CONTENTS

IT CYBER SECURITY

1. INTRODUCTION

Ships are increasingly using systems that rely on digitisation, integration, and automation, which calls for cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) onboard 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. The Company has instituted several procedures to mitigate this risk. Cyber security now forms part of the Safety Management System; accordingly, an IT Policy statement is now provided.

1.1. Responsibility[1]

Master is responsible for managing the cyber security on board the vessel.

CEO and CNO are responsible to Master for ensuring that crew is made aware of the cyber risks and complies with these procedures.

Every employee is responsible for alerting the Master of any possible or potential cyber risks noted while they using the company IT infrastructure. Any cyber security event and non-compliance should immediately be reported to Master. The cyber security responsibility of the specific IT and OT system is specified in Appendix B – IT and OT systems.

IT department is responsible for managing the cyber security in office and assisting Master on board the vessel on cyber security matters.

2. CYBER SECURITY AND SAFETY MANAGEMENT

2.1. Types of Cyber Attack

In general, there are two categories of cyber-attacks, which may affect companies and ships:

- untargeted attacks, where a company or a ship's systems and data are one of many potential targets
- targeted attacks, where a company or a ship's systems and data are the intended target.

Untargeted attacks are likely to use tools and techniques available on the internet which can be used to locate, discover, and exploit widespread vulnerabilities which may also exist in a company and onboard a ship.

[1] W 50 / 2020

Examples include:

2.1.1. Malware

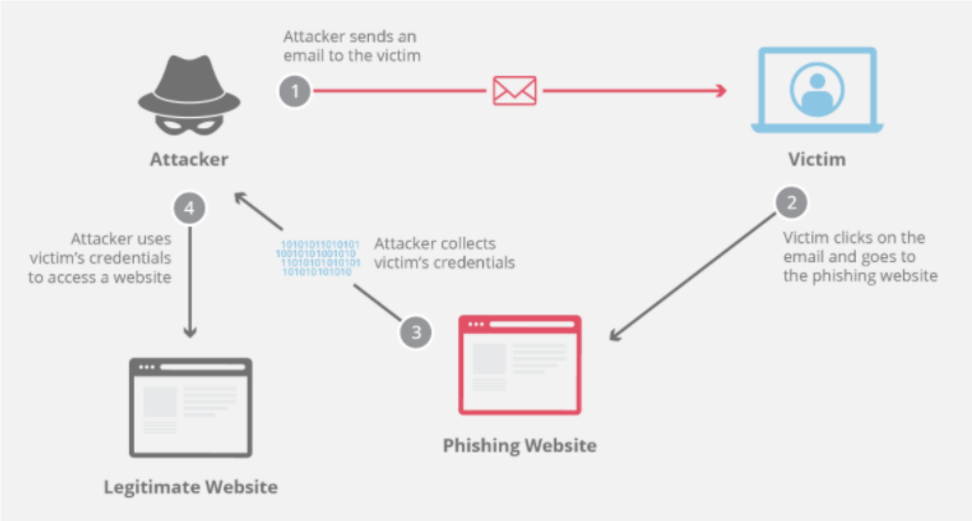
Malicious software which is designed to access or damage a computer without the knowledge of the owner. There are various types of malware including trojans, ransomware, spyware, viruses, and worms. Removable media, unauthorized access and clicking on the unknown link may introduce the malware in the computer.[2]

2.1.2. Social Engineering

A non-technical technique used by potential cyber attackers to manipulate insider individuals into breaking security procedures. Malicious activity is accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.[3]

2.1.3. Phishing

Sending emails to many potential targets asking for pieces of sensitive or confidential information. Such an email may also request that a person visits a fake website using a hyperlink included in the email.[4]


Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
3
Phishing Website
Legitimate Website

i. Attacker sends an email

ii. Victim clicks on the email and goes to the phishing website

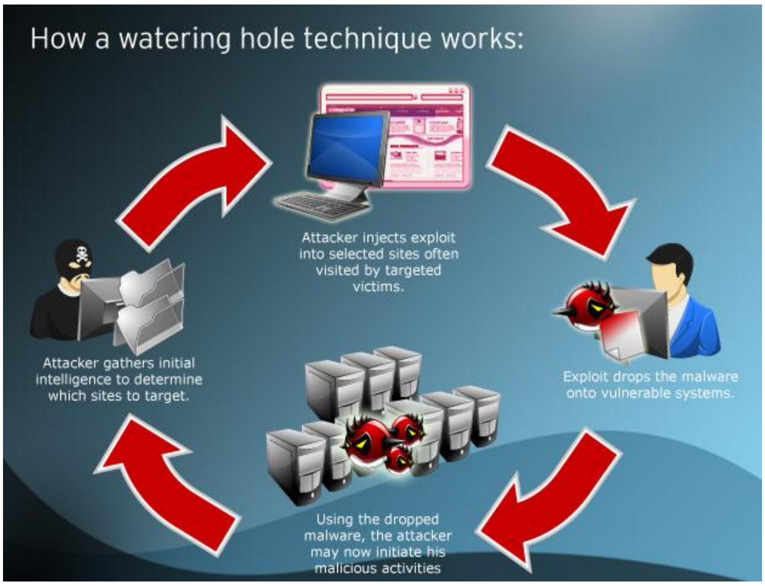
iii. Attacker collects victim's credentials

iv. Attacker uses victim's credentials to access a website

[2] W 50 / 2020
[3] W 50 / 2020
[4] W 50 / 2020

2.1.4. Water Holing

Establishing a fake website or compromising a genuine website to exploit visitors.


