KISH P&I CLUB

Information Updates KISHPNI-IU-JULY-2022

(Data analytics in maritime industry & Cyber-Security Insights)

In the present digital age, competition is fierce in a variety of industries, including the maritime industry, and companies are constantly investing in solutions that can help them increase productivity while lowering overall costs. Consequently, the demand for advanced solutions such as marine data analysis is growing at an impressive rate among commercial shippers and other end users. In the shipping industry, big data is used to control sensors on a ship and to perform predictive analysis to avoid delays and improve efficiency. Enhanced decision making through big data analytics is being actively implemented to avoid and predict additional costs and can be used throughout the life of a ship. The Port of Hamburg (Germany), the Port of Cartagena (Colombia), the Port of Rotterdam (the Netherlands) and several ports in Southeast Asia are actively using big data analytics solutions for their port and terminal operations.

Predictive analytics solutions have the potential to transform the shipping industry by improving overall shipping operations, enhancing ship safety and protecting the environment. In addition, the high level of customization offered by these solutions, depending on the specific needs of any port or shipping company, is expected to fuel demand over the forecast period. With the growth of globalization, the demand for freight transport will increase significantly in the coming years. Consequently, the demand for advanced data processing and predictive analytics will also grow among maritime companies to maximize time efficiency and cost savings. These factors are driving the demand for marine analytics around the world.

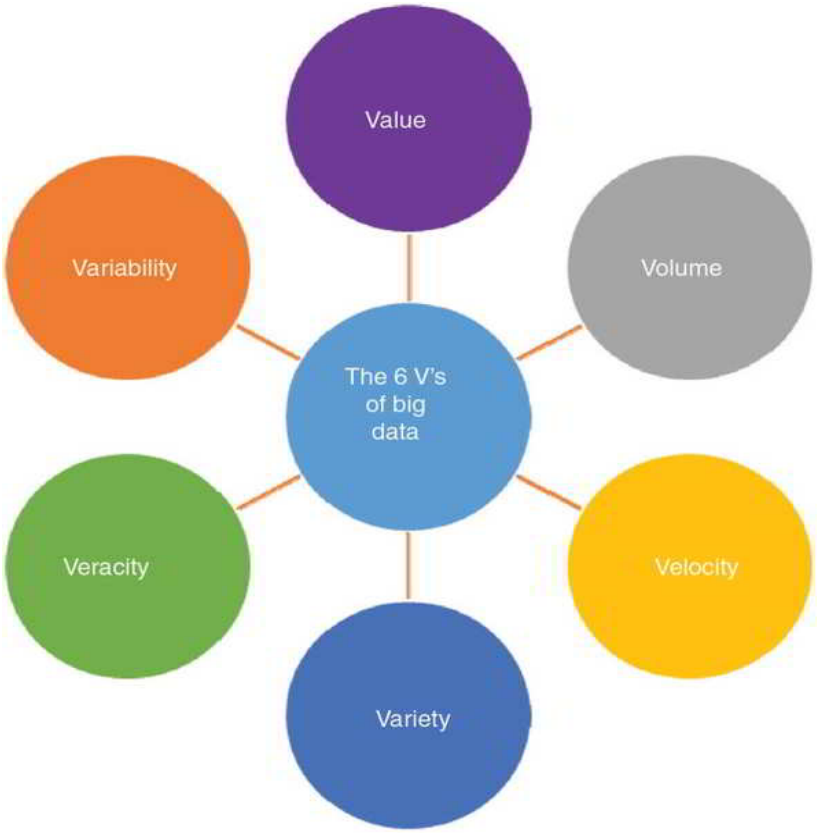
KISH P&I CLUB

The shipping industry is a complex network of people, countries, agencies and authorities. These include ship-owners, port authorities, maritime authorities, classification societies, cargo traders, oil companies and trade organizations to name but a few. This makes the industry a truly global enterprise. For example, a ship built in South Korea, owned by a Greek tycoon registered in Panama, manned by a crew from the Philippines, Singapore and Norway and could carry cargo owned by a US multinational company from a port in China to a port in Europe. Passing through the waters of a dozen other countries. The requirement to track economic flows in this global supply chain while eliminating any legal nightmares has led to extensive industry record keeping.

Some of these include:

- **Each ship has a cargo manifest and a crew manifest**
- **Each ship also maintains a captain's log, a ship's log and other logs, which record the internal and external condition of the ship, including equipment and environmental conditions.**
- **Ports, canals and waterways have many forms that you need to fill out to collect information about the vessel, voyage and cargo transported.**
- **Additional records are maintained by shipping agents, companies, traders, marine insurers, certification agencies, etc.**

Finally, ships generate huge amounts of electronic data such as AIS, LRIT, radar, etc. Electronic data is also generated by separate equipment on board.



