CYBER SECURITY IN SHIPPING

Cdt, Guruprasath M[a], Cdt.Kathiresan M[b] and Cdt.KishoreKumar J[c]
[a]GEIMS, Lonavala, guru98.gme@gmail.com,
[b]GEIMS , Lonavala, kathir0471@gmail.com ,
[c]GEIMS, Lonavala, kishoremarine17@gmail.com,.

Abstract: In recent days, navigation of ship is achieved by receiving the signal from satellite. Satellite act as intermediate between transmitter and receiver. From shore-station the signal is transmitted to ship through satellite. Hacking is the problem occurring during navigation of ship. Suppose if an operator unknowingly connects his hacked device to any system of the ship, the data in the ship can be hacked through the device. Once the data has been hacked, it will be easy for the hijackers to control the navigation system of the ship. In order to avoid this a coding should be done in such a way that it should auto generate random password for every minute. Thus, by this way we can avoid the hijacking of ship navigation.

Keywords: Signal, hacked device, satellite, hijackers, navigation system.

1. Introduction

Ships are increasingly using systems that rely on digitisation, digitalisation, integration, and automation, which call for cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) on-board ships are being networked together – and more frequently connected to the internet. This brings the greater risk of unauthorised access or malicious attacks to ships' systems and networks. Risks may also occur from personnel accessing systems on board, for example by introducing malware via removable media. In 2017, the International Maritime Organization (IMO) adopted resolution MSC428(98) on Maritime Cyber Risk Management in Safety Management System (SMS).

The Resolution stated that, an approved SMS should consider cyber risk management in accordance with the objectives and functional requirements of the ISM Code. As a result of this assessment, a profile is developed, which can help to identify and prioritise actions for reducing cyber risks. This profile is used as a tool for aligning policy, business and technological approaches to manage the risks. These profiles were created by the United States Coast Guard and NIST's National Cybersecurity Centre of Excellence with input from industry stakeholders. Both cyber security and cyber safety are important because of their potential effect on personnel, the ship, environment, company and cargo. The aim of this document is to offer guidance to ship-owners and operators on procedures and actions to maintain the security of cyber systems in the company and on-board the ships.

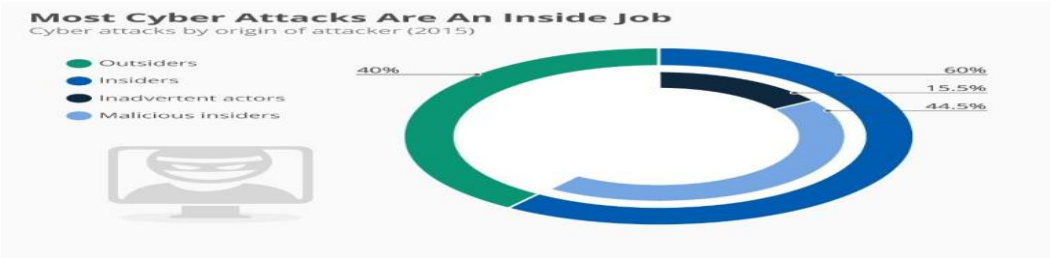

FIGURE 1. Statistics Of Cyber Attacks

2. Main work

In a shipping context a cyber risk may be an failure of an onboard GPS receiver due to a fault with the equipment, extending right through to catastrophe scenarios of vessel systems being attacked and the vessel being disabled, run aground or taken by the malicious third parties. Although the catastrophe scenarios are possible the likelihood of such an incident for most companies is low.

The risk of electronic equipment failure are generally well recognised in the industry and critical equipment will often be required to have redundancy, spares will be carried or manual operation will be possible should the electronics failed.

What has been less well recognised until recently is the risk of electronic systems being subjected to unauthorized access or malicious attacks – lets call them "**Cyber Threats**". Recently there has been a focus on this area and the steps that might be taken to defend shipping companies from unauthorized access or malicious attacks. The defences taken to defend systems are known as "**Cyber Security"**.

