Cyber Risks

Cyber Attacks, which we have seen and heard more in movies/ news, have gradually become a part of our lives and started to occupy the top places in the risk planning for companies. The triggering factor in maritime took place after Maersk, which was exposed to a cyber attack in June 2017, announced US$300 million loss and the number of maritimespecific seminars and workshops on the topic have increased.

Almost all major organizations (BIMCO, Intertanko, Interkargo, Iumi, etc.) published similar recommendations for their members based on IMO cyber risk management recommendations. In terms of insurance, it is also seen that some insurers recommend cyber security specialist companies and offer new products to the members regarding cyber risks that do not fall under traditional insurance coverage.

So, what is the actual severity of the risk for us? The answer to this question can be evaluated as both high and very low. To date, there has been no direct attack on any company or ships as seen in the movies. In other words; there has been no attack in the form of neutralizing the ship's systems or seizing control of the ship. Attacks that have been developed for a specific purpose, such as the Stuxnet virus, that target the infrastructure of countries are already beyond our scope, and it is unlikely that companies will be able to resist such sophisticated attacks on their own. However, the basic cyber risks faced by individuals and companies today are more in the form of data theft or requesting money by blocking data by using viruses such as Petya, NotPetya, WannaCry, Equifax, and so on. For example, the WannaCry virus encrypts the hard disk of the computer to block access and requests a certain amount of money to decrypt and reuse it. Petya and then NotPetya viruses similarly follow the method of preventing data flow in the computer and charging fees to remove the obstacles.

Halil Solak
Assistant Technical Manager
+90 216 545 0300 (D.236)
+90 533 200 2818
halil.solak@turkpandi.com

Halil graduated from Darussafaka High School in 1995 and Maritime Academy of Istanbul Technical University in 1999. He started his marine career at Zodiac Shipping,London. He completed his MBA degree in Risk Management and Insurance at Georgia State University in USA. Before joining Türk P&I as Assistant Manager, he worked as hull and cargo underwriter for Zurich insurance company and later spent 9 years at Omni Broker House as insurance and reinsurance broker. He presented seminars in Risk Management and Marine Insurance, including Exposhipping and his articles are published in local and internetional media.

TÜRK P&I

The interesting thing here is that, the NotPetya virus spreads with an accounting software originating from Ukraine. NotPetya is the cause of Maersk's $ 300 million loss, including operational losses. Equifax is also a large corporation that stores credit data in the United States. With cyber attack, registered user data in Equifax was made public.

As an individual user or as a small and mediumsized company, you need to evaluate how you can prevent a virus originating from the accounting software you use, how well a generic 100 TRY antivirus software available in the market can protect you from such attacks. Today, Cyber Risk Insurances are available but they cannot be provided widespread in Turkey as they contain a risk analysis different from those of the ordinary risks.

As it can be understood from the above, these attacks are aimed at all computer users in general and there has been no cyber attack targeting the maritime sector specifically. Although it is not paid attention as much as the attention given to the main coverages, every Hull & Machinery policy contains a Cyber Risk clause (Institute Cyber Attack Exclusion Clause Cl.380), The full text of this clause can be found easily on the Internet, but if we summarize, Cyber Risks are excluded from coverage.

In P&I insurances, the situation is slightly different. Although P&I insurances contain detailed information on paperless trading, no study on Cyber Risks has been performed yet. In other words, if a liability arises in the event of a cyber attack on the ship, the P&I coverage will apply as for any other liability damage. The only exception applies when such attack is fall under War & Strike Risks.

If we bring it up a little more; vessels had very limited connections with the land while they were cruising on the high seas until recently, but nowadays they maintain electronic connections with land facilities through many equipments, such as AIS, ECDIS, GPS etc. making them more vulnerable to cyber risks than it was in the past. Even if a cyber attack has not taken place so far, if the electronic devices of the ship would be shut down as the result of a cyber attack and any circumstance such as collusion, environmental pollution, damage to third parties or their property which are covered by P&I takes place, the P&I insurers will take part and reimburse the damage incurred. However, the damage to the ship itself as a result of the attack is out of coverage.

Although it seems simple, the experts' first suggestion against cyber attacks is to think twice before opening the attachments in the incoming emails and to confirm the bank details received, by telephone before you make the money transfer.