How a watering hole technique works:
Attacker injects exploit into selected sites often visited by targeted victims.
Attacker gathers initial intelligence to determine which sites to target.
Exploit drops the malware onto vulnerable systems.
Using the dropped malware, the attacker may now initiate his malicious activities

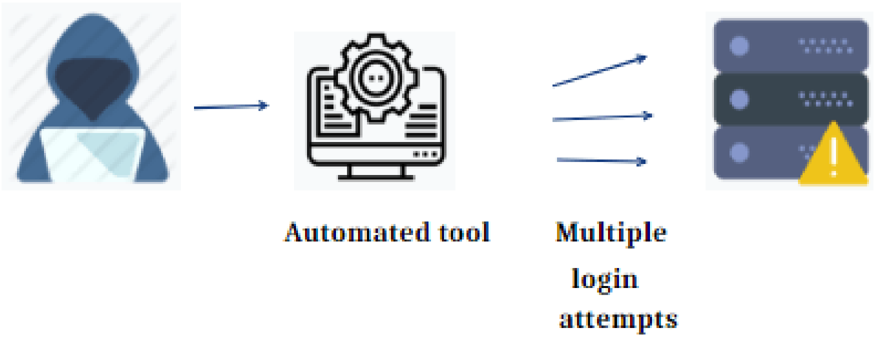
2.1.5. Scanning

Attacking large portions of the internet at random.

Targeted attacks may be more sophisticated and use tools and techniques specifically created for targeting a company or ship.

2.1.6. Brute Force

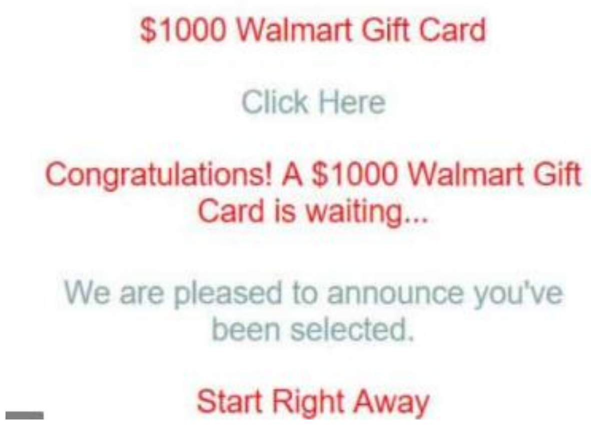
An attack trying many passwords with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords until the correct one is found. It is equivalent of trying every key on your key ring, and eventually finding the right one.[5]



[5] W 50 / 2020

2.1.7. Spear-Phishing

Like phishing but the individuals are targeted with personal emails, often containing malicious software or links that automatically download malicious software.



$1000 Walmart Gift Card

Click Here

Congratulations! A $1000 Walmart Gift Card is waiting...

We are pleased to announce you've been selected.

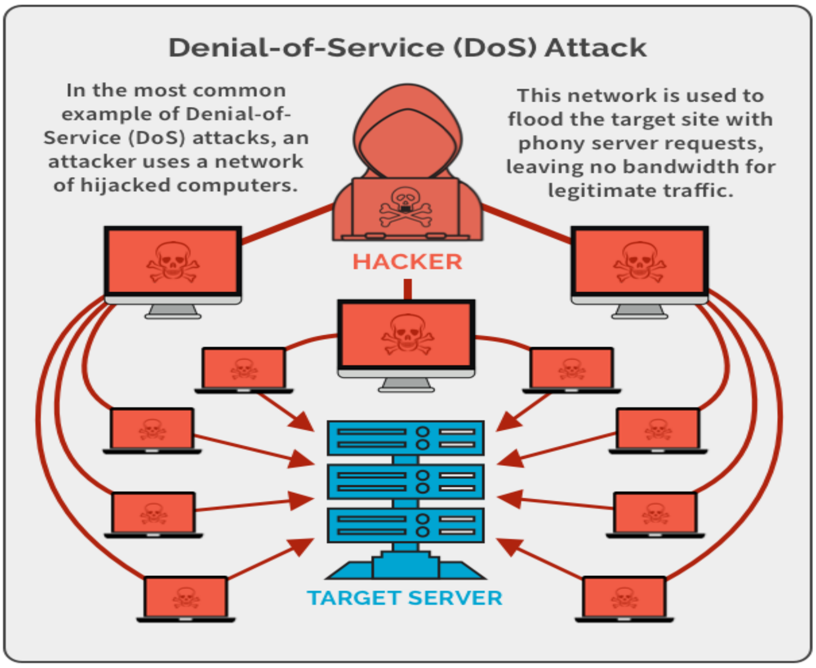
Start Right Away

2.1.8. Subverting the Supply Chain

Attacking a company or ship by compromising equipment, software or supporting services being delivered to the company or ship.

2.1.9. Denial of Service (DoS)

Prevents legitimate and authorised users from accessing information, usually by flooding a network with data. A distributed denial of service (DDoS) attack takes control of multiple computers and/or servers to implement a DoS attack.[6]


Denial-of-Service (DoS) Attack
In the most common example of Denial-of-Service (DoS) attacks, an attacker uses a network of hijacked computers.
This network is used to flood the target site with phony server requests, leaving no bandwidth for legitimate traffic.
HACKER
TARGET SERVER

[6] W 50 / 2020

The above examples are not exhaustive. Other methods are evolving such as impersonating a legitimate shore-based employee in a shipping company to obtain valuable information, which can be used for a further attack.