A secure network depends on the IT/OT set up on-board the ship, and the effectiveness of the company policy based on the outcome of the risk assessment. Control of entry points and physical network control on an existing ship may be limited because cyber risk management had not been considered during the ship's construction. It is recommended that network layout and network control should be planned for all new buildings.

2.1 Cyber Risk

Cyber risk means any risk of accidents, incidents, financial loss, business disruption or damage to the reputation of an organization through failure of its electronics systems or by the persons using those systems.
Advances in technology means that ships systems are not only being networked together but are also connected to the world wide web. This means that ships are now more vulnerable to cyber threats than previously.
It can affect a company's bottom line, damage its reputation or disrupt its business. At the more extreme end of things there is the possibility that malicious groups or individuals may seek to cause shipping accidents although the risks of this are currently thought to be low for most companies.

2.1.1 Types of Cyber Attack

2.1.1.1 Untargeted attacks:

Where a company or a ship's systems and data are one of many potential targets. These are likely to use tools and techniques available on internet, which can be used to locate, discover and exploit widespread vulnerabilities that may also exist in a company an onboard ship.

- Malware
- Phishing
- Water holing
- Scanning

2.1.1.2 Targeted attacks:

Where a company or a ship's systems and data are the intended target. These may be more sophisticated and use tools and techniques specifically created for targeting a company or ship.

- Brute force
- Social engineering
- Denial of service

- Spear-phishing
- Subverting the supply chain

2.1.2 Stages of Cyber Attack

The length of time to prepare a cyber attack can be determined by the motivations and objectives of the attacker, and the resilience of technical and procedural cyber risk controls implemented by the company, including those onboard its ships.

When considering targeted cyber attacks, the general observed stages of an attack are:

- Survey
- Delivery
- Breach
- Pivot

2.2 Consequences of Cyber Attack

2.2.1 Cargo management systems

Shipment-tracking tools available to shippers via the internet. Tracking is not directly between the shipper and the ship.

Interfaces of this kind make cargo management systems and data in cargo manifests and loading lists vulnerable to cyber attacks.

2.2.2 Bridge systems

The increasing use of digital, network navigation systems, with interfaces to shoreside networks for update and provision of services, make such systems vulnerable to cyber attacks.

A cyber incident can affect all systems associated with navigation, including ECDIS, GNSS, AIS, VDR and Radar.

2.2.3 Propulsion and machinery management systems

The use of digital systems to monitor and control onboard machinery, propulsion and steering makes such systems vulnerable to cyber attacks.

The vulnerability of these systems can increase when used in conjunction with remote condition-based monitoring.

2.3 Cyber Security

Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

It is achieved through the following ways:

- identify the roles and responsibilities of users, key personnel, and management both ashore and on board
- identify the systems, assets, data and capabilities, which if disrupted, could pose risks to the ship's operations and safety
- implement technical and procedural measures to protect against a cyber incident and ensure continuity of operations
- implement activities to prepare for and respond to cyber incidents.

2.3.1 Communication systems

Availability of internet connectivity via satellite and/or other wireless communication can increase the vulnerability of ships. The cyber defence mechanisms implemented by the service provider should be carefully considered but should not be solely relied upon to secure every shipboard system and data. Included in these systems are communication links to public authorities for transmission of required ship reporting information. Applicable authentication and access control management requirements by these authorities should be strictly complied with.

