ENHANCING CYBER SECURITY AWARENESS IN MARINE INDUSTRY

Capt. Mihir Chandra

Abstract:
Cyber security is the combination of stakeholders, policies, processes and technologies to protect cyber assets of any industry. It is optimized to levels that help shipping personnel define, balance resources required with usability/manageability and the amount of risk offset. The aim of this paper is to develop understanding and awareness of key aspects of cyber security – identify threats, identify vulnerabilities, assess risk exposure, develop protection & detection measures & establish contingency plans. Furthermore, establish guidelines for operators on how to assess their ship's operations & put in place necessary procedures and actions to maintain the security of cyber systems for marine industry. The integration of technology in shipping operations is being enabled by the integration of Information Technology and the Operation Technology on board ships. This has enhanced the threats of unauthorised access or malicious interventions to ship's systems and networks. The measures to guard against cyber threats should include, (i) quantification and type of risks to security, environment and commerce if no cyber security measures are in place, (ii) due protection to IT and OT infrastructure and its networked equipment, (iii) management of access (iv) protecting data related with its sensitivity. With emerging technologies, there is a direct applicability of trends like Artificial Intelligence to enhance security and fraud prevention. Extending the use of Security Analytics for understanding and detecting risk level of vulnerabilities, improving the performance of own security policy by removal of unnecessary data, feature extraction and selection, data cut off, parallel processing, machine learning and deep learning algorithms – are some examples for the use of advanced technologies for improving Cybersecurity.

Keywords:
IT- Information Technology
OT- Operation Technology

1. INTRODUCTION

On average, hackers attack 2244 times a day (University of Maryland)

Digital era has given many pluses but one of the major negatives hitting hard to netizens is 'cyber-attack'. And Ships, when exposed to interference from one of the many electronic navigation devices, such as the Global Positioning System as the crash rate increases to 70%,or if bugged with viruses in cargo work/ in sensitive and seamless documentation, and /or in the propulsion units of engine room or in machines , any or all can cause serious trouble to the ship owners .And on the blocks now are Autonomous ships and block chain technology for activities of marine logistics and support systems for end to end functions .

In cyber security terms, risk is the potential for a threat (a person or thing that is likely to cause damage) to exploit a vulnerability (a flaw, feature or user error) that may result in some form of negative impact (National cyber security centerUK,NCSC)

The integration of technology in shipping operations is being greatly enabled by the networking of Information Technology (IT) and the Operation Technology (OT) onboard ships over the worldwide web and Internet of things (IOT) is a common happening. Growing use of big data, smart ships, and IOT, is now increasing and therefore the amount of information are getting accessed by attackers of cyberspace. Hence the threats of unauthorised access or malicious attacks to ships systems and networks get greatly heightened. There could also be risks arising from the inadvertent introduction of malware from say removable media by untrained or unaware personnel and compromising the systems and data. Cyber threats are thus a reality and there is need to be aware of how this could work making the systems vulnerable to its attacks.

It becomes imperative that ship-owners and operators regularly assess their operations and develop resilient approaches to safeguard the security of cyber systems onboard of their ships.

56% of IT decision makers believe phishing attacks are their top security threats. 32% of the breaches involved phishing. So phishing awareness and education are some of the best ways to decrease risk. The most common cyber-attack methods include phishing/spear phishing/vishing (voice phishing), rootkit, SQL injection attacks, DDoS attacks and malware like Trojan horse, adware and spyware.

Who might be attacking you? Geo political trade interests, Ship-manning agencies, Chartering and shipbrokers' agencies and cross-border intel- agencies, interested in gaining an economic advantage for the host companies or flag-states. They are Hackers who find interfering with computer systems an enjoyable challenge. Hacktivists who wish to attack companies for political or ideological motives. Employees, or those who have legitimate access, either by accidental or deliberate misuse.

2. Objective: To find out the factors which become a part for awareness and mitigation drive of cyber risk, threat, vulnerabilities in hindsight, at hand and as a foresight to be prepared for treading in uncharted terrains of new possibilities in shipping industry

2.1Discussion-

The cyber risks usually are specific not only to the company and the ship depending on the technology usage, but also its area of operation and the trade they are in. The challenge here becomes manifold due to the fact that no historic data or evidence can be relied upon to get any definitive information on the imminent incident or its impact, unlike the traditional areas of concern on

1. *Research Scholar and Associate Professor, Department of Nautical Studies, Indian Maritime University, Mumbai, India, Email: mchandra@imu.ac.in*

safety or maritime security. The motivation for cyber-attack could range from operation disruption to damaging the reputation to financial or political gain or even plain espionage. The threats could emanate from internal sources like disgruntled employee or outsiders like criminals, opportunists, terrorists or just activists.

There are mainly two types of cyber-attacks – untargeted and targeted. Untargeted attacks happen over taking advantage of the openness of the internet without bothering so much about who the victim is. While targeted attacks are when organizations are singled out for a specific interest and can be more dangerous.

