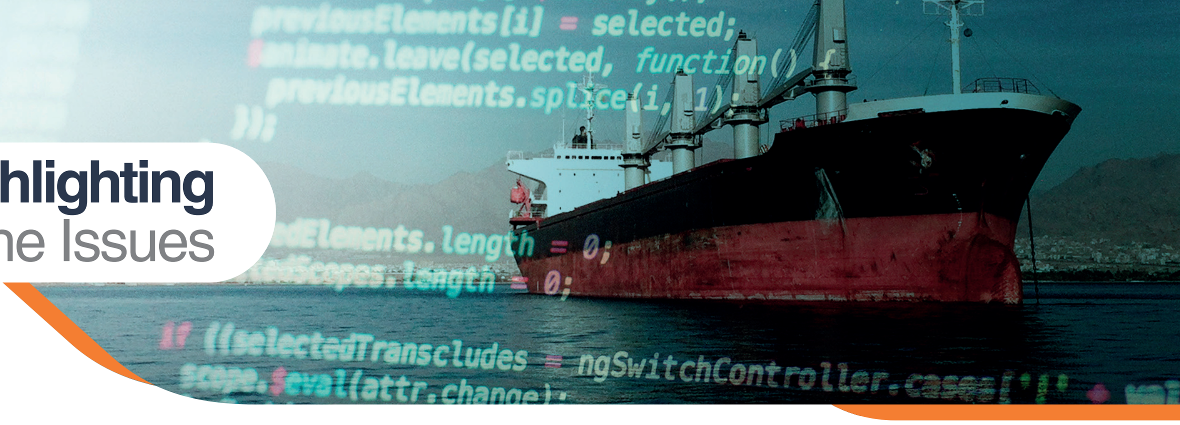


Highlighting
the Issues

Rafael Ageo
Junior Account Executive

FEB.2021

Why should cybersecurity be on everyone's mind?

Introduction

Information has become a critical asset in all types of corporations including the maritime industry. Protection against potential cyber threats to ships is nowadays essential in an environment where information is highly vulnerable to premeditated attacks.

In recent years, there have been many cyber-attacks examples like the virus which affected Maersk causing congestion in several ports, with an estimated cost of 255 million euros, as well as the reputational damage the shipping company suffered. Last year in 2020, another set of incidents happened to companies like MSC and CMA CGM in France. After disrupting their services, hackers even targeted the well-known IMO (International Maritime Organization) shipping's global regulatory body. Following the IMO's statement, "there was a disruption in their service caused by a cyber-attack". To curb this and other cases, companies must implement a cyber risk culture as well as an efficient cyber security management. In recent years, various guidelines have been developed by both national and international bodies, however, due to their complexity and increasing risk, it is necessary for maritime industry players, to accelerate and prioritise their own cyber management to comply with the various international legal obligations and to be able to continue their business efficiently.

At Atlantic, we believe that in the last year there have been three key factors, which have led shipowners to seek risk transfer to cover their cyber exposure.

Increased Connectivity

The advance and development of technology in recent years has made it easier to communicate and develop our lives in different areas, including government, business, among others. The use of cyberspace and/or any other system of interconnected networks, which contain features for the transmission of data, information, orders, or other processes; are constantly under cybernetic perils and threats, which materialise in effective cyber-outbreaks, causing large economic losses, affect image or reputation, and other types of damage to governments and companies in different sectors.

In the maritime industry, vessels are progressively using systems that depend on more and more on digitisation and automation, which in turn trigger the need for cyber risk management on board. As technology has developed, information technology (IT) and operational technology (OT) onboard ships have been networked together – and at the same time more frequently connected to the internet.

When facing a cyber-attack, we need to be aware of what the main assets are that can constitute as an easy target. Vessel systems and procedures that can be compromised by a cyber-attack include:

— Bridge Control Systems (Integrated Navigation Systems, Integrated Engine Control Systems, Door Function Panels, and others).

— Equipment used for navigation such as AIS, GNSS etc.

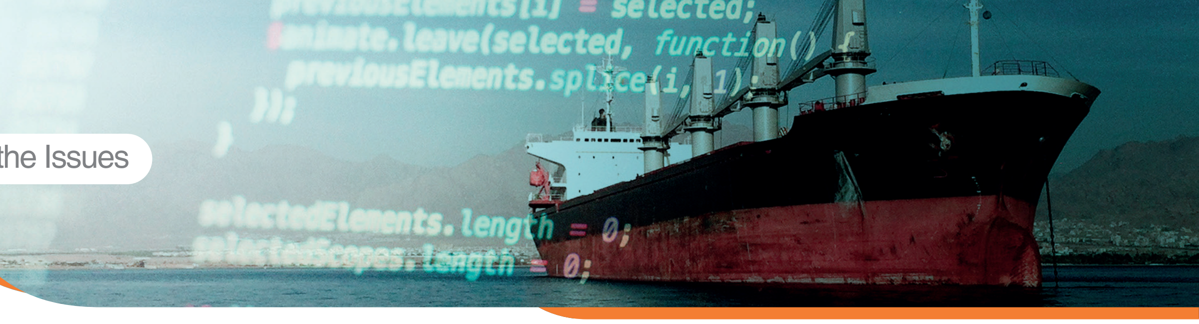
— Communications either through GMDSS or others.

