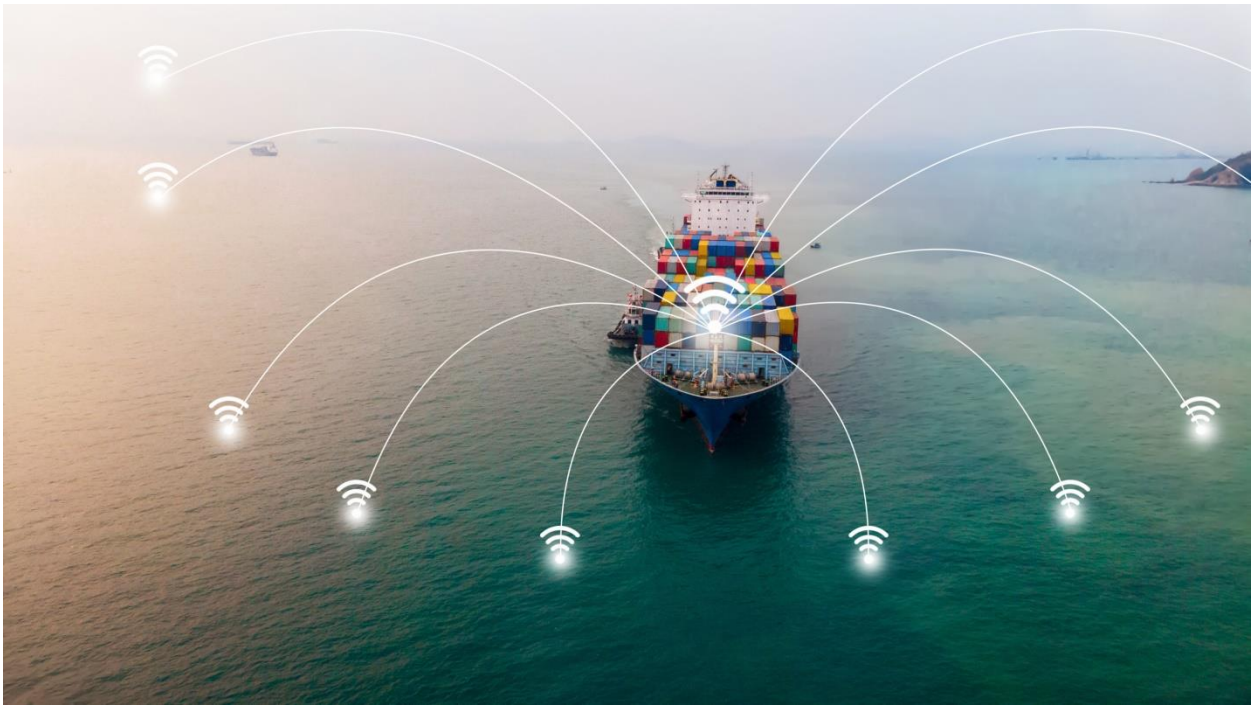
Maritime Cyber Risk: An Emerging Concern for Maritime Industry

S M Anisur Rahman



Introduction

Seas have always played a great role in defining the world's destiny, be it as means of transportation, trade routes or hub of resources. They have also played a significant involvement in bringing people closer, breaking barriers between cultures and religions as well as it helped in spreading new ideas and thoughts. Today, as we stand in the 21st century, seas are essential for the economy in addition to the military needs. Presently, almost as high as 90% of world trade and commerce is being conducted through the sea. The majority of the needed energy sources like oil, gas, and petroleum are extracted and transported through the seas. In fact, maritime trade routes form the lifelines of modern civilization. Today, the whole rhythm of human civilization's development and prosperity depend on the prowess of nations at sea.

Now, the entire world is evolving through digital know-how. Information security and data safety issues are critically important here. Even in the maritime sector, large IT companies develop complex software and hardware solutions; still, their internet platforms and loT (Internet of Things) devices often cannot provide them with the required level of cybersecurity. Like other developed maritime nations, the maritime sector of Bangladesh is also growing digitally. As a result, these maritime industries must be aware of the threat of adversarial cyber-attacks.