2.2. Signs of Computer Virus[7]

Protect your computer from dangerous malware with following symptoms and signs that show your computer has a virus. Viruses are malicious software – known as malware – that can destroy files, steal personal information, and damage your computer. Here are the top ten signs your PC has a virus.

2.2.1. Unexpected Pop-Up Windows

Unexpected onscreen ads are a typical sign of a virus infection. Not only are they annoying, but other malware may also lurk inside poised to wreck further havoc.

Never click on a suspicious pop-up – even if it says ‘a virus was detected’. This is an example of rogue ware, which asks you to pay for a program to remove a fake virus but may in fact allow even more malware to be downloaded.

2.2.2. Slow Start Up and Slow Performance

If your PC is taking longer than normal to start or programs are taking ages to open, then your PC may have a virus. If your computer’s performance is sluggish, check first that it is not due to a lack of RAM memory or hard disk space. If not, the culprit may be a virus.

2.2.3. Suspicious Hard Drive Activity

An excessively active hard disk where it makes continual noise or constantly spins – even though you are not using your computer nor have any programs running – can be a sign your PC is infected with a virus.

2.2.4. Lack of Storage Space

If you suddenly find yourself devoid of storage space on your hard drive, a virus may be doing its utmost to make your computer unusable.

2.2.5. Missing Files

Some malware cause problems by deleting files and programs or moving them around. Some may encrypt your files so you are not able to open them.

[7] W 50 / 2020 (Entire Section)

2.2.6. Crashes and Error Messages

If programs start opening and closing automatically, your system freezes or shuts down for no reason, or you see odd error messages, then you may have a virus infection.

2.2.7. High Network Activity

If your internet connection is very active even when you are not using it, a virus may be busy sending information back and forth across the internet.

2.2.8. Email is Hijacked

If friends start receiving emails or instant messages from your social networks asking them to click on an attachment or link, it is likely that a virus is attempting to spread to other computers via your accounts. If so, change your passwords immediately.

2.2.9. Browser Woes

Your web browser becoming sluggish, your home page changing or being redirected to unusual websites are all warning signs of a computer virus infection.

2.2.10. Security Attacks

Some viruses are designed to disable your computer’s protection. So, if you cannot open or install an anti-virus program or your firewall, your computer may be infected.

3. ANALYSIS OF RISKS AND ASSOCIATED IMPACTS

As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the internet. A comprehensive risk assessment has been completed using CFM[8]. The Risk Assessment includes both IT and OT components, identifying their risks and countermeasures.

Cyber safety is as significant as cyber security. Both have equal potential to affect the safety of onboard personnel, ships, and cargo. Cyber security is concerned with the protection of IT, OT and data from unauthorised access, manipulation and disruption. Cyber safety covers the risks from the loss of availability or integrity of safety critical data and OT.

Cyber safety incidents can arise as the result of:

- A cyber security incident, which affects the availability and integrity of OT, for example corruption of chart data held in an Electronic Chart Display and Information System (ECDIS)

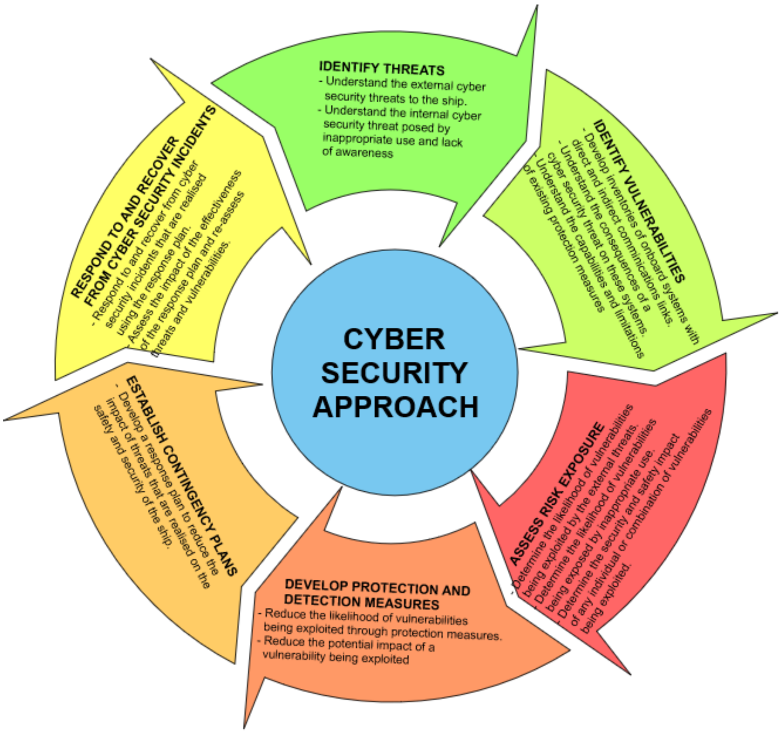
[8] W 30 / 2024

- A failure occurring during software maintenance and patching
- Loss of or manipulation of external sensor data, critical for the operation of a ship. This includes but is not limited to Global Navigation Satellite Systems (GNSS).

Whilst the causes of a cyber safety incident may be different from a cyber security incident, an effective response to both is based upon training and awareness of appropriate company policies and procedures.

The Company has performed a comprehensive Risk Assessment of the IT and OT systems currently onboard the Fleet. Appropriate action to mitigate risks has been undertaken. The Risk Assessment result and associated mitigating measures can be found in Appendix B.