2.1.1 Untargeted Attacks: In un-targeted attacks, attackers indiscriminately target as many devices, services or users as possible. They do not care about who the victim is as there will be a number of machines or services with vulnerabilities. Following are few techniques by which internet becomes slave to attackers which include:

- ''Phishing'' – 'sending emails to large numbers of people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.'
- ''Water holing'' –'setting up a fake website or compromising a legitimate one in order to exploit visiting users.'
- ''Ransomware'' – 'which could include disseminating disk encrypting extortion malware'.
- '' Scanning ''- 'attacking wide swathes of the Internet at random

For ships, untargeted attacks are one where a company or ship's system and data are one of many potential targets'.

Targeted Attacks: In a targeted attack, your organisation is singled out because the attacker has a specific interest in your business, or has been paid to target you. The deliverables are used to penetrate system or users through the optimized path and it is done after investing lot of data and time by attacker. Indigeneity which is engineered and applied in targeted attacks are more sophisticated as they are very specific and so they are more dangerous than non-targeted attacks. For ships targeted attacks are like the system or data being intended targets.

Targeted attacks may include:

- ''Spear-phishing'' - sending emails to targeted individuals that could contain an attachment with malicious software, or a link that downloads malicious software
- ''Deploying a botnet'' - to deliver a DDOS (Distributed Denial of Service) attack
- ''Subverting the supply chain' - to subvert equipment or software for the organisation
- ''Vishing''- voice phishing by adversial AI.

- Water ingress alarm system
- Ballast water system
- Gas liquefaction
- ODMCS-GPS interdependency-compatibility
- Various documents –E-bill of lading, E-logs, E-oil record books (forthcoming MEPC resolutions for MARPOL-to be enforce)

Passenger Services:

- Property management system
- Medical records
- Passenger embarkation access control
- User authentication and authorization system
- Passenger or seafarer boarding with own own device [BYOD]
- Passenger Wi-Fi /-LAN internet access
- Entertainment system
- Communication

Administrative and crew welfare system:

- Certificates in digital format, Seamen-identity document for example
- Quarantine digital reports

Other activities related to shore-side are also as below:

- Berthing /Unberthing activities
- VTS-Pseudo VTS
- Port related documentation-FAL Convention
- C and F agencies
- Port access control
- Tanker and Gas terminals—safety, security, pollution related access, operation, spoofing.

Regardless of whether an attack is targeted or un-targeted, or the attacker is using commodity or bespoke tools, cyber-attacks have a number of stages in common. Some of these will meet their goal whilst others may be blocked.

2.1.2 Stages of an attack

The attacker is effectively probing your defences for weaknesses that, if exploitable, will take them closer to their ultimate goal. So following stages are worth as a learning – lesson.

A number of attack models[13] describe the stages of a cyber-attack. A simplified model is taken that describes the four main stages present in most cyber-attacks:

- 'Survey'' - investigating and analysing available information about the target in order to identify potential vulnerabilities
- 'Delivery' - getting to the point in a system where a vulnerability can be exploited
- 'Breach' - exploiting the vulnerability/vulnerabilities to gain some form of unauthorised access
- 'Affect' -carrying out activities within a system that achieve the attacker's goal

When assessing vulnerability and impacts, the three areas that should be measured are: Confidentiality, Integrity and Availability. The measures to guard against cyber threats include:

(a) assessment of risks to safety, security, environment and commerce if no cyber security measures are in place

(b) due protection to IT and OT infrastructure and its connected and networked equipment

(c) managing access, and

(d) protecting the data depending on its sensitivity

3. Literature review:

- Marine Security professionals have additional resources to defend vulnerable networks and data from cyber attackers - combine the strength of artificial intelligence (AI) with cybersecurity. The use of AI yields automated processes - including continuous risk assessments, autonomous incident response, configuration monitoring, and automatic remediation and integration of security solutions and data. There is a significant reduction in response time to cyber-attacks. According to a report published by *Capgemini*, about 42% of the companies studied had seen a rise in security incidents through time-sensitive applications. However, the use of Artificial Intelligence in addressing areas of cybersecurity can be a considerable threat to ships, apart from being potential solutions[11] (double-edged sword)
  Study from Varonis[9] suggests that 21% of files are not protected and so it suggests for a paradigm shift in cost versus security processes.
- Digital ship newsletter and 'g captain' article of 11th March 2020 has shown through Digital container shipping association's publication named as DCSA cyber security implementation guide, the best practices –manageable task based approach towards meeting IMO resolution[1] MSC.428(98) implementation schedule for January 2021.
- An article by H.A. Boyes[10] suggests that 37% of data breaches were attributed to malicious and criminal acts. The remainder were split between system glitches (29%) and human factors (error/negligence) at 35%.
- Incidents of vessels[10] 'Royal Majesty' highlights the GPS/Autopilot problems, whereas vessel ANNABELLA' suggests of loading software glitches.
- Indian news agencies have reported on 10th March about Data theft of about 3 Lac or more people from Australia from Facebook account by a firm.
- International Maritime Organisation has instructed that by January 2021 all member states to take measures to mitigate cyber threats and adopt policies in safety and security related endeavours to create a sort of preventive mechanism of cyber security.
- In 2017, on June 27, AP Moller-Maersk[8] confirmed that the group was hit as part of global cyber-attack named 'PETYA', affecting multiple sites and select business units. The cost to company for recovery was about 200 to 300 million USD.
- Press trust of India reported that at Jawaharlal Nehru port trust Shewa, Panvel, Maharashtra APM MAERSK faced disruption in operation due to cyber- attack.
- Antwerp Port faced cyber -attacks with respect to containerised cargo getting stolen during 2011-2013 by organised cyber- crime by breach to IT system.
- A survey by IHS fair play in 2017 shows that out of 300 industry responders 65 had been attacked through cyber space. Malware apparently found to be of main attack nature.
- In July 2013 a test was done by research scholars of University of Texas, Austin, for GPS spoofing to a sailing yacht and it was achieved successfully by creating false civil GPS signal
- July 2015, South Korea reported of GPS jamming which paralysed all navigation and auxiliary systems on board. It was intentional interference of Geo-political nature.
- A report by Hugh Mcdowell [7]in 'Quantitative assessment' shows that the risk of cyber-attack is excluded from Insurance cover by ''Institute cyber-attack exclusion clause' [CL380] ,10November 2013. Though P&I CLUB has pooling facility with limit of 30 million USD per ship, provided attack is not an act of war or terrorism.

