www.bunkerspot.com Volume 18 Number 2 April/May 2021

BUNKERSPOT

CREDIT CONTROL

MANAGING RISK IN UNCERTAIN TIMES

INSIDE:

MARINE LUBRICANTS
AMMONIA BUNKERING
CYBER SECURITY
DELIVERING DIVERSITY

Clear and present danger

Ioannis Generalis of Harris Kyriakides finds that cyber security has become an increasingly important issue for the shipping and bunkering communities

Cyber security is fast becoming one of the buzzwords within the shipping community. Though the issue is hardly new, it is becoming more prevalent owing to major recent incidents as well as diverse drivers of change in shipping. These incidents include cyber attacks on the four largest container lines, including an April 2020 attack on Mediterranean Shipping Company (MSC), which led to its systems shutting down for a week. The drivers include the recent COVID-19 pandemic crisis and its ensuing overreliance on working through computers via remote (and often vulnerable) access points, the increased digitisation of the industry in an effort to cut down on cost and increase transparency, and future envisaged developments such as autonomous ships.

In terms of potential cost to stakeholders, cyber attacks bear wide implications. Firstly, there is cost associated with prevention and detection, such as purchasing or developing special protection software, updating company-wide policies, and acquiring specialist consulting services. Secondly, there is cost associated with the business itself, such as brand reputation tarnishing and possible loss of cliental. Thirdly, there is potential legal cost in terms of breach of contract, third party liability, and regulatory violations.

Cyber security threats are therefore both real and increasingly significant. This prompted the International Maritime Organization (IMO) in 2017 to adopt Resolution MSC.428 (98) on 'Maritime Cyber Risk Management in Safety Management Systems', whereby companies are to address cyber risks under their Safety Management Systems (SMS) as defined in the International Safety Management (ISM) Code. IMO 2021, as it is widely known, entered into force in January 2021, and encourages administrations to ensure compliance no later than the first annual verification of a company's Document of Compliance (DOC). Moreover, the IMO published Guidelines on 'cyber risk management' which make specific reference to published industry best practices, such as the 'Guidelines on Cyber Security Onboard Ships' produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.

BUNKER IMPLICATIONS

At this point, you might wonder whether cyber security has anything to do with bunkers. The answer is a perhaps surprising but resounding yes! Going as far back as 2014, bunkering scams through cyber attacks have cost companies millions, such as the attack on World Fuel Services (WFS) which resulted in an estimated $18 million loss for the company. A commonly used mode of attack within this context involves the criminal positioning itself in the middle of an electronic exchange between a shipping company and a bunker supplier, the companies mistakenly believing themselves to be in communication with each other, while in fact eventually communicating with the criminal. An exchange of account details, for instance, may lead to the criminal opportunistically providing false information, the money ultimately flowing into their account.

> 'Bunkering scams through cyber attacks have cost companies millions'

Going a step further, bunkers are now hugely significant in terms of legal compliance with the IMO 2020 low sulphur provisions and incoming decarbonisation regulation. Shipping companies simply cannot afford to be caught burning or carrying the wrong type of fuel. Cyber attacks may wreak havoc in the bunker supply network, with shipping companies ultimately held liable for regulatory violations. Moreover, data collection and flow concerning reporting and monitoring obligations under the European Union Monitoring, Reporting and Verification (EU MRV) or the IMO Data Collection System (DCS) carbon emission monitoring schemes could just as easily be interfered with.

Furthermore, one needs to explore the potential implications of a commonly used type of malware employed in cyber attacks, namely ransomware. Ransomware is designed to force companies into paying criminals to regain access to their hijacked IT systems, or to prevent leakage of stolen sensitive information. While unobstructed IT access may be crucial in terms of operations directly or indirectly affecting bunkers, such as slow steaming and navigation, it is also easy to see why both shipping companies and bunker suppli-

ers would be keen to avoid leakage of sensitive information such as type/origin/quantity of or price paid for bunkers, and exclusive supply agreements, in an effort to maintain a competitive edge, and protect commercial relationships they have invested in.

LIABILITY

Having established there is legal risk associated with cyber attacks, one first needs to consider whether and under what circumstances the party that suffered the attack remains liable, both in terms of contractual and third party liability.

Contractual liability could potentially be excluded under the doctrine of frustration or by invoking force majeure. However, it would be difficult for a shipping company to claim frustration (in terms of lack of foreseeability) or invoke a force majeure clause (should one be present) if, for instance, it failed to apply an update on software that was made available by the manufacturer resulting in vulnerability exploited through the cyber attack, or it failed to apply proper security standards / provide adequate training and an infected USB stick was brought on board. In terms of third-party liability, there is also a good chance such vulnerabilities brought about by poor standards could establish the vessel was not 'seaworthy' when it took to sea, for instance in the case of a systems hijack leading to a collision with possible damage to property and/or loss of life, whereby liability shall not be excluded and marine insurance claims may fail.