The following methodology was employed:


CYBER SECURITY APPROACH
IDENTIFY THREATS
- Understand the external cyber security threats to the ship.
- Understand the internal cyber security threat posed by inappropriate use and lack of awareness
IDENTIFY VULNERABILITIES
- Develop inventories of onboard systems with direct and indirect comminications links.
- Understand the consequences of a cyber security threat on these systems.
- Understand the capabilities and limitations of existing protection measures
ASSESS RISK EXPOSURE
- Determine the likelihood of vulnerabilities being exploited by the external threats.
- Determine the likelihood of vulnerabilities being exposed by inappropriate use.
- Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.
DEVELOP PROTECTION AND DETECTION MEASURES
- Reduce the likelihood of vulnerabilities being exploited through protection measures.
- Reduce the potential impact of a vulnerability being exploited
ESTABLISH CONTINGENCY PLANS
- Develop a response plan to reduce the impact of threats that are realised on the safety and security of the ship.
RESPOND TO AND RECOVER FROM CYBER SECURITY INCIDENTS
- Respond to and recover from cyber security incidents that are realised using the response plan.
- Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.

3.1. Identify Threats

The cyber risk is specific to the company, ship, operation and/or trade. When assessing the risk, the company is aware of specific aspects of their operations that might increase their vulnerability to cyber incidents. There are motives for organisations and individuals to exploit cyber vulnerabilities. The following examples give some indication of the threat posed and the potential consequences for company and the ship[9]:

[9] W 50 / 2020

[10]Groups posing a threat	Motivation	Objective
Activists (including disgruntled employees)	• Reputational damage • Disruption of operations	• Destruction of data • Publication of sensitive data • Media attention • Denial of access to the service or system targeted
Criminals	• Financial gain • Commercial espionage • Industrial espionage	• Selling stolen data • Ransoming stolen data • Ransoming system operability • Arranging fraudulent transportation of cargo • Gathering intelligence for more • sophisticated crime, exact cargo location, ship transportation and handling plans etc
Opportunists	• The challenge	• Getting through cyber security defences • Financial gain
States, State sponsored organisations, Terrorists	• Political gain • Espionage	• Gaining knowledge • Disruption to economies and critical national infrastructure
Unintentional actions by company personnel	NA	NA

3.2. Identify Vulnerabilities Onboard vessels

The Company has performed an assessment of the systems onboard and the procedures in place to counteract any potential threat. Stand-alone systems will be less vulnerable to external cyber-attacks compared to those attached to uncontrolled networks or directly to the internet. Care should be taken to understand how critical shipboard systems might be connected to uncontrolled networks. Systems onboard the vessels include:

3.2.1. 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. Bridge systems that are not connected to other networks may be equally vulnerable, as removable media are often used to update such systems from other controlled or uncontrolled networks

[10] W 50 / 2020

3.2.2. Cargo Management Systems

Digital systems used for the management and control of cargo, including hazardous cargo

3.2.3. Propulsion and Machinery Management and Power Control Systems

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

3.2.4. Administrative and Crew Welfare Systems

Onboard computer networks used for administration of the ship or the welfare of the crew are particularly vulnerable when they provide internet access and email. Availability of internet connectivity via satellite and/or other wireless communication can increase the vulnerability of ships.

3.2.5. Ship Communication systems

Business related e-mail systems to the Master which are critical for the forthcoming voyage and the safety of the ship.

The vulnerable shipboard IT and OT systems containing the risk involved and control measures are provided in Appendix B.[11]

3.3. Protection and Detection Measures

The outcome of the risk assessment and review of the company's cyber security strategy is a reduction in risk by the identification of vulnerabilities and the formulation of specific countermeasures against those areas of vulnerabilities. At a technical level, this would include the necessary actions to be implemented to establish and maintain an agreed level of cyber security. In general there are two types of protection measures – Technical and Procedural.[12]

3.3.1. Technical Protection Measures[13]

The protection measures comprise of a list of Critical Security Controls (CSC) that are prioritised and vetted to ensure that they provide an effective approach for the company to assess and improve its defences. The technical measures deal with the equipment and systems. Critical Security controls may include:

- Limitation to and control of network ports, protocols, and services
- Configuration of network devices such as firewalls, routers and switches

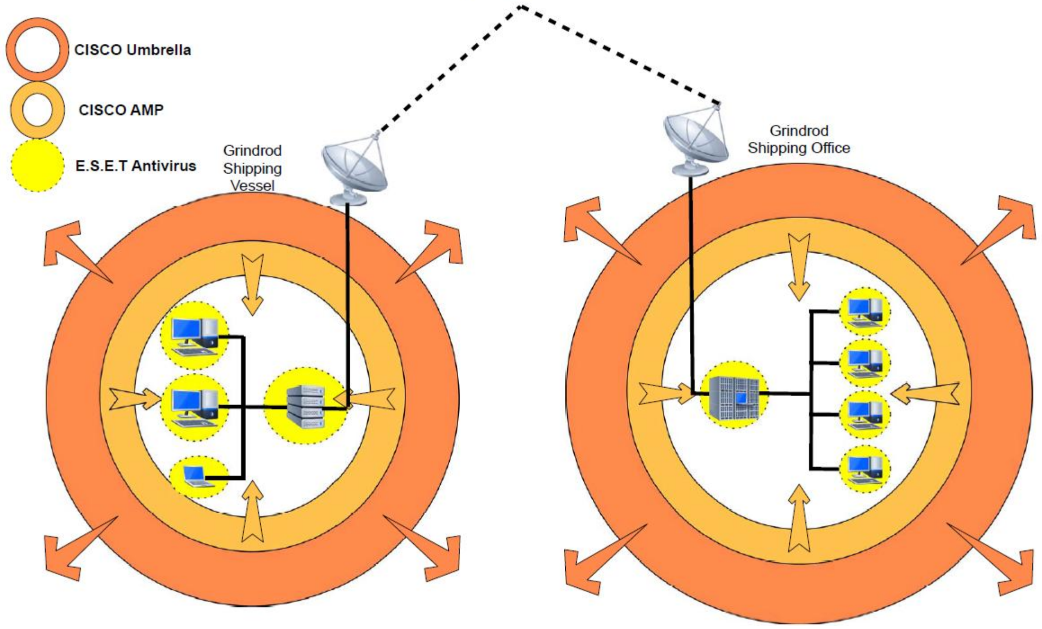
[11] W 50 / 2020
[12] W 50 / 2020
[13] W 50 / 2020

