IJSTA

International Journal of Scientific and Technical Advancements

ISSN: 2454-1532

Cyber Preparedness in Maritime Industry

N.Kala[1], Mahesh Balakrishnan[2]

Director i/c, Center - Cyber Forensics and Information Security, University of Madras, Chennai – 600005
[2]Information Security Consultant, Chennai-600080,
[1]kalabaskar@gmail.com
[2]mahesh.balakrishnan@live.com

Abstract - Automation, digitization and integration drive maritime industries now more than ever. The maritime infrastructure is more reliant on cyber technology. Consequently, cyber security has been a major cause of alarm in maritime industry. Cyber related incidents involving navigating, movement of cargo, and other processes threaten lives, environment, property, and considerably disrupt maritime trade movement as a result of cyber-attacks. Compared to other areas of protection and security, cyber risk management is more challenging due to lack of information about the cyber-attacks and its impact. Until this information is acquired, the impact and probability will continue to be uncertain. Recent experience of cyber-attacks in maritime industry and from other business sectors such as banking, finance and insurance sectors, public administration and airline industry have shown that any successful cyber-attacks might result in substantial impact in providing services and compromise on safety of organizations assets. The main objectives of cyber-attacks in the maritime business include media attention, denial of service, access to system targeted, selling stolen data, hold the organizations for ransom on stolen data and system operability, organizing fraudulent movement of cargo, gathering intelligence on precise location of the cargo, ship transportation, handling plans, circumventing cyber security defenses, financial gain, disruption of economy, gaining knowledge about critical information/national infrastructure. This paper focuses on the cyberspace risks related with maritime industry and cyber preparedness in current global context.

Keywords - Dedicated Maritime systems, Cyber Risks, threats and Vulnerabilities; Cyber Security, Cyber Preparedness.

Introduction

Maritime Industry

The maritime industry includes all enterprises engaged in the business of designing, constructing, manufacturing, acquiring, operating, supplying, repairing and/or maintaining vessels, or component parts. The industry manages and operates shipping lines, and customs brokerage services, shipyards and dry docks. Maritime transport is responsible for about 85% of global trade. The act of carriage of cargo using shipping services offered by shipping lines, the processes involved in getting the cargo from the manufacturers warehouse to the receiver’s warehouse including arranging for shipping services offered by the shipping lines using the ships and anything related to the ocean, sea, ships, navigation of ships, seafarers, ship owning and other related activities.

Cyberattack

Cyberattack is an offensive exercise that targets computer information systems, infrastructure, computer networks, or personal computer devices. An attacker is a person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent. A cyber-attack can be employed by nation-states, individuals, groups, society or organizations. A cyber-attack may originate from an anonymous source. A cyber-attack may steal, alter, or destroy a specified target by hacking into a susceptible system. Cyber-attacks can range from installing spyware on a personal computer to attempting to destroy the infrastructure of entire nations. Cyber-attacks have become increasingly sophisticated and dangerous.

Manufactured products, oil, natural gas, raw materials, and agricultural products move through ports every day. While these are manufactured in many locations, they are transported to ports via rail, truck or specifically designed pipelines, where they are loaded onto ships and barges for export to other international destinations. Worldwide, the maritime business is making increasing use of technology for business and operational functions.

Vessel and service operators use computer systems and inter-connected technologies for navigating, communicating, engineering, movement of cargo, ballast, protection, and environmental mechanism. Ports use computer-generated systems to work with drawbridges, control traffic lights, schedule trucks to deliver, pick up containers and SCADA systems to control pumps, valves, and pipelines delivering fuel.

Dedicated Systems

Emergency systems such as security monitoring, cameras, fire detection, and alarms increasingly rely on cyber technology. Various cyber dependent dedicated systems associated with maritime industry is illustrated in figure1.

