JAPAN P&I NEWS

No.949-18/3/15

To the Members

Dear Sirs,

Cyber Risks and Cyber Security (No.3)

This is the last in the series of three Club circulars issued to inform and update members on cyber risks and cyber security issues. The first circular was published on 10 November, 2017 and provided a general introduction to cyber risks. The second circular was published on 20 February, 2018 and addressed the international regulations and guidance on cyber security. This third circular considers some possible cyber security scenarios.

INTRODUCTION

Regardless of technological developments, certain familiar issues will continue to threaten the safe operation of ships. These include perils of the sea, other vessels operating in close vicinity and system failures.

However with the increase in electrical systems onboard ships, new "cyber" threats are being identified. These risks can arise from malicious software, targeted attacks and user error.

SCENARIO 1 – Unseaworthy vessel?

A bulk cargo vessel carrying grain has run aground on a sandbank due to an electronic systems failure on board. There was water ingress into the cargo holds. As a result, a salvage operation was undertaken. Due to water ingress into the holds, around 50% of the cargo was lost. General average was declared by Owners and expenses were incurred in bringing the vessel into a safe port and discharging the cargo.

Investigations into the cause of the systems failure found that a critical software patch was not applied to one of the vessel's electronic operating systems. The evidence also showed that in the months leading up to the grounding, the software manufacturer had sent numerous emails to one of the senior managers at Owners' offices advising that the software patch needed to be applied. These emails had been overlooked by the manager and the recommendations were therefore not followed. As a result of this failure, the systems were vulnerable to the malicious software which caused the blackout on board the vessel.

Cargo Interests have claims for the lost cargo and for an indemnity for the amount they have

had to pay the salvors. These claims would be pursued against Owners pursuant to the contract of carriage which is likely to incorporate the Hague or Hague-Visby Rules.

To bring a successful claim against Owners, Cargo Interests would need to show that the ship was unseaworthy at the commencement of the voyage. Under English law, this would involve assessing whether Owners had acted prudently to ensure that the vessel was fit for the voyage. Owners would be judged by reference to the state of knowledge of the industry at the time. In light of the BIMCO Guidelines and industry guidance (see Circular 2), Owners would be criticised for failing to update their electronic software.

As a matter of English law, Owners would be required to disclose details as to the cause of the grounding. Evidence of the missed software patch would give rise to a very strong case that the vessel was unseaworthy at the commencement of the voyage.

Owners may then argue that, despite the vessel being unseaworthy, they had exercised due diligence. Such a defence would be very difficult to sustain where the senior manager had failed to act on the software manufacturers' guidance. As a matter of English law, the likelihood is that Owners' defence would be unsuccessful and Cargo Interests would be able to make a recovery for the lost cargo and their salvage indemnity claim.

Furthermore, in circumstances where the vessel has been found unseaworthy due to a failure to exercise due diligence, Owners would not be able to recover any GA contribution from Cargo Interests.

Although P&I cover should respond in these circumstances, we would urge all members to ensure that they are addressing issues of cyber security to maximise the prospects of defending claims of the type described in this briefing. The Club's second circular dated 20 February, 2018 identifies the guidelines and standards that Owners should be striving to achieve. Please kindly refer to that Circular for further guidance.

SCENARIO 2 – Mandate fraud

The Club is also increasingly aware of cases involving mandate fraud. Mandate fraud refers to the fraud committed by a party (i.e. the fraudster) fraudulently changing payment instructions so that funds are diverted from the intended recipient to a third-party bank account.

These cases often begin with a vulnerability in shoreside electronic systems which allows a fraudster to monitor email exchanges of a company. At the appropriate time in a transaction

between that company and its suppliers (for example), the fraudster, posing as the supplier will send an email with payment instructions. These payment instructions would direct money to be remitted to a third party's bank account instead of the supplier's account. The email from the fraudster is often sent from an email address which, at first glance, looks to have come from the correct supplier. On closer investigation, it is likely to show that one of the letters in the sender's email address is different.

To avoid being the victim of mandate fraud, it is important to ensure that your systems are secure. We would also recommend that practices are put in place to minimise risk. For example, before a payment is made, a telephone call could be made to the intended recipient of the payment to check the bank details. In such circumstances, responding to the email with the payment instructions to verify the payment would not assist.

CONCLUSION

We trust that this series of circulars has helped highlight the importance of cyber security within your business.

[This Circular has been prepared for Japan P&I Club by Ms. Jean Koh of HFW, a leading maritime law firm Holman Fenwick Willan LLP (http://www.hfw.com/Home). If you have any further questions please do not hesitate to contact the Club or Ms. Jean Koh of HFW who have prepared these circulars.]

Yours faithfully,

The Japan Ship Owners' Mutual Protection & Indemnity Association