- Security and safety critical equipment and cable runs should be protected from unauthorised access
- Detection, blocking and alerts. Scanning software that can automatically detect and address the presence of malware in systems onboard
- Cyber security of the radio and satellite connection should be considered in collaboration with the service provider
- Email and web browser protection
- Data recovery capability is the ability to restore a system and/or data from a secure copy or image thereby allowing the restoration of a clean system

Protection & Detection Software for the Company Cyber Security Requirements[14]

Company provides the following software to reinforce its cyber security requirements. On a micro level each PC or Laptop is protected using ESET Antivirus software. All end-users (PC's and Laptops) are updated with the latest version of software as the software becomes available. Within the ship or office environment CISCO AMP provides security protection to the system architecture. CISCO Umbrella provides protection regarding the external environment, intercepting a cyber-attack before it embeds into the local system architecture. The following diagram shows a typical network and the different levels of protection provided by the software:[15]

Cyber Security Protection
Grindrod Shipping Business Network



ESET PC/Laptop Antivirus protection:[16]

[14] W 50 / 2020
[15] W 50 / 2020
[16] W 50 / 2020

ESET antivirus is installed on each Laptop or PC and provides the following protection:

Removable Media Control: Allows to prevent unauthorized copying of your private data to external device.

Anti-Phishing: Protects against malicious websites attempting to acquire your sensitive information – usernames, passwords, banking information or credit card details.

Antivirus and Antispyware: Eliminates all types of threats, including viruses, worms and spyware. Whitelisting of safe files based on file reputation database in the cloud.

Web and Email Scanning: Scans websites (HTTP) while you browse and checks all incoming emails (POP3 / IMAP) for viruses and other threats.

Auto-scan of Removable Media: Scans devices and media for malware immediately upon insertion. Scanning options include Scan / No Action / Setup / Remember this action.

Cisco Umbrella and AMP Provides the following protection to the Vessel or Office environment

Prevent	**Detect**	**Respond**
AMP for Endpoints	**AMP for Endpoints**	**AMP for Endpoints**
• Blocks attacks at initial inspection, monitoring files, memory, and behaviour	• Continuously analyses all file activity to detect malicious behaviour and retrospectively alert on new threats	• Shows the full history and context of a compromise
• Uses sandbox (powered by Cisco Threat Grid) to analyse unknown files		• Provides blocking of malware with a single click
Umbrella	**Umbrella**	**Umbrella**
• Blocks malicious Internet requests (domain, URL, and IP) before connections are ever made	• Learns where attacks are staged and detects attackers' infrastructure in order to proactively block threats	• Provides rich threat intelligence on domains, IPs, and file hashes so you can triage faster

Cisco AMP for Endpoints (Endpoints are vessel PC/Laptop or Office PC/Laptop)[17]

AMP for Endpoints is a cloud-managed endpoint security solution that prevents cyber-attacks and rapidly detects, contains, and remediates malicious files on the endpoints.

[17] W 50 / 2020

- Antivirus protection and continuous behavioural monitoring of the local environment
- Dynamic file analysis and vulnerability identification
- Endpoint (vessel PC/Laptop or Office PC/Laptop) isolation
- Advanced Endpoint Detection and Response (EDR)
- Proactive blocking - AMP for Endpoints uses a combination of file reputation, behavioural indicators, sandboxing technology, and global threat intelligence provided by the Cisco Talos® Security Intelligence Group to analyse unknown files and automatically block malware from trying to run on endpoints.
- Continuous analysis and retrospective security - Advanced malware can evade front-line defences and infiltrate an endpoint.

AMP for Endpoints continuously monitors and records all file activity on endpoints to quickly spot malicious behaviour.

Cisco Umbrella[18]

Umbrella unifies firewall, secure web gateway, DNS-layer security, cloud access security broker (CASB), and threat intelligence solutions into a single cloud service to help company secure its network. Umbrella extends its protection to roaming users and the company fleet.

Umbrella uncovers and blocks a broad spectrum of malicious domains, IPs, URLs, and files that are being used in attacks. By enforcing security at the DNS and IP layers, Umbrella blocks requests to malware, ransomware, phishing, and botnets before a connection is even established — before they reach the network or endpoints. The secure web gateway logs and inspects all web traffic for greater transparency, control, and protection. The cloud-delivered firewall helps to log and block traffic using IP, port, and protocol rules for consistent enforcement throughout your environment.

Umbrella categorizes and retains all internet activity to simplify company investigation process and reduce incident response times. Automated response actions simplify security by eliminating manual tasks and stopping attacks earlier in the process.