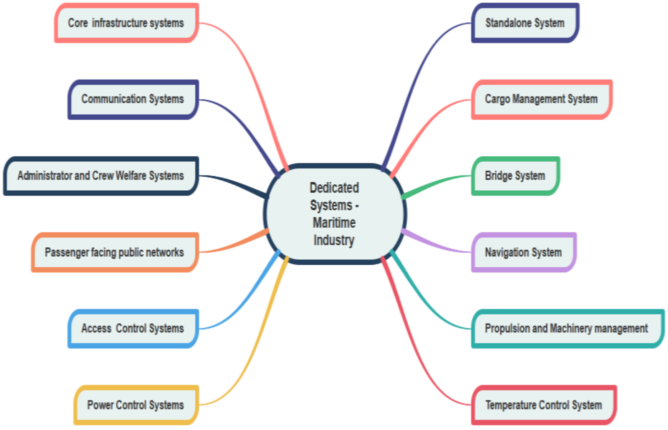
Core infrastructure systems
Communication Systems
Administrator and Crew Welfare Systems
Passenger facing public networks
Access Control Systems
Power Control Systems
Dedicated Systems - Maritime Industry
Standalone System
Cargo Management System
Bridge System
Navigation System
Propulsion and Machinery management
Temperature Control System

Figure 1: Dedicated systems associated to maritime industry

The maritime business uses interconnected cyber network to enable financial transactions, implement contracts, place orders, and perform related business functions over wireless networks compared to other businesses.

The international aspect of maritime transportation means that operators use interconnected cyber systems to provide ship, cargo, passenger, and crew information to customs officials around the world. While these technologies enable maritime industry to be efficient and reliable, they introduce risks. Exploitation or disruption of the interconnected cyber systems cause disruption of trade and harm the maritime industry.

Vessels use geographic position system for navigation on exclusively networked GPS, while using the same technologies for cargo tracking control. Any disruption, multiple points of failure via a disruption to the GPS signals or malware, controls the way the signal is read, exhibited and used on the vessel or facility. There are various intentions for organizations and individuals to exploit these vulnerabilities.

Those who target the maritime industry include but are not limited to, or hacktivists, disgruntled employees, cyber criminals, opportunists, state sponsored attacks and terrorists. The motivation of such attacks includes reputational damage, disruption of operations, financial gain, commercial and industrial espionage, competitive intelligence, challenge, thrill or political gain. Understanding cyber security threats and risks is illustrated below.

Threat Actors

Motivation: Disruption, Espionage and Financial Gain

Outsider

- Hacktivists
- Nation State Sponsored
- Criminal Syndicates
- Terrorists

Insider

- Accidental/Unintentional
- Malicious Deliberate Insider
- Disgruntled Employees

I. Cyber Vulnerabilities in Maritime Industry

While cyber system exposures in shipboard systems are startling to professionals, it requires an unusual skill set and precise timing to exploit these vulnerabilities to disrupt shipping operations or cause alternatively a serious maritime casualty. GPS jamming is one such weakness.

GPS Jammers produce a signal on the same frequency comparable to that from the Global Navigation Satellite Systems (GNSS) at a very close range, overriding the dependable signal. The incidents related to jamming signals are particularly difficult to locate when operated in a thickly populated area. Disrupting shipboard navigation requires a GPS jammer to be placed in the vicinity of the GPS probes onboard the ship and control through steering of a regulated area. Interference in the GPS signal would activate an alarm on the navigation system, enabling a priority to manual systems to autopilot.

It is questionable that the interference of GPS signals places a vessel in a dangerous position, provided the signal officer is alert and acts in accordance with his or her training and procedures. While this example portrays a radio signal manipulation, not a cyber-attack, it still exposes the risks of navigation in an example that discloses the tip of the iceberg.

The voyage data recorder (VDR) is another area to show cyberspace vulnerabilities.

A VDR resembles an aircraft's black box and essential component during investigations. It accounts inputs like bridge audio and VHF communications; vessel's position, speed, and heading; watertight and re door status; radar, ECDIS, AIS, and echo depth sounder data; and other information, as required by international regulations. Hackers can control data captured by the VDR.

For instance, a hacker can use this vulnerability to shield the cause of an attack or get rid of evidence of criminal activity on-board a vessel. Although the risks related with VDR vulnerabilities is marginal since VDRs don't directly control the movement of a vessel, such vulnerabilities could cause major harm when planned with other malicious activities.

