JAPAN P&I NEWS

No.929-17/11/10

To the Members

Dear Sirs,

Cyber Risks and Cyber Security (No.1)

This is the first of three Club circulars issued to inform and update members on cyber risks and cyber security issues. This first circular is a general introduction to cyber risks. The second circular will address the international regulations and guidance on cyber security. In the third circular, we will consider some case study scenario of a cyber incident. The second and third circulars will be published during November.

INTRODUCTION TO CYBER RISKS

Cyber security is not a new topic but it is receiving a large amount of attention in the international news and the shipping press. Members are likely to have read about many high profile cyber security breaches this year. For example, Maersk were the subject of a high profile cyber attack caused by a virus called "NotPetya". This attack impacted Maersk Line, APM Terminals and Damco causing several weeks of disruption in July 2017.

As the attack on Maersk has shown, the shipping industry needs to take the risk of a cyber attack very seriously. Information technology and electronic systems play an essential role in the shipping industry. To take some obvious examples:

- Automatic Identification Systems (AIS) exchange vessel tracking and identification data with other vessels, ports and the coastguard;

- A ship's position and speed are displayed on the Electronic Chart and Display Information System (ECDIS) which is often updated via the internet.

- Ships and container ports also rely on electronic Global Positioning Systems (GPS) to identify vessel positions, steer cranes and stack containers.

In general, these technological advances have brought about increased efficiency and operations. However it has become clear that these systems have vulnerabilities which could be exploited. There is an increased risk where there are interconnected systems or different components operating on the same network. As such these electronic systems needs to be carefully operated, safeguarded and secured.

AWARENESS OF TYPES OF RISKS AND THEIR IMPACT

Risks may result from incorrect operation, technology failures, lack of training, inadequacies in the system design or from a deliberate malicious attack. If a vulnerability is exploited, this could compromise security, confidentiality, system operations and safety-critical equipment. There is a clear incentive for a hacker to try and attack the shipping industry with its high value assets, passenger data and the movement of expensive cargoes on a daily basis.

In the Club's view, members are particularly vulnerable as shipping becomes increasingly dependent on electronic systems and the internet which play a role in navigation, engine control, steering and cargo handling. With such increased dependence, it is necessary for members to ensure that sufficient attention is paid to cyber security issues. If, for example, obsolete operating systems are being used or if the necessary repairs on computer systems are not being undertaken, then there is an increased risk of a cyber attack. The more vulnerable a system is, the higher chance a cyber attacker will try and exploit that.

The damage that a cyber attack may cause is difficult to quantify. Recent estimates suggest that Maersk may have suffered losses of over USD 300 million following the "NotPetya" attack. In addition to the financial cost, there is likely to be reputational damage if it is shown that systems are not secure. If cargoes are damaged or delayed then that may also lead to claims. Last, but not least, there is the risk of fines or criminal action being taken depending on the nature of the attack and the jurisdiction in which it took place.

RESPONSE TO CYBER RISKS

The Japan P&I Club rules do not specifically comment on cyber risks. A claim arising out of a cyber attack or cyber breach would be considered in the usual way with reference to the Rules. When the cyber attack would not fall under “war” or “act of terrorism” under the rule 35, a member’s normal P&I cover will respond. The shipping industry is widely regarded as having moved slowly to address cyber risks. However, since 2015, cyber security has been prioritised by organisations such BIMCO, IUMI, the International Chamber of Shipping, Intertanko and most recently the IMO. A definition of cyber attack in the context of a P&I cover will become more clear as discussions in maritime organisations above including the International Group of P&I Clubs develops.

Nonetheless, we would urge members to address cyber risk management prudently and carefully to minimise the prospects of a cyber attack.

In our second circular we will be considering the guidelines and recommendations that have been issued. This will set out the steps that we recommend members take to understand whether there are potential vulnerabilities in their systems. It will also set out recommendations on how to react to a cyber attack.

In our third circular we will be considering examples of potential cyber attacks which members may be exposed to. This will include a grounding incident caused by a failure to update electronic software. We will also consider mandate fraud where a cyber attacker finds a way to redirect funds to a different bank account.

[This Circular has been prepared for JPIA by Mr. Matthew Montgomery / Ms. Jean Koh of HFW, a leading maritime law firm Holman Fenwick Willan LLP (http://www.hfw.com/Home)]

Yours faithfully,

The Japan Ship Owners' Mutual Protection & Indemnity Association