3.3.2. Procedural Protection Measures[19]

Procedural controls are focused on how personnel use the onboard systems. Plans and procedures that contain sensitive information should be kept confidential and handled according to company policies. Examples for procedural actions can be:

- Training and awareness is the key supporting element to an effective approach to cyber safety and security. Company sends monthly Cyber Security campaigns to educate crew on board. Cyber Security campaigns are available

[18] W 50 / 2020
[19] W 50 / 2020

in the SHEQ/Memo/Cyber Security portal. Master is responsible for the onboard cyber security familiarization of the crew.

- Visitors such as authorities, technicians, agents, port officials, and cargo surveyors should be restricted with regard to computer access whilst on board. Should a USB device be handed over to be printed, the crew member should insert the USB Drive directly into the printer and print.
- The use of hardware and software, which is no longer supported, should be carefully evaluated and updated to maintain a sufficient security level.
- Anti-Virus software updates are supervised by IT department on all relevant computers on board.
- The Company IT Department are the only ones allowed remote access to onboard IT systems.
- User privileges are removed when the people concerned are no longer on board. Specific user accounts should not be passed on from one user to the next using generic usernames.
- Passwords are an important aspect of computer security. They are the front line of protection for user accounts. Password should be strong and changed periodically. Passwords should be a minimum of six (6) characters long. Use a combination of upper case & lower case characters, numbers and special symbols is recommended. Password should never be displayed on or near computers. If the password is written down as a part of handing over notes, it must be kept at secure place and should be changed after taking over the duties by on-signer. Don’t reveal a password over the phone or in email message.
- Only trusted websites “on business need” basis have been allowed on common working computers.
- Transferring data from uncontrolled systems (Removable media) to controlled systems is not allowed as it represents a major risk of introducing malware.
- Firmware upgrades of the OT systems onboard may have the unintended consequence of corrupting the system itself due to incompatibilities between the new software and the older hardware. Should any service provider require access to the OT system, this is to be approved directly by the Ship Manager PRIOR to commencement of the job. The IT Manager or IT representative is to oversee the operation and remote access by the Service Provider. The Ship Manager is to satisfy himself that the Service Provider is the Original Manufacturer representative of the System or someone approved by the System Manufacturer.
- Company Cyber Security Committee who meets regularly to discuss and implement changes required, due to new developments of threats and solutions available.

3.3.3. Detecting and Reporting of Cyber Event[20]

The virus signs as described in section 2.2 will assist in detecting that computer has been compromised which should be treated as possible cyber incident.

The cyber related incident, non-conformities and near miss detected on board must be reported to office. Examples of such incident, non-conformities and near miss are:

- unauthorised access to network infrastructure
- unauthorized or inappropriate use of administrator privileges
- suspicious network activity
- unauthorised access to critical systems
- unauthorised use of removable media
- unauthorised connection of personal devices
- failure to comply with software maintenance procedures
- failure to apply malware and network protection updates
- loss or disruption to the availability of critical systems
- loss or disruption to the availability of data required by critical systems

3.3.4. Equipment Disposal, Including Data Destruction[21]

Obsolete equipment can contain crew personal data and data which is commercially sensitive/confidential. Prior to disposal of the equipment or transfer of the vessel to new manager/owner, company sensitive and crew personal data information is destroyed from the equipment by IT department. Only IT department is authorized to dispose or transfer the computer equipment.

3.4. Contingency Plans[22]

It is important to understand the significance of any cyber incident, particularly for IT and OT systems and prioritise response actions accordingly. Any cyber incident should be assessed to estimate the impact on operations, assets etc. In most cases, a loss of IT systems on board, including a data breach of confidential information, will be a business continuity issue and should not have any impact on the safe operation of the ship.

The loss of OT systems may have a significant and immediate impact on the safe operation of the ship. Should a cyber incident result in the loss or malfunctioning of OT systems, it will be essential that effective actions are taken to ensure the immediate safety of the crew, ship, cargo and protection of the marine environment. It is important that onboard personnel understand

[20] W 50 / 2020
[21] W 50 / 2020
[22] W 50 / 2020

that the loss of OT systems due to a cyber incident must be treated like any other equipment failure.

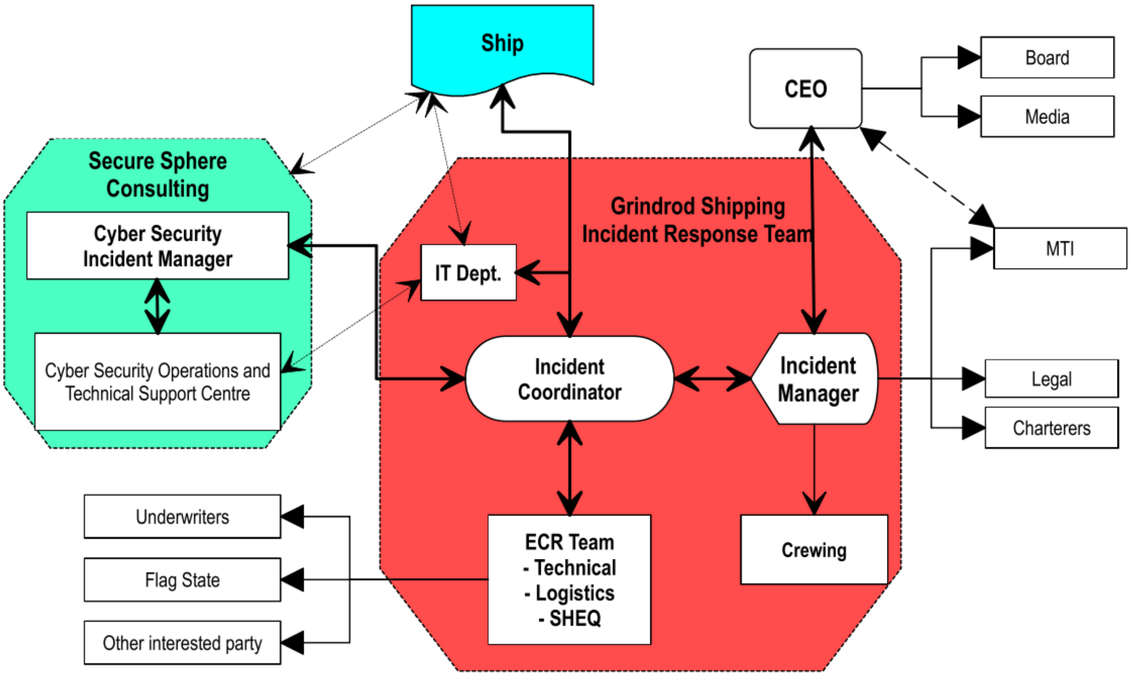
If an onboard OT system is compromised due to cyber-attack or any other reason, the relevant response plans provided in the contingency plan manual must be activated.