Cargo system and movement of cargo is another part that causes substantial distractions at a port during freight movement. This has become a proven method for trafficking goods into a port. This is enabled by presenting malicious code which targets the movement of cargo and cargo management system on-board the ships network.

Once the malware is planted in the freight management system, the malicious code allows remote management of the cargo manifest. Cocaine was trafficked through a port embedding the malware.

Ransomware is additional tool for unsettling the shipping industry, a technique to introduce a virus into a shipboard network using phishing/spear phishing emails with attachments, facilitating downloading from the internet, or through a storage device. Any computer connected to the network is locked out unless a ransom is paid. There are growing reports of logistics organizations being affected. Some organizations pay via multiple payment mechanisms to maintain their functioning and decrease disruptions.

Vendors for warranty purposes control cargo and propulsion systems through remote monitoring which presents another dimension of vulnerabilities. The unintentional introduction of malware vis-à-vis targeted malicious attacks is serious-and much more likely to occur. Various stakeholders have access to critical systems, which increases the opportunity for introduction of malware in maritime trade.

Obsolescence in technology Old and obsolete operating systems are seldom updated, one of the leading causes for significant exposures in monitoring and detection systems. Safety, communications, freight control, ballast water management, engineering, environmental control, and other systems are equally vulnerable to such cyber-attacks.

Third-party access Third parties visiting the ships require a connection to one or more computers on board resulting in linking the ship to shore. Operators, engineers, mechanics, port officials, agents, vendors, board the ship and plug in storage devices, laptops and tablets. Some require the use of removable media to update computers, copy data and/or perform other tasks.

Customs officials and port officials board ships and demand using a computer to "print official documents" through removable media. Lack of control to access onboard systems result in disruptions to operate the ship, e.g. during dry-docking and layups.

In such cases, it is challenging to recognize if malicious code has been embedded in the onboard systems. It is suggested that sensitive data is removed from the ship and reinstalled on returning to the ship. Where possible, systems should be scanned for malware prior to use. OT systems should be tested to check that they are functioning correctly.

Some IT and OT systems are remotely accessible and may operate with an uninterrupted internet connection for remote monitoring, data collection, and ongoing maintenance functions, protection and security. These systems can be "third party systems", whereby the vendor remotely monitors and manages the systems. These systems could include two-way data flow and upload-only.

The following systems and work stations work with remote access are:

- Bridge and engine room systems and work stations on the ship's administrative network
- Cargo such as containers with temperature control systems or specialized consignment that are tracked remotely
- Stability decision support systems
- Hull stress monitoring systems
- Navigational systems including Electronic Navigation Chart (ENC) Voyage Data Recorder (VDR), dynamic positioning (DP)
- Freight handling and stowage, engine, and freight management and load planning systems
- Safety and security networks, such as CCTV (closed circuit television)
- Specialized systems such as drilling operations, blow out preventers, subsea installation systems
- Emergency Shutdown (ESD) for gas tankers, submarine cable installation and repair.

II. CYBER RISK

Risk is the uncertainty on achieving organization's objectives.

Cyber risk means any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems.

The following are some of the maritime cyber risks which can materialize and their potential impact for businesses and the ships they operate. The same is illustrated in Table 1.

TABLE 1: Cyberspace Risks Associated With Maritime Industry.

Group	**Objective / Risk**	**Motivation**	**Impact**
Communication	Deleting data	Disruption	Destruction of Data
	AIS Spoofing	Modification Penetration	Penetration of AIS
	Controlled navigation	Signal Modification	Entire vessel
	GPS jamming	Disruption	Onboard communication disrupted
	Penetrating satellite communications	Exploitation of vulnerabilities	Remote attacks
APT	Pre-install malware	Business disruption	Destruction of data
	Interruption of services	Malicious intention	Business operations
Access Controls	Alternative Services	Ghost Shipping	Drugs smuggled
	Bypassing customs	Penetrating systems	Access to containers
	Fraudulent actions	Perform different roles	Inappropriate access rights
	Penetration Code Exploits	Modification - Code	Unauthorized access
Activists	Geopolitical Damage to intangible assets Inefficiency in	Cause harm to operations	Loss of business Media attention