Present Digital Protection of Maritime Industries

According to CEOWORD Magazine Research, in 2021, Greece was the top maritime country in the world in terms of the maritime industry. Surprisingly, five locations in Asia (Japan, China, Singapore, Hong Kong and South Korea) were among the top 10 major players in this sector. Bangladesh, India, Pakistan, and Vietnam had significant maritime expansions in South Asia over the last few years. In 2021, during the COVID-19 pandemic, BIMCO conducted their annual Maritime Cyber Security Survey to examine how the maritime industries were handling digital protection in the wake of high-profile cyber incidents. A total of 350 individuals took part in the survey, filling out 25 questions in total. More than a fifth of respondents acknowledged that they had been victims of cyber-incidents, with 72% of these respondents mentioning that their companies were the victims of cybercrime-related incidents in the last 12 months. Phishing and malware-like viruses (49%), Trojans and worms (44%) were the most common form of incident faced by respondents, mostly leading to service disruption (49%) and system downtime (44%). Due to these attacks, 49% of respondents acknowledged that they had various service disruptions, except system downtime, reputational damage, financial loss, criminal activities, cargo theft etc. The survey also revealed that all the incidents had cost involvements. Many cyber incidents occurred exclusively onboard ships and caused multiple damages. The shipping agencies are also targeted to manipulate various information, e.g cargo data, crew and passengers documents, etc. In July 2021, Sky News reported that only cyber attackers from Russia had spoofed ships' GPS at least 7,910 times between 2016 and 2019, affecting about 1300 commercial ships. In 2017, North Korean navigation jamming was said to be behind the forced return of hundreds of South Korean fishing vessels, and its cyber-attacks led to the devastating NotPetya attacks that crippled the large Maersk shipping line in the same year.

What is Maritime Cyber Risk?

International Maritime Organization (IMO) defined the, maritime cyber risk as ‘To a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping- related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised’. Many globally connected networks and infrastructures at sea still leverage legacy technologies that are not built to be connected to the internet. These complex networks include a blend of Information Technology (IT) and Operational Technology (OT) systems and are used by internal crew and third-party vendors, extending the potential for compromises by hackers or even insider threats.

There was a time when connectivity on a vessel was minimal, and ship control engineers addressed security issues with air-gapping to physically isolate a secure network from unsecured networks. By definition, an air-gapped system is neither connected to the internet nor any other system. But now, using something as simple as a USB flash drive or unsecured Wi-Fi connection, a malicious hacker or even an inexperienced insider can infiltrate and infect critical systems. This development is especially concerning because of the connectivity of modern maritime vessels to the internet or external devices. These may cause instability or mistrust of bridge control, propulsion & power, navigation, loading & stability, safety systems, communications, operations security, network security, physical security, ship networks and the e-supply chain of any marine vessel. In recent days, significant technological advances in navigation, communication, and propulsion systems are becoming more ubiquitous, providing the crew with a more comprehensive view of what is happening inside and outside of a ship. Even in the ocean or high sea, ships may always need to be globally connected. As a result, the requirement for human crewmembers is being reduced day by day to man modern ships. This dependency on technologies increases the vessel's presence in the cyber domain, increasing its chances of being targeted and offering new vectors for such attacks. Thus, any modern vessel is always at risk or may be targeted for the following cyber-attacks:

> Denial of Service (DoS): Targets the availability of data

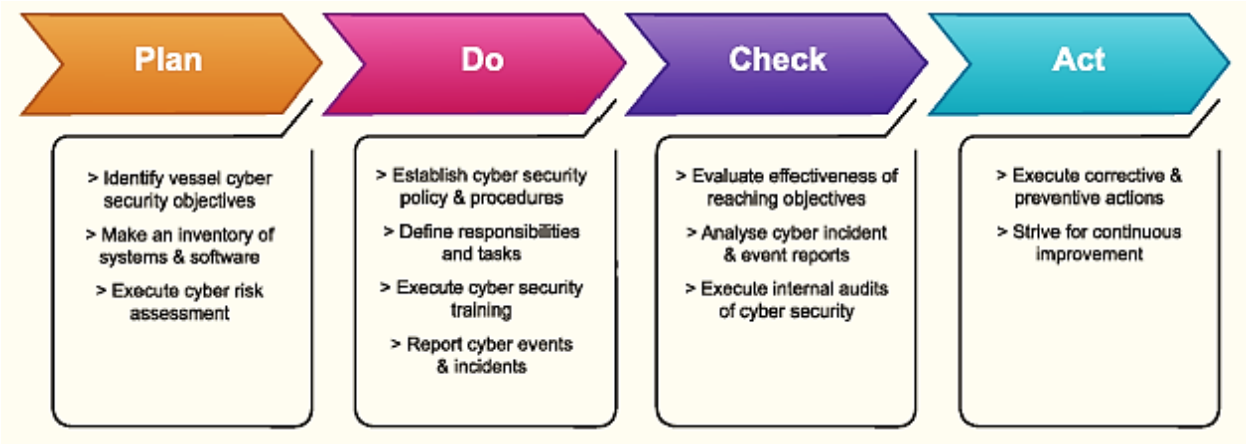
> Spoofing: Targets the integrity of data

