SEMAPHORE

Newsletter of the Maritime Law Association of Australia and New Zealand

New World of Cyber Security Risk

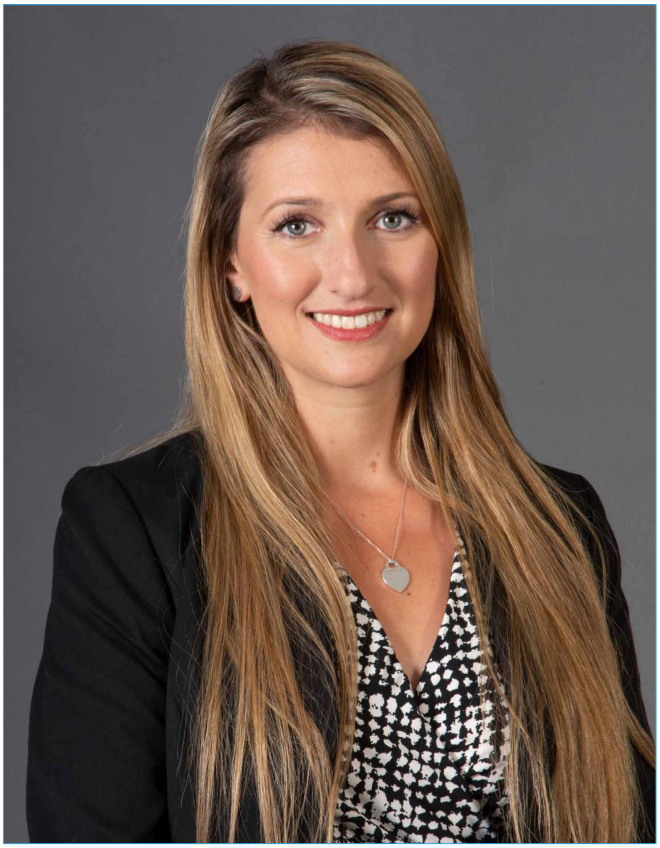
Increasing reliance on advanced computer software in the navigation of modern cargo vessels has simultaneously raised the risk and consequence of cyber security breaches – particularly in regard to the expanding area of unmanned shipping.

Such topics were explored by DLA Piper senior associate Sophie Hudson within her presentation to the recent New Zealand branch conference of the Maritime Law Association of Australia and New Zealand New Zealand.

Drawing particular focus on the insurance ramifications, Ms Hudson says to date cyber security risk has played a small part in marine insurance, “but is rapidly increasing”.

“A report by Verisk, an American data analytic company, estimates that by 2020 the Untied States commercial cyber liability insurance market will reach US$6.2 billion in written premiums, up from US$2.5 billion in 2016,” says Ms Hudson.

“Unless specifically included, standard insurance policies do not include cyber risks.



DLA Piper senior associate Sophie Hudson

“Of particular relevance in standard marine policies is Institute Cyber Attack Exclusion Clause 380. This exclusion applies where the cyber vulnerability is exploited with malicious intent, that is ‘inflicting harm’ (which is usually the case), but means the exclusion will not apply for internal human error during programming or system failures and shut down.

“This clause is accepted in many marine policies, but arguably is overly archaic given the technological advances and reliance on these systems. In 2017 Lloyd’s of London undertook a review of cyber risks and Cl 380 and found that some policies provide write backs for certain cyber risks and others were simply silent on cyber, but also noted the risk of reinsurers not covering in reliance on Cl 380 being included.”

Normal P&I cover, which has no express cyber exclusion, will respond to P&I liabilities, so long as the attack is not “terrorism”, “a hostile act by or against a belligerent power” or another war risk excluded (again requiring a malicious act), notes Ms Hudson.

“It depends on the motivation behind the attack – ie, if the act aims to kill, maim or destroy indiscriminately for a public cause then this is terrorism, but if there is no public cause and it is just to be generally disruptive, then it’s likely cover will apply.

Copyright 2009-2019 Maritime Law Association of Australia and New Zealand

"This was confirmed in *Atlasnavios* last year in United Kingdom Supreme Court where unknown third parties attached drugs to the hull to try and smuggle them from Venezuela, causing the vessel to be detained. As it was not a 'malicious act', as there was no intent to cause loss or damage to the vessel itself, the insurance policy applied."

Ms Hudson cites an older case involving *Tektrol* in the Court of Appeal, whereby a malicious virus was received by E-mail attached to an apparent Christmas card, which deleted the laptop source code. Two weeks later the only hard copy and two other computers with source code were stolen.

"However, although the author of code was a 'malicious person', it was not directed specifically at the insured's computer system so the exclusion did not apply.

"Relevant to these exclusion clauses, is determining what or who carried out the cyber attack. But it is difficult/impossible to trace attacks so it is not always known if there was a malicious intent – was it a bored computer-savvy 17-year-old or a state-approved hacking – the onus will be on insurer to prove malicious intent if wanting to rely on the exclusion."

Numerous organisations are now providing guidance and standards on how to manage maritime cyber security risks, adds Ms Hudson.

"The IMO has identified that the shipowner must have an adequate cyber risk management system in order to maintain unmanned vessels' cyber systems in a seaworthy condition. This is referred to as the process of identifying, analysing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders. The goal of the management system is to support safe and secure shipping, which is operationally resilient to cyber risks.

"IMO Resolution MSC.428(98) incorporated maritime cyber risk management into the mandatory International Safety Management (ISM) Code making it mandatory for shipowners to account for such risks – failure to do so results in the vessel being detained.

"From the shipping industry's perspective, protection against cyber risk is largely dependent on the use of security software, monitoring by the crew and the management of cyber security and safety – but there is no ability for crew to maintain and monitor security software on unmanned vessels."