	operations		
Dos/DDoS Phishing Spear Phishing Backdoor	Install malware Reputational damage Extract information	Malicious intent	Denial of services Selling stolen data Disruption in supply chain
Espionage	Commercial Industrial	Financial gain	Selling stolen data Reconnaissance for further attacks
Cyber insurance	Coverage of cyber insurance is excluded	To cover malicious act of cyber attacks	Payouts are excluded for cyber attacks
Network	Breach enterprise network and subsequently ships	Penetration of information systems	Disruption of business
Obsolescence	Legacy systems are not updated	Lack of review on information systems	Vulnerabilities exploited
People	Posting information in public forums	Financial gain	Shipping routes available in public domain
	Social engineering	Penetrating maritime authorities	Denial of critical services
	Employees charging personal devices onboard the ship	Inadvertent downloads of malicious content	Denial of services
Privacy	Data transfer across borders	Transfer of personal information	Inappropriate data privacy regulations

Based on the risks mentioned above, the following are the cyber-attacks in the maritime business which are classified as targeted and untargeted attacks. The same is shown in figure 2.

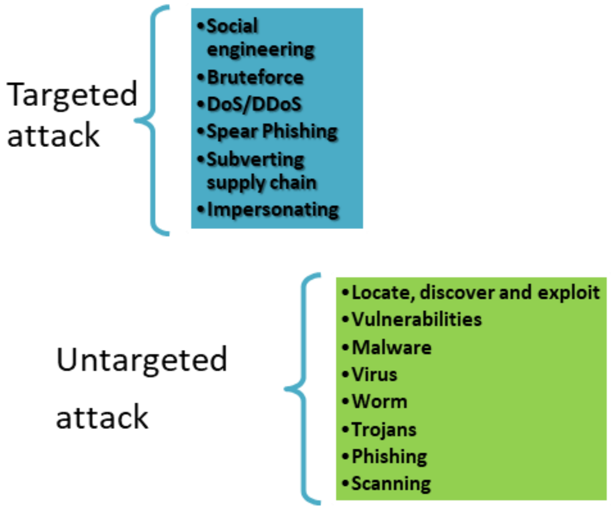

Figure 2: Cyber-attacks in the maritime trade

Cyber Preparedness

While it is not possible to mitigate all the cyber incidents, prevention mechanisms is very important to reduce the overall risks to the public and maritime industry. Cyber risk assessment should be focused at board level of an organization, rather than operations or IT department.

Primary drivers for cyber preparedness

- Regulatory compliance
- High frequency and cost related to cyber security incidents
- Concerns over reputational damage
- Loss of information

Cyber preparedness starts with designing and developing a cyber-security program with the following elements.

- Defined desired outcomes and objectives for cyber security.
- Determine current state
- Gap Analysis
- Develop strategy and create roadmap
- Develop program to implement cyber security
- Manage Program

Cyber security strategy aligned with organizations objectives

- Designed with cooperation from management and other stakeholders
- Effective metrics developed for cyber security strategy and execution
- Optimally address
  - Strategic alignment
  - Risk Management
  - Resource management
  - Value Delivery
  - Assurance process
  - Performance measurement
  - Integration
- Business processes, training, safety of the ship and the environment need to be focused more.
- Awareness on how the organization interacts with customers, suppliers, authorities and co-operation between the parties need to be coordinated.
- Allocate the budget to execute a full risk assessment and develop or acquire solutions to be implemented in the organization.
- Identify systems that are important to operation, safety and environmental protection.
- Assign the persons responsible for setting cyber policies, procedures and enforce monitoring.
- Determine where secure remote access should use multiple defense layers and where protection of networks should be disconnected from the internet.
- Identification of needs for training of personnel.

There are threat agents which exposes the vulnerability to cyber incidents in maritime industry as well.

- The cyber controls implemented by the enterprise onboard its ships.
- Stakeholder management is one of the key factors in the operation and chartering of a ship providing accountability for the IT infrastructure.
- Critical business and sensitive information shared with shore-based service providers, including terminal information and where applicable, to the public authorities to be controlled.
- The availability and use of computer-controlled critical systems for the ship's safety and for environmental protection.