> Packet sniffing: Targets the confidentiality of data

>Replay/Man-in-the-Middle (MITM): Targets both confidentiality and integrity of data

International Maritime Organization (IMO) Safety Code and Its Challenges

IMO has included a cyber-chapter with specific compliance terms, including mandatory obligation: MSC-FAL1/Circ.3 guidelines on maritime cyber risk management. According



to the regulation, all vessels are required to implement the necessary cybersecurity measures no later than January 2020. The said regulation mandates the implementation of several layers of protection to be implemented in addition to conducting a cyber-risk assessment. IMO regulation is part of much larger guidance and standards such as BIMCO, CLIA, ICS, OCIMF, ISO/IEC 27001 standard on information technology, and the United States NIST framework for improving critical infrastructure for cyber security.

Though IMO is cogent about maritime cyber risk management, most shipping industries face many challenges to accomplish. The following are some of the most common cybersecurity challenges faced by the maritime industry, which are similar to those faced by other industries that engage with IT networks:

> No clear understanding of all systems and devices on the Operational Technology (OT) network across a fleet or operation

> Lack of visibility into each vessel's OT networks

> Lack of real-time monitoring or segmentation of the OT network

> Inadvertently connected IT and OT networks

> Use of unsecured wireless networks

> 24/7 remote access granted to third-party from Original Equipment Manufacturer(OEM)

> Lack of visibility into third-party OEM networks (black box)