The Company has a Cyber Security Plan and Cyber Security Recovery Plan in-place. Both Plans and countermeasures remain confidential but are available to certain parties when authorised by senior management.

3.5. Respond to and Recover from Cyber Security Incidents

The Company has enlisted the services of a dedicated Cyber Security Consultants to advise the Emergency Response Team on the procedure to follow in addressing and recovering from a Cyber Security attack. Both the Vessels and Offices are monitored by the consultants continuously and they will inform The Company of a Cyber-attack.[23]

The Company will then activate it's Cyber Security Emergency Response protocol as detailed in the organogram below:[24]



An effective response should at least consist of the following steps

[23] W 50 / 2020
[24] W 50 / 2020

3.5.1. Initial Assessment:

To ensure an appropriate response, it is essential that the response team find out:

- how the incident occurred
- which IT and/or OT systems were affected and how
- the extent to which the commercial and/or operational data is affected
- to what extent any threat to IT and OT remains.

3.5.2. Recover Systems and Data

Following an initial assessment of the cyber incident, IT and OT systems and data should be cleaned, recovered, and restored, so far as is possible, to an operational condition by removing threats from the system and restoring software.

Record of back-up software available on board in form of CD/DVD/USB is to be kept in Form 1.8.4.[25]

General Recovery procedure is as following which should be carried out under the guidance of IT department:[26]

- Remove the threat
- Clean up the programme
- If clean-up is not possible, restore the programme from a backup (if backup available on board) or
- Attendance on board by an authorized service provider or
- Purchase new OT System/equipment if necessary[27]

3.5.3. Investigate the Incident

To understand the causes and consequences of a cyber incident, an investigation should be undertaken by the company, with support from an external expert, if appropriate. The information from an investigation will play a significant role in preventing a potential recurrence.

3.5.4. Prevent a Re-Occurrence

Considering the outcome of the investigation mentioned above, actions to address any inadequacies in technical and/or procedural protection measures should be

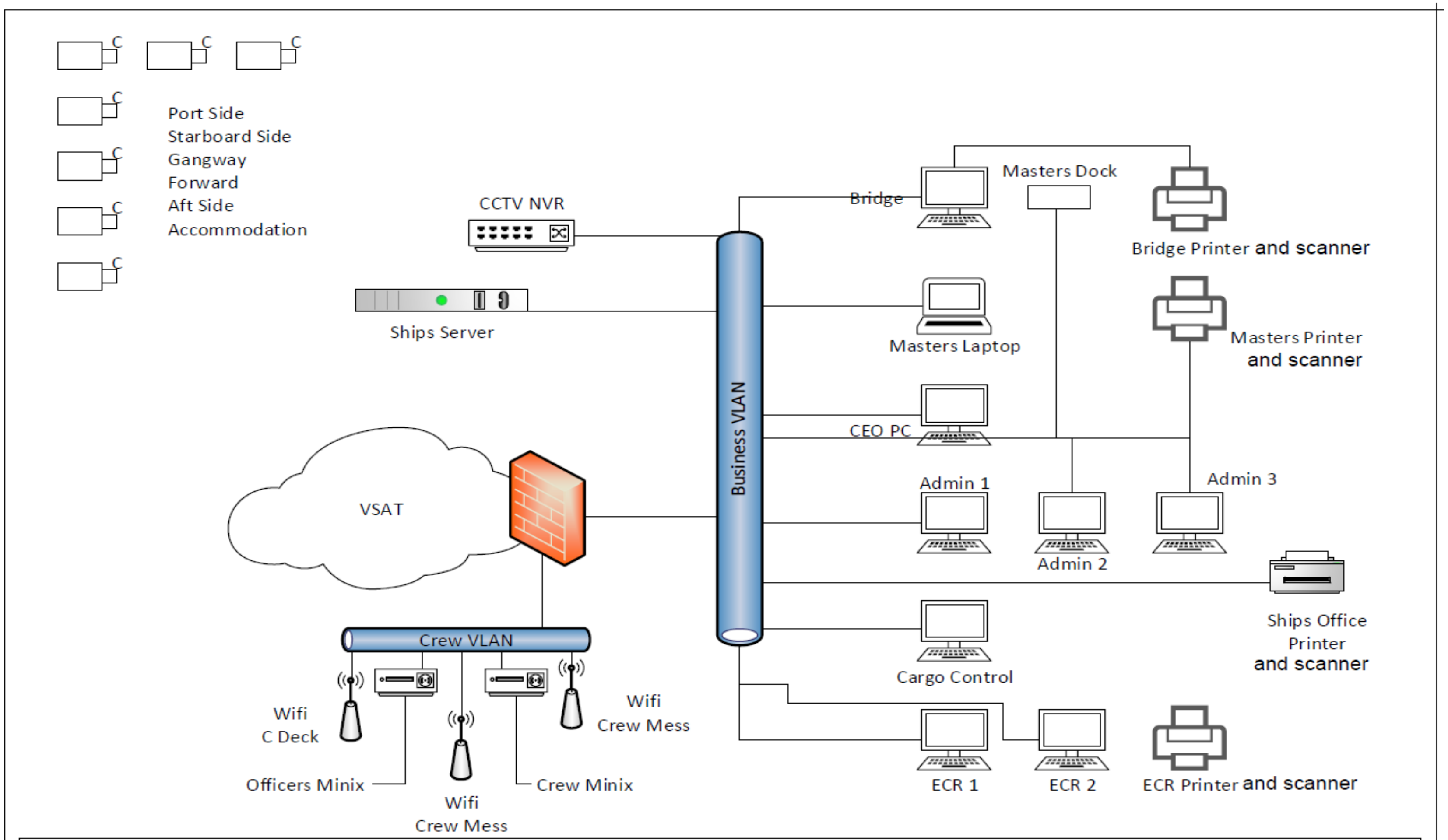
[25] W 50 / 2020
[26] W 50 / 2020
[27] W 50 / 2020