KISH P&I CLUB

Given the variety and volume of data generated, Big Data in maritime and marine data analytics can be roughly divided into three groups:

1. Vessel management using data available in various logs, manifests, system parameters, bunker statistics, etc. This will include efficient bunkering, better vehicle maintenance using digital twins, crew management, etc.

2. Port and cargo management using data held by port authorities, freight forwarders, trading houses, etc. This will include efficient cargo handling, tracking goods, optimizing port facilities, etc.

3. Analysis of spatial imagery using data from position tracking systems such as AIS and LRIT, images from ships, coastal and space radars, optical sensors, etc. This will include efficient routing, fleet tracking, traffic pattern analysis and anomaly detection etc. soon.

Until recently, records were mostly kept for short-term transaction history or for autopsy in the event of any incident. Modern analysis methods now allow us to use this data to predict and provide information to improve the system and prevent future disruptions.

Much needs to be done to adapt to the changing landscape of data, software. Like the Internet more than 20 years ago, data analytics and the Internet of Things will change the world around us. No company can do it alone anymore. The right investments and smart technology choices are the keys to digital transformation. Collaborative innovation will support the development of the industry today and prepare it for what unfolds in the future.

The COVID-19 crisis is evolving rapidly, posing major challenges to logistics, supply chain, shipping and maritime traffic. In this scenario, data analytics and technology adoption are expected to gain traction in the post-COVID phase, which is expected to stabilize the maritime industry and push it towards growth.

The development process have formed 4 available solutions that are suitable for charters, ship-owners and fleet managers of different types of vessels for:

- **Weather routeing and voyage optimization for managing ETA**
- **Real time monitoring of vessel performance**
- **Predictive maintenance of equipment onboard**
- **Reduction in fuel consumption and GHG emissions**

KISH P&I CLUB

Cyber Security Insights:

Cyber-Security matters being a necessity in every Safety Management System may well be a good reason to have a look at some insights while talking about maritime data analytics.
The following insights on cyber security and its part in the shipping industry highlight that shipping is far off the goal, in regards to how it treats cyber risks. Important to note that to some extent, the COVID-19 crisis has had a positive impact on the digital evolution.

Starting the discussion, question was that where the industry stands concerning cyber security. All the insights agree that the industry has still a long way to go, in order to be fully protected from the cyber risks or adopt a notion of dealing with an attack.

Key takeaways on cyber security:
• There is a gap between technology and the measures to protect smart vessels
• IMO's Resolution challenges ship operators

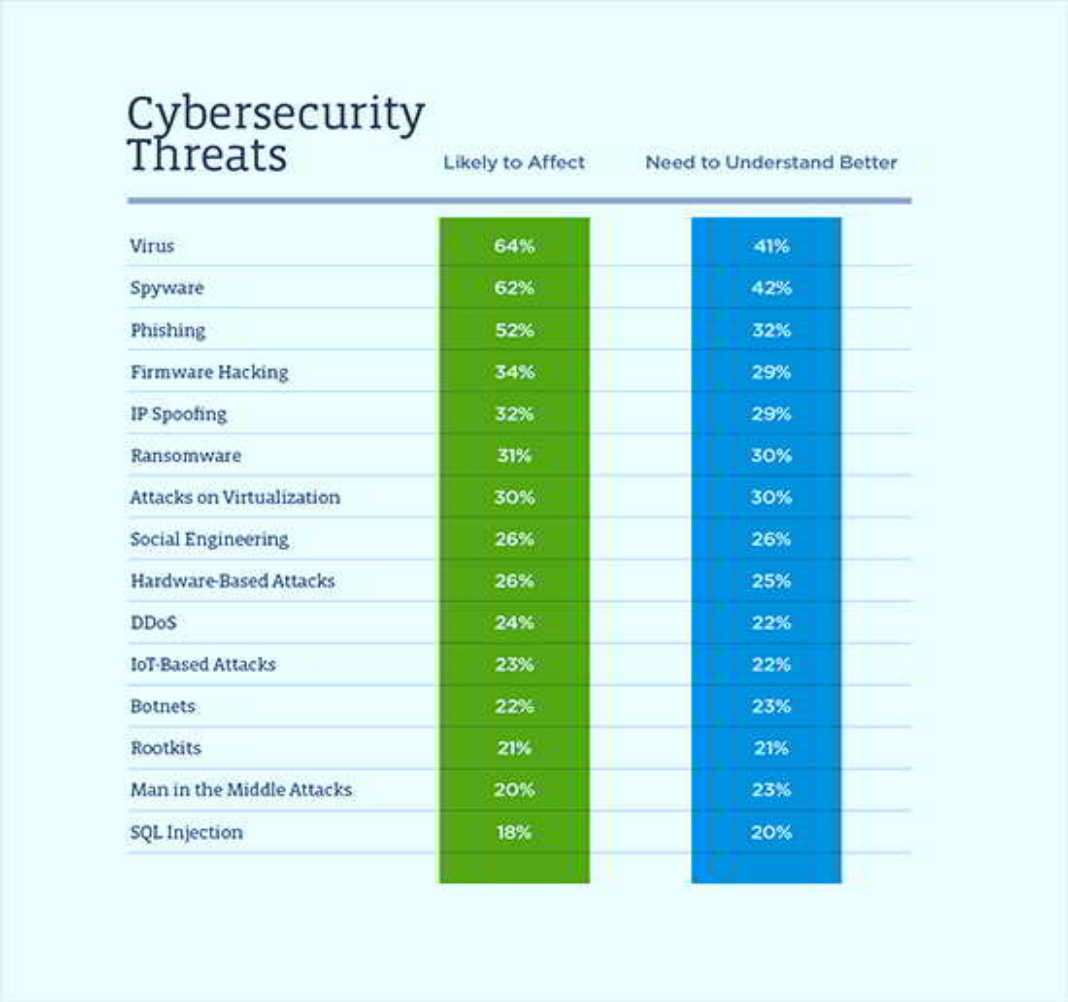
Shipping must improve its cyber resilience:
• 4 categories of cyber-hit companies
• The right mindset is needed to remain protected from a cyber attack
• It is important to understand/analyze the hacker's motivation
• Cyber safety & security has become a business imperative
• COVID-19 has accelerated digitalization