— During cargo handling, calculation software, which is used for loading, stowage and unloading.

— Propulsion and machinery control systems.

— Access control systems either through CCTV or similar, authorization cards, boarding passes (PAX/RO-PAX vessels) among others.

One needs to also look at the risks ashore where shipowners´ organizational systems (The Maersk incident for example) cater for the operation and often also for the technical maintenance of the company´s vessels. Finally, reference should be made to crew and their online activities when off duty.


selected;
animate.leave(selected, function() {
previousElements.splice(i, 1);
});
selectedElements.length = 0;
selectedScopes.length = 0;

COVID-19

Remote working – triggers higher cyber exposure

COVID-19, naturally, is an important factor to consider. Restrictions imposed by governments to stop the transmission of the virus have encouraged many businesses to send their employees home where these then work remotely. Therefore, technology has become more important in both our working and personal lives, making us spend even more time online.

At the same time, COVID-19 has prompted many Governments to close their international borders, leaving hundreds of thousands of seafarers stranded on board of their ships. Last October more than 500.000 seafarers were affected, and a similar number of seafarers were prohibited from returning to their working vessels.

This compelled seafarers to turn to social media, communication Apps and other online platforms to communicate with home or surf the internet to have something to do as a pastime. Given the fact that a huge number of vessels are not sufficiently protected nor were prepared for this shift to massive online usage the exposure has grown significantly.

Regulatory Compliance

IMO:
Cyber Risk Management now mandatory (2021)

Finally, from the 1st of January 2021, as stipulated by International Maritime Organization (IMO) resolution, shipowners are obliged to include a cyber risk management schedule in line with the ISM code.

After adopting the Resolution MSC.428(98) aimed to address cyber risks in the maritime industry, the IMO encourages shipowners and administrators to include cyber risk management in their safety management systems. The IMO have also published guidelines to make this arrangement easier for shipowners and the method consists of the following stages:

- Assessment of Cyber Risks: shipowners must identify cyber perils in their vessels and operations.
- Design a secure Cyber plan: shipowners must create a cyber management schedule and risk management framework.
- Lastly, shipowners must protect their vessels by applying safeguards ensuring their operational resiliency.

Regardless whether one is a shipowner or operator, or whether proactive approach or not to the subject prevails, there is a now a legal obligation to comply with IMO/ISM cyber regulations and these procedures will have to be applied across the shipping industry.

Cyber now part of Tanker Management and Self-Assessment (2018)

From 2018, a new cyber security component was incorporated into the third edition of the TMSA. This was released by the Oil Companies International Maritime Forum (OCIMF) last 2017 and has become a fundamental commercial imperative for tanker operators, and they were addressed to carry out a self-assessment and rate themselves against the (KPIs) Key Performance Indicators included in the TMSA3.

In summary this new version of the TMSA included two new elements (Elements 7 and 13) that implied the establishment of an efficient Maritime Security and moreover addressed Cyber Perils:

- The mentioned elements required shipping companies to have in place a Cyber-Risk Management procedure for vessels, shore sites and the interaction between them.
- To put it succinctly, the Cyber Risk Assessment was to address all threats and mitigation measures as well as a response procedure.

In conclusion, TMSA3 has made cyber risk management a priority for tanker operators.

previousElements[i] = selected;
animate.leave(selected, function() {
previousElements.splice(i, 1);
});
}
selectedElements.length = 0;
selectedScopes.length = 0;

Conclusion

Overall, it is fair to say that the development of technology in recent years has much enhanced communication and connectivity in different areas, including government, business, and personal.

The mentioned development has allowed cybercrime to generate substantial business interruption (economic losses) and harm to image or reputation to companies in different sectors (one being the maritime industry) where numerous cases of serious cybercrime or even cyber activism have occurred.

At Atlantic we think that knowledge, preparation, and awareness of cybersecurity is the first step to protecting assets, processes, data, information, and the shipowner´s business model as such. Unfortunately, the exposure is growing every day and we will face greater challenges in this silent but powerful battle so we must be prepared to counter it.

As the offering of cyber preparedness, consultants and cyber insurance policy grows steadily we have undertaken a thorough review of the main risk transfer solutions out there – please contact Rafael Ageo or Richard Adler if you are interested to obtain further insight. We are convinced that shipping remains a very personal business and that every client therefore deserves a very bespoke cyber security consultation and ultimately a tailor-made solution, too.

Contact

RICHARD ADLER
Key Client Broker CCO
adler@atlanticinsbrokers.com
+44 7393 600 724

RAFAEL AGEO
Junior Account Executive
ageo@atlanticinsbrokers.com
+34 616 838 475

atlanticinsbrokers.com | atlantic@atlanticinsbrokers.com

MADRID
Núñez de Balboa 120
6ª planta izquierda
28006 Madrid
+34 915 638 632

LONDON
40 Gracechurch St
1st floor
EC3V 0BT London
+44 (0) 203 440 37 62

MIAMI
40 SW 13th St
Suite 902
Miami FL 33130
+1 305 377 7887

BOGOTA
Calle 76 N° 10-28
Bogota
+57 310 699 3585
+57 1 746 37 01

HOUSTON
1001 McKinney St
3rd floor
Houston
77002 Texas

ATLANTIC
INSURANCE & REINSURANCE BROKERS S.L.