2.4 Identification of Threats

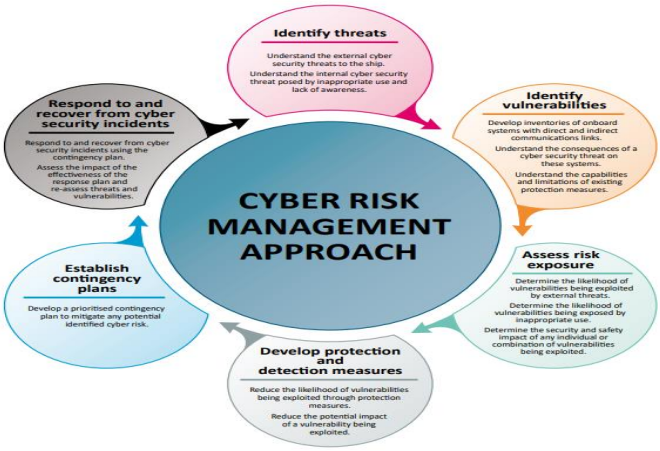

FIGURE 2. Cyber Risk Management Approach

TABLE 1. Motivation and objectives

GROUP	MOTIVATION	OBJECTIVE
Activists	• Reputational damage • Disruption of operations	➢ Destruction of data ➢ Publication of sensitive data ➢ Media Attention
Criminals	• Financial gain • Commercial espionage • Industrial espionage	➢ Selling stolen data ➢ Ransoming stolen data & system operability ➢ Arranging fraud transport of cargo
Opportunists	• The Challenge	➢ Getting through cyber security defences ➢ Financial gain
State Sponsored Organisation	• Political gain espionage	➢ Gaining knowledge ➢ Disruption to economies and national infrastructure

2.5 Cyber Security Protection Measures

2.5.1 Technical protective measures:

- Limitation to and control of network ports, protocols and services
- Configuration of network devices such as firewalls, routers and switches
- Physical security
- Detection, blocking and alerts
- Satellite and radio communication
- Wireless access control
- Malware detection
- Secure configuration for hardware and software
- Email and web browser protection
- Data recovery capability
- Application software security (patch management)

2.5.2 Procedural protective measures:

- Training and awareness
- Controlled access for visitors
- Upgrades and software maintenance
- Anti-virus and anti-malware tool updates
- Remote access
- Use of administrator privileges
- Physical and removable media controls
- Equipment disposal, including data destruction
- Obtaining support from ashore and contingency plans

2.6 Recovery Plan

- Recovery plans should be available in hard copy on board and ashore. The purpose of the plan is to support the recovery of systems and data necessary to restore IT and OT to an operational state.
- To help ensure the safety of onboard personnel, the operation and navigation of the ship should be prioritized in the plan. The recovery plan should be understood by personnel responsible for cybersecurity.
- The incident response team should consider carefully the implications of recovery actions (such as wiping of drives), which may result in the destruction of evidence that could provide valuable information as to the causes of an incident.
- Recovery of OT may be more complex especially if there are no backup systems available and may require assistance from ashore. Details of where this assistance is available and by whom, should be part of the recovery plan, for example by proceeding to a port to obtain assistance from a service engineer.