A RINA Senior Consultant, highlighted that there has always been a gap between the technology and its evolution, with how the industry protects the smart vessels and its technologies from attacks. He also focused on the importance of implementing risk assessment, as a crucial step to understand the challenges of cyber-attacks, and advised that shipping companies should begin their cyber security plans from the base; the port facilities and the vessels.
An IT Manager stated that although the resolution is here, technically, the sector is not 100% ready. In the meantime argued that the IMO's advice that cyber security should be included in the ship's SMS is a sign that the vessel's security and safety are merged.

During the discussion, four categories of cyber-hit companies were revealed;

1. The companies that have been hacked
2. The companies that haven't been hacked
3. The companies that have been hacked, but they don't know it
4. The companies that have been hacked and will be hacked again in the future.

The four categories reveal the gap existing in the shipping industry, with some shipping companies not focusing enough on the cyber risks, and acting like there is no risk.



Having the right mindset:
Having the right mindset to keep up with the evolution and the technological changes, plays a crucial role on how the industry will deal with the cyber security challenges arising.

In that regard, it is advised to keep in mind the following:

- Implement cyber security safety in a line manner
- Hackers do not stay idle; they evolve and improve
- Stay alert on anything not tested or used in the past
- For top security, you have to sacrifice cherished things, such as the easiness of doing things

The lack of mindset throughout the industry can be also seen on the way many organizations address cyber security. An example is the lack of awareness as to which assets to protect and which vulnerabilities to address. Moreover, another challenge remains the human error and the lack of training, which comes with the lack of cyber skilled staff that may lead to a cyber-attack.
Furthermore, the importance of understanding the motivation behind the hacker's attack, as argued that the attack is not only being done for the money. Referring to the geopolitical attacks, which are being done by people who make a living out of it, giving a geopolitical perspective in cyber-attacks.

Cyber-attack as a business imperative:
It was argued that the shipping industry is both aware and unaware of cyber hazards. The mentality noticed in the shipping sector is "cyber-attack might happen to somebody else and not to me". This shows that the industry remains partly ignorant of how severe a cyber-attack could be for both the shipping company, as it could lead to economic losses, as well as the vessel's safe operation, as it could lead to a fatality or severe casualty. Concerning the industry's evolution on handling cyber-attacks is not a wait and see situation.
In addition, cyber security has to be a business decision for shipping companies. In other words, as operations become more and more connected between vessels and companies on shore, it is highly crucial that shipping companies develop and implement a cyber-security plan.

COVID-19 role in digitalization:
The new norms arising during the pandemic is now remote surveys and inspections, as much as possible. In the question on how the COVID-19 impacted the shipping's evolution in the digital part, it is noted that the people of the sector quickly adapted to the new norms. In addition, it was stated that money spent on technology will always come with a fruitful outcome, as seen now. Technology plays a crucial role during the pandemic, from remote inspections to the majority of employees working from home.

Concluding that, cyber security regulations and their implementation will be a good start to drastically deal with the cyber risks. The mentality should be that whatever the regulations and legislations are, the industry has to change its mind and move forward.