These factors should be considered and relevant controls incorporated into the company cyber security policies, physical and safety management systems, and ship security plans.

Users of these guidelines need to refer to specific national, international and flag state conventions, principles, regulations, procedures in addition to pertinent international and industry standards and best practices when designing, developing and implementing cyber risk management processes associated to maritime trade.

IT and OT systems, enterprises need to consider auditing the third party service providers and vendors on software, hardware and maintenance services they provide. Some companies use different providers responsible for software and cyber security checks. The growing use of big data, smart ships and the "internet of things" will result in information available to cyber attackers and the potential attack surface to cyber criminals. This makes the need for robust approaches to cyber risk management important both now and in the future.

III. Approach to Cyber Risk Management

Risk management addresses cyber-related risks by extending security controls to technologies in maritime trade. Risk management in maritime trade, much like any other operational or financial risk, involves identifying risks, analyzing risks quantitatively or qualitatively, evaluating risks, and finally treating risks responding to incidents, and recovering from an incident by implementing continuous improvement mechanisms.

The shipping company should decide the implementation of a cyber-risk management program and include guidance for various personnel of the organization, from the CEO down to the deck plates. Many establishments have pursued to define how cyber risk management should be implemented on ships, and agreed to follow the Cyber security Framework developed by the National Institute of Standards and Technology (NIST).

The NIST framework was developed in 2014. The framework was designed to be an umbrella framework so that it could cater to any sector, ranging from financial or medical to transportation or security. It defines five functional elements that form the backbone of a thorough cyber risk management program. Additional guidelines and best practices were derived within the maritime industry from this framework.

The Inter-national Maritime Organization (IMO)'s Maritime Safety Committee (MSC) developed guidelines providing high-level recommendations to safeguard maritime trade from current and evolving cyber-related threats and vulnerabilities. The IMO guidelines on Maritime Cyber Risk Management were finalized in July 2017 as MSC-FAL.1/Circ.3.

These guidelines were an important landmark in the management of cyber risks in the maritime industry. They implement the five functional elements detailed in the NIST framework, with the goal of embedding these elements into all aspects of operations of the company and personnel management in the same way industry has embraced safety culture by adopting and safeguarding through safety management systems.

In June 2017, the IMO's Maritime Safety Committee published resolution 428(98) Cyber Risk Management in Safety Management Systems. The focus was to empower organizations and further develop best practices and additional implementation recommendations and incorporating cyber risk management into existing safety management systems as provided by the foundational guidelines.

A target of the first annual review of the company's Document of Compliance after January 1, 2021 was affirmed by this resolution to be addressed by safety management system which became the first mandatory deadline in the maritime industry for establishment of cyber-related risks, and it is a critical step in protecting the maritime transportation system and the industry as a whole from the ever-growing array of cyber threats.

One industry publication highlighting foundational elements is “The Guidelines on Cyber Safety and Security On-board Ships”. A proactive approach to embed cyber risk management into the existing safety culture before a significant incident occurs.

The table 2 illustrates various global maritime cyber security regulations.

Cyber Security Regulations

The table 2 illustrates various global maritime cyber security regulations.

TABLE 2: Various global maritime Cyber Security Regulation

USA	• Development of maritime regulations since Sept 2016 • Require incident reporting since Jan 2017 • Draft navigation and vessel inspection circular NVIC 05-17 (hearing)
France	• Recommendations on maritime cyber security from Sept 2016
Norway	• Norwegian Maritime Authorities’ report “Digital vulnerabilities in the maritime sector” by DNV GL from April 2015
Netherland	• Dutch Data Processing and Cyber security Notification

	Obligation Act, since Jan 2017
Japan	• Development of Japanese guideline for cyber security applicable to maritime assets supported by DNV GL since 2016
Germany	• IT-Sicherheitsgesetz from June 2015 –includes ports but not ships
India	• Guidelines on maritime Cyber Safety, 2017

