Cyber security: A P&I Perspective

by: Elina Souli

Regional Business Development Director (EMEA)

Vice President and FD&D Manager (Hellas)

The American P&I Club

Over recent years the maritime industry has increasingly depended on digitalization and IT technologies in order to improve efficiency and reliability. The same goes for cargo operations. Years ago, the industry depended more on human labor and manual methods. Cargo handling is rapidly depending on digitalization as well. A serious incident with Maersk in June 2017 caused a huge disruption to Maersk operations and terminals worldwide and the accumulating losses exceeded USD 300 million. That demonstrates the increased threat of security risks from hacking and sabotage.

A common factor that exists between P&I insurance and cyber threats is the human element. P&I insurance covers third party liabilities where the majority of incidents are caused by human error. Therefore, all P&I Clubs have developed robust loss prevention departments in order to share awareness and knowledge as well as to train all the parties involved on how to best prevent such incidents.

When it comes to cyber attacks there is an awareness gap which is one of the main reasons why cyber threats and associated risks have spread around the globe so quickly during the last few years. Over the last decade incidents have increased at an alarming rate. Thankfully that rate has recently stabilized due to higher awareness in the shipping market. Nevertheless, the maritime community has a growing concern about cyber risks. That is mainly linked to the fact that 50,000 vessels are at port or at sea at any given time and recent reports say that there are nearly 17 million attacks worldwide on a weekly basis. That gives a clear picture as to cyber security's importance.

Another crucial issue is crew-member awareness. A 2018 survey revealed that close to 47% of the seafarers that were questioned said that they had sailed on a vessel that been a target of a cyber attack. Regrettably, only 15% of those seafarers had received any form of cyber security training. That which had been provided was done by the manning agents before leaving on their next contract. That means the training was not specific either to the company or to the particular ship. Thus, it is evident that there is an immediate need for preventative measures to reduce or eliminate the occurrence of cyber risks. Obviously, prevention is preferable to needing a cure.

We have to adopt a holistic approach in order to ensure that there is sufficient training and education but on a specific basis. It is essential that every party assess the relevant risks and work towards training to that effect. The maritime industry needs to be well equipped to meet future cyber challenges as well, such as those that may emerge with the advent of fully autonomous vessels.

The American Club has a strict policy in place for employees to receive sufficient training specific to our needs and to obtain adequate certification. Cyber threats are constantly evolving. Hackers seem to be on top of new technologies, so market players need to enhance their defenses by continuously assessing their systems and developing procedures that will enable them to spot red flags.

How should P&I insurance respond to a cyber risk event once it materializes? Obviously, each and every case must be dealt with based on its own facts. In order to give you a few examples, we have created some scenarios.

The first one is related to unauthorized access into an agent's system. When a shipowner tries to remit funds to his agent's bank account, these funds end up being redirected to the hackers' bank account. That is obviously an act of fraud which causes economic losses to the owners. Unfortunately, these losses fall outside of P&I cover. However, we are still able to provide assistance within the context of FD&D cover and take legal action in order to recover those misdirected funds.

Another possible scenario is where malware is accidentally installed to the vessel's navigation systems by a seafarer; for example with the use of an infected USB stick. This could potentially create problems with the navigation system of the vessel, resulting in a major casualty such as a collision or an injury. In this situation, we have a common element which is human error and therefore the P&I insurance will respond as usual. But this could have been prevented by using the main principle of loss prevention: training and the implementation of strict policies.

The last scenario has to do with a virus, which can be planted by a seafarer's mistake and cause an engine failure. The losses - which inevitably will be incurred by the shipowner due to the disruption to the vessel's operation - will fall outside P&I cover.

Due to the extensive development of cyber risks, maritime organizations have responded by issuing guidance and initiatives to the industry. The International Maritime Organization (IMO) issued guidelines on maritime cyber risk management and also adopted a resolution in June 2017, to ensure that cyber risks are properly addressed within the safety management system with a deadline of January 1, 2021. If a vessel has not complied by that date, it runs the risk of detention.

BIMCO has also responded and issued guidelines on cyber security onboard ships with the assistance and support of other international organizations. The aim is to provide the basic guidelines by way of a diagram in order for companies to define personnel rules, develop consistency plans to assess the assets at risk and to be able to detect a cyber event in a timely manner. What is also important is to develop a plan in order to provide resilience and to restore the systems as soon as they have been attacked. Last, but not least, is the importance of preventing any reoccurrence.

At the American Club we support all of these guidelines. We have issued alerts and reminders to our Members and we are always at their disposal, should we be able to provide additional clarifications. The last initiative taken by BIMCO is their Cyber Security Clause 2019 which aims to spread awareness to all contractual parties in a charter party - the owner, the charterer and the broker - in order to push them to create systems which not only eliminate the risks of a cyber event occurring but which also mitigate any adverse effects should such an event occur.

In conclusion, it is important to consider and assess your risks as well as to focus on any insurance gaps which need to be bridged in consultation with your insurance experts. Keep in mind that while there are no cyber exclusions within your P&I cover, P&I insurance won't be able to cover each and every scenario. The way forward is to establish training and education procedures across all levels of your company in order to ensure a robust cyber environment.

The preceding text is an edited version of Ms. Elina Souli's presentation during the 2020 SMART4SEA Forum.