With the literature survey done, it is observed that a specific network architecture should be in place for assessing the systems as it is demand of the day with threat perceptions looming larger by every passing day when autonomous ships will be plying across waters and their function will depend mostly on, Information communication technology, ICT, high integration of systems and their connectivity with shore system and internet. A contingency

plan to be ready to Identify, Detect, Respond, Recover processes[12]for cyber attacks.

4.Conclusion :

Shipping industry is a unique but complex organization wherein different stakes are existing for different vendors having long life periods, systems, and vessels which are almost different to each other in network topology. This industry had plenty of case studies of damages, loss of life and claims of cargo losses in past and analysis of yore shows the human element for the failures and resulted error chain dynamics, but now it is at hand to deal with human element act from remote to do intentional, unintentional, targeted or untargeted attacks without being with the machine on board. STCW, ISM, ISPS codes did deal with filling the gaps of KSA – by having KPIs. Now the need is to train the manpower of industry with essential security tools, paradigm realignment with cutting edge technologies.

With the shipping industry's increasing reliance on technology and remote monitoring, maritime cyber security is no longer optional, but is business-critical. It is imperative that companies are ready to tackle the cyber challenge and remain resilient. Whilst the risk is real, a company can only be resilient to get up back to business if their cyber-preparedness is swift and up to date and it needs investment in real sense to pay dividend. Artificial intelligence, though is double edged sword; it is still need of the hour in this industry to cap the human element body as integrated with. Sound cyber capability in shipping is need of the hour which may be jacked up by inculcating disciplined appropriate systems, by training and resources in place to effectively hone the skill and knowledge to use Artificial intelligence cyber security solutions and by employing the 'White hat hackers' system of Artificial intelligence to counter Adversial intelligence's neural networks and also to raise the cyber defences. At length it is summarized as to have tough international digital legislation, to have commonly managed appliances and last but the most important of all to impart cyber related education to user as Human being the weakest link in the length of this Shackle and needless to add a shackle length of cable is as strong as to every link.

Disclaimer: This paper is not intended to be a standalone or exhaustive guide to cyber risk management. Users to ensure about specific guidelines for specific need of ship-types.

Acknowledgements: Thanks with humility to Dr, (Capt.) S. Bhardwaj , Resident Director and Principal ,MASSA Academy Chennai, Dr. K.Sivasami , Associate Professor, HoD, SMET and to all my colleagues at IMU-NMC/CC, for guidance and support in this endeavour.

References-

1. IMO resolution MSC.428(98) –Maritime cyber risk management in SMS.
2. Bhardwaj; (2018). Technology integration in shipping –potentials and challenges.ISBN:978-81-933569-6-8. ISF Institute of research and education, Mumbai.
3. UTNews. http://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an 80-million-yacht at sea.
4. BIMCO. The guidelines on cybersecurity on board ships,2017
5. IHS fairplay, Maritime cyber security survey 2016
6. Hugh McDowell. Munin D 9.3: Quantitative Assessment 2015
7. Laguvardou.S. 'Maritime cyber security concepts, problems and models, DTU Management engineering, University of Denmark
8. MAERSK.AP Moller A/S (22756214)2017
9. http://www.varonis.com/blog/cybersecurity statistics/
10. Boyce,H.A. , Resilience, security and risk in transport,2013,pp.56-63,The Institution of engineering and technology,Stevenge,UK,ISSN-2041-5923
11. Thesslstore.com/blog/AI-in-cyber-security-the savior
12. National institute of standards and technology, US Department of commerce.
13. How cyber attacks work- NCSC.GOV.UK