There is a market demand for more consideration of cyber risks since 2017. Those include

- Tanker Management and self -assessment (TMSA) no.3 was published in April 2017 by including two elements especially for cyber security. These include:
    - Element 7, which talks about Change management
    - Element 13, which talks about Maritime Security
- KPIs and third party audits
    - Software management procedures covers all shipboard and shore systems
    - Actively promoting cyber security awareness
    - Policy and procedures include cyber security
    - Charters demand TSMA audits of ships and TMSA 3 to be met from 1st Jan. 2018 onwards

Owing to the impact of cyber risks – it should be addressed in safety management of systems according to the International Maritime Organization, the Maritime Safety committee agreed that there is an urgent need to raise the awareness on cyber risks and threats and vulnerabilities. Integration cyber risks as a part of safety management systems (ISPS and ISM Codes). MSC 98 adopted resolution MSC.428 (98) on Maritime Cyber Risk Management in Management systems are one of the major suggestions given by them. Though the guidelines are not mandatory, the member governments are encouraged to apply them.

Cyber threat assessment in maritime industry should have a holistic approach inclusive of people, process and technology and operations as illustrated in figure 3.

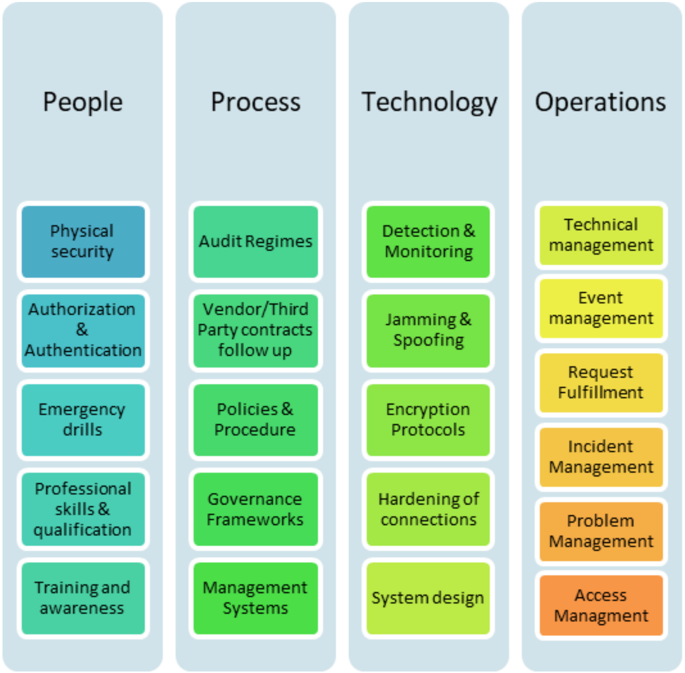

Figure 3: Holistic approach to cyber security

Conclusion

Addressing the risks and vulnerabilities through a cyber-security program helps the maritime industry to be prepared in the cyber world in the current global environment. Obtaining the definitive information about the cyber-attacks in the business sectors helps maritime industry and the other organizations to be proactively prepared in the cyber arena. Cyber risk management through the risk identification, risk assessment, risk evaluation and risk treatment will drive the automation, digitization and integration in the maritime trade.

IV. References

1. The guidelines on Cyber security onboard ships (2018), Bimco, CLIA, ICS, Intercargo,

Intermanager, Intertanko, IUMI, OCIMFand World Shipping Council.
2. Advanced Persistent Threat Awareness (2014), ISACA, Available online: www.isaca.org/cyber
3. Cyber Security resilience Management for ships and mobile offshore units in operation (2016). Available online: http://www.dnvgl.com
4. Guidelines on Maritime Cyber Safety (2017) IRCLASS, Indian Register of Shipping
5. International Union of Marine Insurance (IUMI).(2017). Ship Operation Safety & Security
6. ISM Code Examples of Cyber Security audit findings: Simple steps to get started (2017). Available online: www.dnvgl.com/rpcs.
7. ISTQB Standard glossary of terms used in Software Testing
8. W., Lin, Tom C. (14 April 2016). "Financial Weapons of War"
9. https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/