Model clauses are available and may be incorporated into contracts in an attempt to delineate and limit cyber related liability, such as BIMCO's 'Cyber Security Clause 2019' featuring in charterparties. The BIMCO clause creates obligations in terms of (i) implementing and reviewing systems, plans and procedures both pre and post cyber incident, (ii) using reasonable endeavours to ensure third parties providing services comply with these systems, plans and procedures, and (iii) notifying the other party of any incident affecting or likely to affect cyber security. There is a provision within the clause of limiting liability (the default limit amounting to $100,000), unless gross negligence or willful misconduct is proven.

INSURANCE

The next question to ask is whether insurers are likely to cover cyber-related liability. It is estimated 92% of the costs that may result from a cyber attack are uninsured[1], and widely acknowledged that available cover is both limited and restricted. With regards to third party liability insurance, P&I Clubs have now principally adopted the LMA 5403 'Marine Cyber Endorsement' model clause, in preference to the former widely applied CL 380 Institute 'Cyber Attack Exclusion' clause. The latter was criticised over its failure to address 'silent cyber', i.e. recoverable losses under traditional insurance policies emanating from the cyber attack, such policies containing no express cyber risk inclusion/exclusion wording.

> 'IMO 2021 and its accompanying Guidelines constitute the IMO's response to the increasing cyber threat by laying out an emerging regulatory framework'

Under LMA 5403, insurance cover is excluded for liability '*caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme*, malicious code, computer virus, computer process or any other electronic system' [my emphasis]. Cover is however provided where such use or operation does not constitute a means of inflicting harm, in contrast to the LMA 5402 'Marine Cyber Exclusion' clause. Moreover, where LMA 5403 is endorsed under policies covering war risk, cover includes a cyber attack which results in firing a weapon.

Furthermore, insurers may include the JCC 'Cyber Attack Exclusion Clause and Write-Back'. This model clause also excludes liability deriving from a cyber attack intending to inflict harm, but for 'an otherwise covered physical loss of or physical damage to the Insured's property caused by a Targeted Cyber Attack' (the write-back). The burden of proof under the write-back falls on the insured, who must demonstrate inter alia that the motive behind the cyber attack was to inflict harm solely on the Insured or its property.

IMO 2021 & GUIDELINES

Within this general context, IMO 2021 and its accompanying Guidelines constitute the IMO's response to the increasing cyber threat by laying out an emerging regulatory framework.

The Guidelines are presented as '*high level recommendations*' for cyber risk management, and are '*complementary to the safety and security management practices*' established by the IMO. As such they are an attempt to apply a *global standard*, and therein lies their value. They take note of industry best practices, and rely on a risk management framework incorporating five elements: identification, protection, detection, response, and recovery.

As for IMO 2021, it serves a dual purpose. Firstly, it *affirms* an approved SMS should take into account cyber risk management in accordance with the ISM Code. Secondly, it *encourages* administrations to ensure cyber risks are addressed in the SMS no later than the first annual verification of a company's DOC. Viewed together these two elements create an indirect obligation, as they confirm cyber risks should and indeed do form part of an approved SMS under the ISM Code, therefore any administration reviewing the DOC on the first annual verification would be prudent, though not legally mandated, to ensure compliance. When combined with the Guidelines, the end result of IMO 2021 is that shipping companies must review and update their SMS to address cyber threats under IMO recommendations, and industry best practices.

CONCLUDING REMARKS

Cyber security is a very real issue embracing all stakeholders in the maritime industry. Given insurers provide limited and restricted cover to the majority of the losses that may arise following a cyber attack, it is crucial companies review and adopt such systems and measures as to ensure they can detect, minimise and mitigate the risk of cyber attacks, and/or incorporate appropriate clauses into their contracts, in an effort to limit or escape liability. Though presented in terms of recommendations and encouragement, IMO 2021 and its accompanying Guidelines set shipping companies on that path, by applying a global standard, and 'retrospectively' affirming cyber security forms part of existing approved SMS, indirectly obliging companies to review and comply.

1. https://www.maritimelondon.com/news/meeting-the-cyber-threat-challenge-in-the-maritime-industry-protection-beyond-regulation

Ioannis Generalis,
Trainee Associate,
Harris Kyriakides

Tel: +357 2420 1600
Email: i.generalis@harriskyriakides.law
Web: www.harriskyriakides.law