2.7 Secured Work Environment

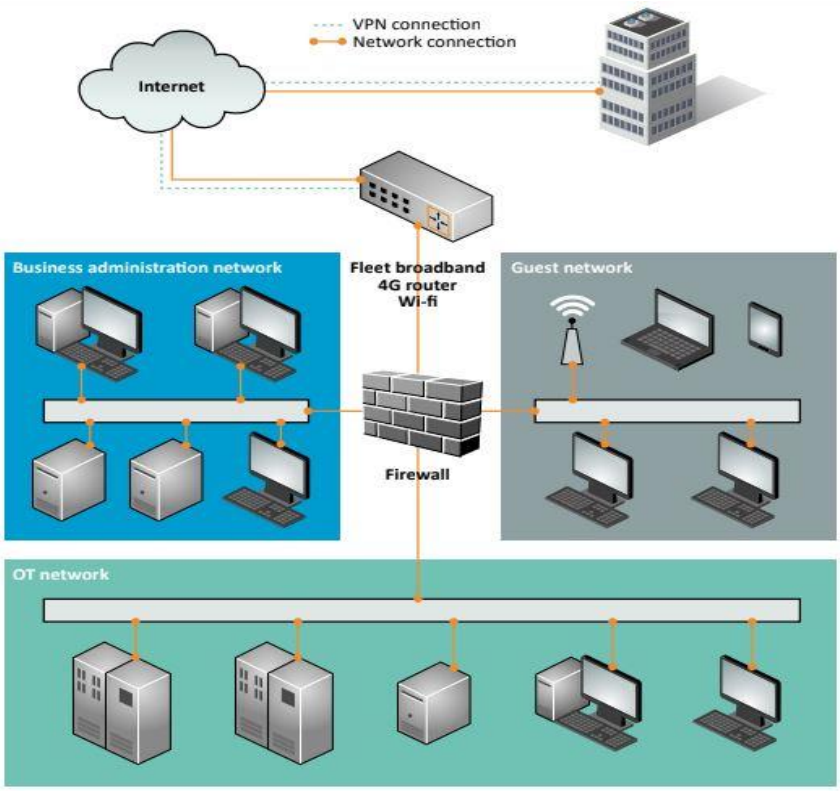

FIGURE 3. Example Of An Onboard Network

2.7.1 Clear Screen Policy

- Lock your computer (Ctrl-Alt-Del)
- You are responsible for any activity performed using your logon id.
- Do not share your username and password with anyone.
- Always shutdown or log off when your work is over or during extended break's.

2.7.2 Clean Desk Policy

- At the end of the working day & during extended break (lunch) tidy your desk & lock your sensitive files in drawers /cabinets
- Clear sensitive or classified information from the printer immediately.
- A messy desk is a vulnerable desk.

2.8 We can make the difference

2.8.1 Don'ts

- Share password with anyone
- Share credentials or vital information with unknown
- Read unsolicited mails
- Forward junk and chain mails
- Use official Email IDs for personal communication
- Install pirated or unauthorized software
- Discuss important or sensitive topics in public
- Save passwords or credentials while on public internet.

- Use data upload sites, webmail for sharing sensitive information
- Use your colleagues credentials to access any resource
- Try to stop/ disable the Anti-virus real-time or scheduled scan process

2.8.2 Do's

- Lock your machine while leaving it unattended
- Use strong passwords and change them regularly
- Clean your desk while leaving for the day
- Use Internet judiciously
- Use printing judiciously
- Use Mobile devices judiciously
- Be attentive while on social networking sites or platforms
- Destroy documents no longer in use
- Co-operate with the IT engineer while machine is scanned with antivirus
- Co-operate while security patches are being installed / applied
- Regularly backup your important data and files.
- For backup of Video files, contact IT Department
- Report and respond to security incidents and breaches.
- Practice these policies and encourage others to do so as well

3. Conclusions

Some aspects of cyber risk management may include commercially sensitive or confidential information. Companies should, therefore, consider protecting this information appropriately, and as far as possible, not include sensitive information in their Safety Management System (SMS). Whilst the causes of a cyber safety incident may be different from a cyber security incident, the effective response to both is based upon training and awareness. In section 2.4, this paper described essential cyber security measures that should be undertaken on a ship. It explored how a ships facility interconnects, and, as an example of a cyber threat, how hackers fabricate GPS signals.
It is, therefore, important that senior management stays engaged throughout the process to ensure that the protection, contingency and response planning are balanced in relation to the threats, vulnerabilities, risk exposure and consequences of a potential cyber incident. Company plans and procedures for cyber risk management should be incorporated into existing security and safety risk management requirements contained in the ISM Code and ISPS Code.

Acknowledgments

Thanks to our Principal, Capt. A.P.Sethi, Vice Principal Capt. Philip John, course in charge, Mr. Mukund Joglekar, IT instructors and all Engineering Faculty, who have all carved out their valuable time , in compilation of this paper.

Thanks to Mrs. Meena Ravi Shankar, soft skills trainer, for the persistent assistance given while preparing our paper.

Lastly, we extend our thanks to "**TRANSTECH 2020",** to have given us this opportunity in presenting our chosen technical paper clearly

References

Maritime Cyber Security and Big Data, https://cbs- executive.dk/en/programme/maritime-cyber-security-and-big-data/, Accessed August 9, 2017.
Maritime Industry is Easy Meat for Cyber Criminals, https://www.kaspersky.com/blog/maritime-cyber-security/8796/, Accessed May 17, 2017.
International Maritime Organization (IMO), MSC- FAL.1/Circ.3, "GUIDELINES ON MARITIME CYBER RISK MANAGEMENT," 2017.
International Maritime Organization (IMO), MSC.1/Circ.1526, "INTERIM GUIDELINES ON MARITIME CYBER RISK MANAGEMENT," 2016.
International Maritime Organization (IMO), MSC.428(98), "MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS," 2017.