Furthermore, Ms Hudson says cyber security risk may provide for a new meaning of seaworthiness, particularly where the vessel is unmanned.

"All familiar with section 40 of the Marine Insurance Act 1908 – which is arguably one of the most fundamental requirements in shipping – will note that insurance protection is specifically excluded where the vessel is unseaworthy.

"The Section 40 subsection (4) – 'reasonably fit in all respects' – definition of seaworthy is dynamic – 'all respects' must include cyber security and must include specific cyber risks.

"In terms of cyber, there is a need to ensure that the cyber security systems maintains seaworthiness for the ensure voyage, rather than just on commencement of the voyage."

In conclusion, Ms Hudson says increasing cyber security risk means a need for appropriate insurance – cyber insurance generally. including third party and property loss.

"Looking at the strict liability regime being implemented in the United Kingdom in regard to autonomous vehicles, the current strict liability regime for domestic carriage in New Zealand and the no-fault ACC regime – the insurance market will follow the statutory framework.

Copyright 2009-2019 Maritime Law Association of Australia and New Zealand

"So obviously we can't yet know what will happen, but how the world is addressing autonomous technology and what is being done so far in terms of strict liability, means it is not beyond the realms of possibility for strict liability to be imposed on insurers for the carriage of goods.

"The risk is transferring from the commercial parties to the insurers – no matter who is at fault."

Cyber Attack Reporting Urged

Meanwhile, the United Kingdom-based Company Security Officer (CSO) Alliance has introduced an anonymised avenue for its members to submit cyber security incident reports as a means of advancing knowledge in the field.

"Through building up this data we will have a better understanding of the nature and extent of the issues we face," states the Website of the organisation, which aims to be the "one-stop-shop for maritime and other industry sector security professionals around the world".

"This information can also help inform regulation and ensure a more effective response."

Axis Capital cyber insurance underwriter Georgie Furness-Smith observes that while "mega-attacks" get the most attention, cyber attacks in general are occurring at "an even greater rate than the public is led to believe".

"This issue – the under-reporting of cyber attacks – is a serious challenge for insurers and reinsurance as it skews the perception of the risk," says Ms Furness-Smith.

"This problem is particularly pertinent to the maritime industry, which many believe is already behind in its awareness of and preparedness for cyber risks."

Hence, she says the CSO Alliance's anonymous reporting initiative may help alleviate the problem of under-reporting of cyber attacks in the sector and "shine a light on the outdated perception that cyber security is a costly endeavour rather than a protector".

"In fact, cyber security programmes enable maritime businesses to be prepared, whatever the circumstance. Accurate reporting of cyber security incidents is a first, critical step.

"Equally important is the need for the maritime industry to understand the nature and volume of these attacks. This will help raise awareness, increase industry preparedness and mitigate the risks of subsequent attacks.

"If companies only hear about occasional cyber attacks within the maritime industry that have come to light because they affected large companies – such as the US$300 million Maersk incident in 2017 or the ransomware attack on Norsk Hydro earlier this year – they may believe cyber criminals target big businesses only. This can perpetuate a sense of denial."

Maersk Advice

Following its recovery from the June 2017 global cyber attack, NotPetya, Maersk urged shippers to take proactive steps to minimise the potential to have personal information stolen, malicious software installed on their systems or their computer's activities illicitly tracked.

The world's largest containerline's key hints to avoid phishing include:

- by moving your mouse over potential links you can see the site to which it links – do not open any links that do not contain ".maersk.com" before confirming with your local Maersk rep

Copyright 2009-2019 Maritime Law Association of Australia and New Zealand

- by checking the sender field carefully, you can often see an alternative E-mail – be cautious if it does not show “@maersk.com” or “@news.maerskline.com” and it is posing as a Maersk E-mail
- do not open executable attachments such as .exe files from untrusted sources

Maersk emphasises that it would never ask for personal information such as bank account details, credit card numbers or other financial data through E-mail nor ever send program installation files.

New Zealand Transport Sector Attack

Representing 80% of road freight operators in New Zealand, the Road Transport Forum also fell victim to a ransomware attack in March last year that caused a four-day shutdown of its computer network.

The attack was made via a Remote Desktop Protocol (RDP) connection previously setup for support services and, upon discovery that data files had not been sufficiently backed up to complete a full system restore, the organisation reluctantly engaged in transaction with the hacker.

It is understood that all data was subsequently retrieved and that no sensitive stakeholder data/ private documents were compromised. However, with the encryption having extended to system as well as data files, the de-encryption process left the system needing to be rebuilt in a time and money-consuming process.

Nick Harrison Consulting director Nick Harrison, who was engaged to complete the system restoration, also ensured the previous RDP connection was replaced with Virtual Private Network (VPN) access only.

“Our advice is to not have public-facing remote desktop connections and if you do want to have remote access then to create two-factor authentication, encrypted tunnels or VPNs,” he said at the time.

“That means you don’t have to have any firewall ports open.

“Having good security is of course important in terms of your perimeter, your firewalls. But nobody knows what the next hacker is going to invent – it is a never-ending battle – so the only one sure thing you can do is regular, good backups and to have those off site.

“This will be a lesson for the RTF, so hopefully they will now no longer just keep all of their work on their desktops but instead save it all to their server.”

The-then RTF communications and stakeholder engagement manager Hayden Cox added that the incident highlighted “just how vulnerable” small organisations could be to cyber security attacks.

“For a freight or logistics business where everything is run off a computer system, a ransomware attack could be absolutely crippling,” he said.

“While we had a very high level of protection on our system, the attackers managed to find a small opening through which they could encrypt everything. We would encourage all small businesses to invest in the best possible security measures they can.”

September 2019

Copyright 2009-2019 Maritime Law Association of Australia and New Zealand