enriched is a very open question, affected by a conflict of case law.

It might be asserted that the bank has acted dishonestly, having knowledge of impropriety prior to making payment—again very difficult to prove. Going against the fraudsters might well mean throwing good money after bad. However, for the motivated victim of a fraud, the courts have been keen to enable action against fraudsters—if they are ever found.

All this produces some understandably aggrieved charterers who feel they followed all advice, checked the email address very carefully and found things—apparently—completely in order.

Thomas Steward, barrister at 36 Stone, highlighted the vulnerability of vessels and ports to cyber piracy attack, with advances in vessel technology sometimes increasing vulnerability. The perpetrators might be criminal gangs, hostile states, disgruntled former employees or even bored teenagers—all usually anonymous.

The motivation behind cyber-attacks varied widely: financial, commercial, even political. While ransomware is obviously aimed at immediate financial gain, hackers might wish to steal trade secrets or cause disruption to facilitate extended criminal operations. Risks include property damage, the imposition of fines for data breaches by regulators; reputational damage; and even loss of life. A cyber attack could render a ship unable to move or no longer in control of its movements, increasing the risk of grounding which could endanger crew, vessel and cargo.

Multiple possible entry points for attacks increased vulnerability. Connecting with the internet increased the level of risk arising from the number of computers on board. Hackers can take control of personal computers. Connection to a ship's wi-fi could provide access to a vessel's onboard systems, thereby gaining control of the vessel or allowing the installation of ransomware or malware.

Impersonating trusted institutions such as governments or banks could persuade people to part with sensitive information such as bank details. In response, national and international bodies have been addressing cyber risks for many years. The EU Agency for Cyber Security published its Guidelines in 2011. The US Coast Guard published its cyber strategy in 2015, underlining the threat of attacks to the nation's maritime transportation system and critical infrastructure—360 sea and river ports, handling more than $1.3 trillion in cargo annually.

In 2017, the IMO published a resolution and complementary guidelines re maritime cyber risk management. These provide that a safety management system should take cyber risk into account under the ISM Code. Some commentators feel that ambiguities in the resolution and guidelines could lead to varied implementation by flag states.

BIMCO has issued its own guidelines. Its 2019 cyber security clause for charterparty/bills of lading contracts has four aspects: a requirement to ensure cyber health; the imposition of responsibilities on third party security providers; recognition of the speed and invisibility at which attacks can happen; and liability limitation with a default cap of US$100,000. However, no clause could cover every case, given the huge range of potential attacks and the differing vulnerabilities of trades. Each case would depend upon its facts.

Seaworthiness remains the paramount consideration, given that a ship vulnerable to cyber attack might now be regarded as unseaworthy. Owners and operators must ensure that known defects are made good before sending their ships to sea. They must take account of their own knowledge of their vessels, the risks presented by their trades and the industry's standards and practices. SMS must be adequate, hardware and software up to date and drydock and maintenance programmes scheduled.

Seaworthiness should encompass on board systems to cover inspection, monitoring and repair of damage, and effective anti-viral and updated software for operating systems. Easily 'guessable' passwords are not good enough.

Sensitive aspects will change as the dependence of ships on developing technology increases. The advent of autonomous ships with highly specialised technology and a 'master' operating from dry land probably means that vulnerability to cyber attacks will increase. It may be prudent for companies to retain their own IT experts to verify and monitor their vessels' cyber health. However, while an owner may rely on software provided by a highly reputable third party, seaworthiness in itself is 'non delegable.' The liability regime for owners, operators and managers must remain the same.

Published guidance, regulations and articles will help owners and operators to keep abreast of the ingenious innovations of hackers and the counter measures being developed.

Hit by the hackers

Mr. Steward cited a number of hacking incidents, arising in very different circumstances, which illustrated the difficulties of identifying risk and, therefore, setting up countermeasures.

In 2013, it emerged that hackers had entrenched themselves in the IT systems which controlled the movement and location of containers in the Port of Antwerp. Criminals had secreted cocaine and heroin in containers among legitimate cargoes. Destinations and delivery schedules were altered to enable them to intercept the drugs at the point of discharge.

In 2014, hackers shut down a floating oil platform by tilting it.

In 2017, a ransomware virus hit the IT systems of Maersk. Although back-up systems ensured operations were not brought to a complete standstill, tens of thousands of computers were rendered unusable. The remedial bill was an estimated $300 million.

In 2019, a spoofing attack on the Stena Impero caused the vessel to drift into Iranian waters, where it was initially seized by the authorities.

In 2020, CMACGM was hit by ransomware. Apparently, the hackers requested the French carrier to contact them through Live Chat and pay for the special decryption code. Their identity is still not known.

Martin Rowland – LSLC Consultant