



The effect of cyber-attacks on the shipping industry

AUTHOR / KEY CONTACT



Linda Jacques
Partner

✉ Linda.jacques@LA-law.com
☎ 01202 702611

High-profile cyber-attacks have raised some major concerns within the shipping and insurance industries in recent years. A recent survey conducted by Futureonautics showed that 44% of ship operators believed that their current IT defences were incapable of eliminating the risk of cyber-attacks, while 39% admitted that they had experienced a cyber-attack within the past 12 months.

A major cyber incident could have a catastrophic impact on cargo operations and could potentially cost shipping companies millions of dollars in lost revenues. For example, Maersk suffered damages amounting to \$300m after its system was infected with the NotPetya ransomware in June 2017, which caused disruption to its booking system

Generally speaking, however, the consequences of cyber-attacks are usually excluded from marine insurance

coverage through the operation of the Institute Cyber Attack Exclusion Clause CL380. It is therefore crucial for ship operators to ensure that there are no gaps in their policies in order to cover against this risk.

From a legal point of view, the risks posed to the shipping industry by developments in cyber technology are a new concept. If a cyber-attack causes damage to a ship or cargo, could it be said that the attack has compromised the vessel's seaworthiness or cargoworthiness or that the ship was unseaworthy?

In this respect, it is important to remember the central principles of the concept of vessel seaworthiness or cargoworthiness. Under Article 3(1) of the Hague-Visby Rules a carrier must, before and at the beginning of a voyage, exercise due diligence to make the ship seaworthy, to properly man, equip and supply the ship and to make the ship cargoworthy. Given the technological developments within the marine industry in recent years, ship operators' risk management systems should now contain some level of cyber risk management that will eliminate any potential damage emanating from cyber-attacks.

For example, consider a situation where a cargo handling system has been hacked and corrupted by a cyber-attack, causing cargo to be damaged. The cargo interest would then be in a position to argue that the vessel did not have sufficient, efficient or competent crew on board and was not cargoworthy with reference to the Hague-Visby Rules, as sufficient measures were not in place to meet the challenges posed by a cyber-attack.

Such measures will be evaluated with reference to the state of knowledge in the industry at the time. Taking the state of current knowledge in the industry, in light of the increasing number of cyber-attacks in recent years and considering the foregoing as a growing systematic risk, it will be difficult for ship operators to argue that they were unaware of the threat and the need to safeguard themselves from it.

The IMO Maritime Safety Committee, in June 2017, adopted Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems. The resolution implements regulatory measures "ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code)", by January 1, 2021. New legislation is now in the process of being drafted and is most likely to contain a requirement that ships are issued with a cyber-security certificate by an approved body or flag or port state. Vessels can be detained if their owners do not have such a certificate in place.

In addition, with the implementation of the EU's Networks and Information Systems (NIS) directive, ship owners, as "operators of essential services", will be considered liable in the near future for failing to "take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies". These developments clearly show that serious and rapid importance of cyber risks has now been recognised as a high priority by the industry. It is advisable that shipping companies obtain proper advice on these new policies and procedures and implement frameworks for data protection in order to eliminate the risk of cyber incidents.

