Junge

Client Newsletter
Junge & Co.
Issue: June 2020

Cyber-Attacks - Your Exposure

In a world increasingly dependent on digitalisation, companies are more vulnerable than ever to cyber-attacks. Especially the maritime industry has to face increased risks of cyber-attacks but same have not been that much in the focus so far. Shipping companies rely both their land-based and shore-based activities on constantly evolving technology and are therefore an attractive target for cybercrime. As a result, cybercrime is increasingly becoming an apparent risk for shipping companies.

The possible damages are not limited to business interruption but also Hull & Machinery damage, cyber extortion, vessel detainment and regulatory fines as well as damage to shore based equipment and loss of data could be results of cyber-attacks.

Recent developments have shown that cyber risk management is critical in today's business environment and that a contingency plan must be developed before the company becomes the target of a cyber-attack. Not only need the above-mentioned risks be assessed but shipowners also have to establish a way of responding when under attack. In order to keep losses to a minimum, shipowners are required to react in a timely manner and allow specialists to fight the attack so that operations can continue as usual.

The latest cyber-attack on a large scale was aimed at one of the largest box carriers in April 2020 and resulted in the disruption of the services of the company across the world to a partial note. Attacks like this and the increased exposure during the Covid-19 pandemic show the need to act.

Many employees are working from their homes during the Covid-19 pandemic and criminals are trying to profit from this situation, when private home networks, laptops and smart phones are being used to enter the company's networks.

Lastly, the International Maritime Organisation released guidelines and high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. Furthermore, the Maritime Safety Committee, at its 98th session in June 2017, also adopted a resolution in which the organisation encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

Hence, considering the above we would like to draw your attention to the advantages of a cyber insurance.

Cyber Insurance proves to assist in three ways:

- Cyber Insurance pays the loss occurred based on the different components which have been insured
- Cyber Insurance providers offer immediate on-site assistance by specialists to fight a possible attack in order to mitigate a loss.
- Before the insurance becomes effective, the company's risks will be assessed in order to minimise the possibility of a cyber attack and to prevent incidents

We at Junge & Co. are prepared to offer you tailormade solutions and cyber-risks insurances for your individual needs. Should you be interested in receiving an offer for a possible insurance cover for cyber-risks or would like to discuss this matter in more detail please feel free to contact us.