Cyber Security. Is the ship seaworthy?

The International Maritime Organization (IMO) defines the Maritime Cyber Risk as a measure of the extent to which a technology asset is threatened by an event, which may result in shipping related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

As the Internet era rolled in, most shipping companies exposed all onboard and office systems to the Internet without thinking their actions through and taking necessary security precautions. Today the ships’ infrastructure (ship systems, communication protocols, etc.) are mostly outdated in cyber security aspects. This includes but is not limited to the Automatic Identification System (AIS), Global Maritime Distress and Safety System (GMDSS), Navtex, which have been designed without cyber security in mind. The shortcomings of such onboard technologies have been recently revealed.

The following are only few examples of the recent successful attempts to disrupt the flow of the maritime industry:

* **AP Moeller – Maersk**
  In late June 2017, AP Moeller-Maersk was forced to shut down its container operations in the Port of Los Angeles. The company’s IT systems were infected with the NotPetya ransomware which caused disruption to the booking systems. The company suffered damages amounting to USD 300 million.

* **Bunker Supplier**
  A small virus was planted after the company’s systems were hacked. The hackers were able to monitor all emails to and from people in the finance department. Whenever one of the firm’s fuel suppliers would send an email asking for payment, the virus simply changed the text of the message before it was read, adding a different bank account number.

* **ECDIS Attack**
  The Electronic Chart Display (the ECDIS) has also been hit. One of the ship’s crew had brought a USB stick on board with some paperwork that needed to be printed. That was how the malware got into the ship’s computers in the first instance. But it was when a second crew member went to update the ship’s charts before sailing, also via USB, that the navigation systems were infected. Departure was delayed.

* **Port of Antwerp hacked for drug smuggling**
  In late 2013, it was made public that the port of Antwerp had been subjected to a persistent cyber attack, which had been ongoing since June 2011. The penetration allowed the attackers to have a remote access to the terminal systems and thereby they were able to release containers to their own truckers without knowledge of the port or the shipping line.
Developments in the cyber technology and the risks of the cyber attacks posed to the shipping industry are a relatively new concept. Such risks need to be well understood in view of the carrier’s duty to make the ship seaworthy and cargoworthy.

The traditional approach is that 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, as well as to make the ship cargoworthy.

According to Carver on Carriage of Goods by Sea: ‘A ship must have that degree of fitness which an ordinary careful and prudent owner would require his vessel to have at the commencement of her voyage having regard to all the probable circumstances of it’. Notably, a ship’s seaworthiness extends beyond her physical fitness for the relevant voyage.

If the cyber-attack causes damage to a ship or cargo, could it be said that the attack has compromised the ship’s seaworthiness or cargoworthiness? Or can the suffering party deem that the ship has been unseaworthy at the beginning of the voyage?

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 ship did not have sufficient and competent crew on board, that the management did not implement efficient safety management and was not cargoworthy, as sufficient measures were not in place to meet the challenges posed by a cyber-attack.

Given the technological developments within the maritime industry in recent years, the ship operators’ risk management systems should now be prepared to eliminate any potential damage emanating from cyber-attacks.

For the liability considerations, the measures taken by the ship operators will be evaluated with reference to the present state of knowledge in the industry. Speaking about a current state of knowledge in the industry, in light of the increasing number of cyber-attacks in recent years, it will be difficult for the ship operators to argue that they were unaware of the threat and the need to safeguard the system on shore and afloat.

In terms of marine insurance, it is important to remember that often the consequences of cyber-attacks are excluded from marine insurance coverage through the relevant exclusion clauses. It is therefore crucial for the ship operators to ensure that they are prepared to meet the challenges of the new evolving risks.

What measures can be taken?

The researchers are advocating for the introduction of the basic security policies in modern ships. Whilst there are multiple types of equipment found on a ship that connect online, the researchers say that satellite antennas must be secured first. The cyber security can be to some extent achieved through technical solutions. However, any technological security developments should also be complemented with an appropriate research in the area of human factors.

A large part of successful attacks include a human element – usually termed social engineering. This part includes elements such as getting employees to open email attachments containing viruses, getting people to click on the links they should not click on, providing information over the phone which they should not. These elements cannot be addressed through the technical solutions. Instead, they have to be addressed through a combination of business processes and awareness training of the employees.
There is a call for establishment of a forum of maritime companies, where the industry players could share tactical cyber defense information as well as develop standards and processes to jointly improve industry cyber defenses. Some of the industry’s other initiatives are as follows:

- In order to gain a clearer picture of the extent of the problem, DNV GL has begun working through the International Association of Classification Societies to set up a platform so that cyber attack incidents in the maritime sector can be reported anonymously;

- BIMCO released The Guidelines on Cyber Security Onboard Ships in February 2016;

- The IMO has plans to incorporate cyber risk management into the International Safety Management Code from 2021 and it has given ship owners and managers until 2021 to incorporate cyber risk management into ship safety system. 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.

- In addition, with the implementation of the EU’s Networks and Information Systems (NIS) directive, shipowners, as “operators of essential services”, will be considered liable in the near future for failing to “take appropriate and proportionate technical and organizational measures to manage risks posed to the security of the network and information systems on which their essential service relies”.

The maritime industry and its extended supply chains should respond to the call for a proper cyber security management and get prepared. The first and main step is to recognize that the cyber risks are real and the attempts to attack the industry are taking place. As a next step, it is recommended to obtain a proper advice on the newly introduced requirements and implement frameworks for data protection.

Prepared:
Svetlana Ormane
Marine Underwriting Services, Claims Handler
www.underwriting.lv