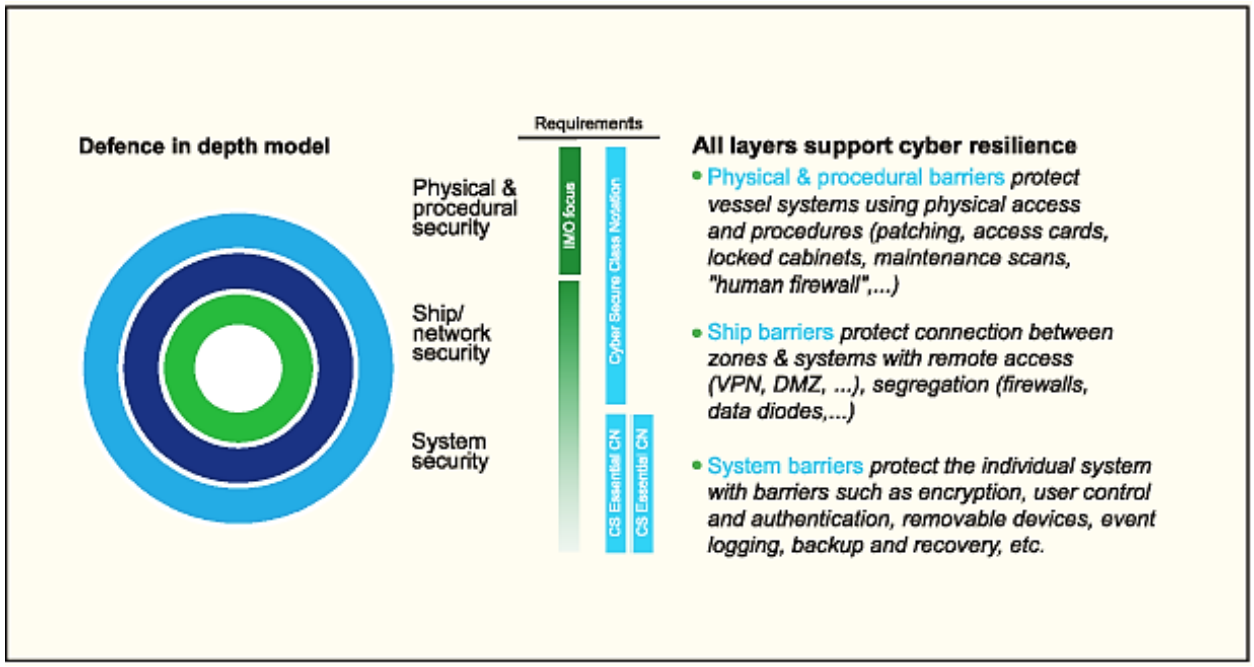
> Poor physical security controls

> Lack of cybersecurity awareness among the crew, employees and contractors

Cyber Risk Mitigation Approach in Shipping

An essential step to mitigating cyber-attacks on maritime vessels is updating existing ship systems and, more importantly, designing ships for increased security. It does not necessarily require fancier and more expensive equipment but can be achieved with intelligent isolation of different and more secure systems which is still usable, e.g. password-protected. Machineries or systems subject to compromise must have recovery mechanisms. Furthermore, the provision of alerts for instability in all loT devices and inter/intra connected systems should be obligatory. It will also help to detect exploitation by any vector for cyber-attack. Here the resilience of command and control systems is also essential. The modern navies are already developing Resilient Hull, Mechanical and Electrical Security (RHIMES), which aims to introduce diversity and prevent the same exploit from succeeding on multiple controllers. However, as these systems are currently limited and shall be limited until the next generation of ships, it is prudent to take advantage of the human element onboard ships. A human crew may be advantageous in many ways in terms of security. Firstly, the crew may verify that the systems function as intended. Secondly, if the systems are modified only by the authorized and trained crew, it is more difficult for an attacker to go undetected during any potential cyber-attacks. Training on how to keep these systems secure is also essential. There are many cyber risk management models which can be followed onboard marine vessels. One of the most followed processes is Plan-Do-Check-Act (PDCA) model.

In the PDCA model, the first step in the 'Plan' phase is to identify cybersecurity objectives relevant to the vessel's safe operation. In addition to the IMO requirements, other internal and external stakeholder requirements on cybersecurity should be accounted for when determining the objectives. In the "Do' phase, the cyber risk assessment results should be utilized to define an implementation plan for rolling out



suitable barriers. In the "Check" phase, the effectiveness of the cybersecurity measures must be checked continuously. In the 'Act' phase, corrective and preventive actions should be implemented based on the findings of the internal and external review reports.

Another widely followed cyber risk management process is the 'Defence in depth' model, applied on different ship safety layers, commonly known as barriers. These barriers are implemented based on IMO security requirements and cybersecurity guidelines, which confirm the marine vessel's system, network, and physical security. As the vessels and systems are increasingly interconnecting and malicious cyber threats are continually changing, the key to future successful cybersecurity resilience is to improve continuously by updating the cyber risk assessment, policies and procedures.

Conclusion and Way Forward

Any marine vessel that is built is usually put to use for a long time. Though all the marine vessels maintain their routine maintenance from time to time, most of the firmware of the core systems remains untouched. Thus, the software used by the hardware becomes outdated. Often ships are being built without cybersecurity in mind. As a result, the possibility of being attacked by the vulnerable vector/threads is becoming an emerging concern for maritime industries. Both security firms and hackers have found specific and real-world flaws within the systems running in the maritime industry. To date, several successful cyber-attacks have been launched on the navigation systems of ships. Presently, all modern ships are designed with integrated compact modules that include communication, navigation, propulsion and cargo handling systems. This integration leads to the probability of being infected by any of the systems and being compromised by cyber-attackers. International Ship and Port Facility Security (ISPS) should be expanded beyond physical safety and security aspects. Revisions of national and international legal as well as regulatory frameworks are also necessary to fight against cyber-related maritime threats.

Writer: Lt Cdr S M Anisur Rahman, (H3), BN is the Director (Admin) of BIMRAD

The article was published in PAAL Magazine, Volume 05, Issue 01, April 2022