As digitalizing is taking over almost all aspects of our life there is an increasing threat of cybersecurity that industries are facing today. Cybersecurity has been classified as one of the most dangerous global risks by the World Economic Forum. Moreover, according to experts, the risks related to cybersecurity will only increase with time as the world is becoming more and more dependent on digitalization.

Similar to many other industries the maritime industry has started to heavily depend on digital systems to improve the accuracy and efficiency of their operations. Consequently, they are faced with certain cybersecurity-related challenges that could have a lasting impact if they are not dealt with on time.

Let’s have a look at some of the most significant cyber-security challenges that the maritime industry has to face, but before we do that let's try to understand the need for cybersecurity in ships in the first place.

# The Need for Cybersecurity in Ships

The alarming number of cybersecurity attacks lately has emphasized the need of implementing certain precautionary measures to prevent a bigger issue from arising later. The Clarksons cybersecurity ship attack in 2017 was one of the biggest security breaches in the world and is something the maritime industry needs to takes a lesson from. The Clarkson's was once the biggest ship exporter.

They suffered a cyber-security breach when an unknown account hacked into their system. Although the company was able to recover after the attack it did highlight the importance of cybersecurity in ships. After the attack, the company rigorously worked on improving their system's security. The lack of cybersecurity has indeed opened our eyes to how security is a must in the maritime industry. The advent of satellite-based technologies has made ships more vulnerable to cyberattacks.

Security attacks could result in ships losing confidential data or in the worst-case scenario these hackers could cause the ships to reroute and change their course. Another cybersecurity threat is invoice frauds which are seen at the port. It is also a safe practice to integrate your ship’s system with a reliable credit and debit card company like [Cardzgroup](http://www.cardzgroup.com) to prevent the occurrence of any fraudulent activity. This will also give your customers assurance regarding their financial transactions.

The impact of a cybersecurity attack could be massive; however, the implementation is a challenge on its own. Let’s discuss the most common challenges faced below:

**The slow rate of adoption**

The shipping industry has found it difficult to utilize data for making their ships secure and safe. The main cause of the slow adoption rate is that the maritime industry has been functioning in this manner for years – centuries to be exact. It is not easy to leave age-old practices and adopt new ways. This mindset has brought a huge hurdle in the development of the maritime industry and the security aligned with it. If companies in the maritime industry can adopt these practices easily it can help in overcoming these challenges.

**Complex systems**

Ships run through complex systems that are not easy to break down. In current times, technological trends are changing almost every day. This has made adaptability even more difficult for people working in the maritime industry. It is worth mentioning though that over the last couple of years there has been a noticeable improvement in the digitalized services that are offered onboard, this has somehow increased the magnitude of the threat that the maritime industry has to overcome.

**Lack of training**

The crew members on board are constantly on rotation which means that if a set of crew members undergo training at one point in time, they will be replaced by those who don’t have the technical know-how of how the machinery works. The level of inconsistency in the training of the crew has indeed played a big role in how things are handled and how exposed the ship is to a cyber-security threat. Crew members who are not aware of cyber-attacks can leave the ship’s data exposed and it is easy for hackers to gain access.

**Depending on terrestrial infrastructure**

Ships are highly dependent on terrestrial systems which are connected to the systems onboard. This can cause unnecessary delays in everyday tasks and may even cause a bigger challenge if the ship faces a cybersecurity attack. Due to the nature of the maritime industry dependency on terrestrial functions is a must and cannot be avoided unless more sophisticated technology is introduced.

# A guide to mitigating cyber-security risks at sea

If you want to successfully control a cyber-security threat at sea then certain precautionary measures need to be put into effect right away. Our guide will walk you through these measures.

**Securing the network**

Securing the ship's network is one of the most basic and obvious ways to start with. Since all of the ship's data is stored in the system which is connected to a satellite there is a very big risk of losing that data through the satellite. Therefore, it is imperative to limit any unauthorized entry which can be done by tightening the security of the system. A security breach can be avoided by having multiple firewalls and training your staff to respond as required.

**Malware prevention**

Having an anti-malware policy is crucial to the network security of data. Malware is malicious software that can destroy a system and leave data exposed. Therefore, all technical crew members on board must be trained to detect any suspicious activity and deal with it effectively.

**Containing risk**

Companies must also be equipped with the right tools that would help them contain the risk in case of a cyber-attack. The sooner the issue is controlled the lesser will be the impact of the cyber-attack. It is also useful to keep a backup of all the useful files so that in case of a ransomware attack the company already has a backup of confidential data.

**Awareness**

The major challenge that shipping companies face is that their employees are not aware of the security practices and measures that need to be put into place. Therefore, relevant training and required skillset can improve the way they handle a cyber-security attack. Companies could save huge amounts of money later if they think of the training as an investment for a better future.

# Conclusion

Having a contingency plan in place is extremely important when it comes to security and safety. Maritime industries need to be aware of all the threats that they could face so that it is easier for them to implement the necessary security measures. Having the right set of rules in place can prevent an organization from a massive security attack.