considered, in accordance with the company procedures for implementation of corrective action.

Appendix A: Typical IT Infrastructure found onboard vessels:

Appendix B: Risk Assessment - List of IT and OT systems, Cyber risk, and Control measures

APPENDIX A: TYPICAL IT INFRASTRUCTURE FOUND ONBOARD VESSELS:[28]



Vessel PC Layout – February 2022

[28] W 18 / 2023

APPENDIX B : RISK ASSESSMENT - LIST OF IT AND OT SYSTEMS, CYBER RISK, AND CONTROL MEASURES[29]

IT and OT systems

Information technology (IT) and Operational technology (OT) systems have been identified posing different risk levels to shipboard operations that may be caused by cyber-attacks or by installing the unauthorized software or using the unauthorized removable media. Control measures indicated to mitigate the risk are in addition to the routine maintenance/check/tests conducted on the equipment.

No program shall be installed on board IT and OT system without the knowledge of office.

List of IT and OT systems, Cyber risk, and Control measures

Communication systems (IT)	**Failure consequence/ HSE harm (1-4)**		**Likelihood of failure (1-4)**				**Risk factor= (Consequence x Exposure)**	**Protection/Control measures**	**Person responsible to implement the control measures**
Communication system Business Network (Server)	Impact	1 to 4	Web exposure No=0 Yes=2	USB/Removable media exposure No=0 Yes=2	Other media (external signal) No=0 Yes=2	**Total** (Not less than 1 and not more than 4)			
Communication system Satellite Equipment (VSAT + FBB)	Communication failure, commercial loss	2	2	2	0	4	8	Anti-virus and Firewall in place Auto update of anti-virus Access protected by password No unauthorized access	Master

[29] W 50 / 2020

Communication systems (IT)	**Failure consequence/ HSE harm (1-4)**		**Likelihood of failure (1-4)**				**Risk factor= (Consequence x Exposure)**	**Protection/Control measures**	**Person responsible to implement the control measures**
Communication system Business Network (Server)	Impact	1 to 4	Web exposure No=0 Yes=2	USB/Removable media exposure No=0 Yes=2	Other media (external signal) No=0 Yes=2	**Total** (Not less than 1 and not more than 4)			
Business communication computers – Internet system	Communication failure, commercial loss	2	2	2	0	4	8	Equipment maker's Fireball in place Annual health check by maker Only maker's authorized technician allowed for repair No unauthorized access	Master
Communication system Business Network (Server)	Communication failure, commercial loss	2	2	2	0	4	8	Anti-virus and Firewall in place Auto update of anti-virus No unauthorized access Password protection No unauthorized USB allowed	Master
CREW WELFARE (IT)									
Crew communication computers – Internet system	Contact with family breakdown	2	2	2	0	4	8	Anti-virus and Firewall in place Auto update of anti-virus USB ports made inactive No unauthorized access Password protection USB port inactive	Master
Crew communication system - Wi-Fi network	Contact with family breakdown	2	2	0	0	2	4	Anti-virus and Firewall in place Auto update of anti-virus No unauthorized access Password protection	Master
BRIDGE SYSTEMS (OT)									

Communication systems (IT)	**Failure consequence/ HSE harm (1-4)**		**Likelihood of failure (1-4)**				**Risk factor= (Consequence x Exposure)**	**Protection/Control measures**	**Person responsible to implement the control measures**
Communication system Business Network (Server)	Impact	1 to 4	Web exposure No=0 Yes=2	USB/Removable media exposure No=0 Yes=2	Other media (external signal) No=0 Yes=2	**Total** (Not less than 1 and not more than 4)			
ECDIS	Unavailability of chart, Grounding	4	0	2	0	2	8	Use of dedicated USB for updates by authorized personnel only No unauthorized access Only authorized technician for repair	2NO
GPS	Unavailability of ship's position, Grounding	4	0	2	2	4	16	GPS positions accuracy check No unauthorized access Pay extra attention when navigating in the areas known for jamming and spoofing Duplicated GPS fitted	2NO
Radar	Collision	4	0	2	0	2	8	No unauthorized access Only authorized technician for repair Duplication of the equipment	2NO
Gyro	Steering affected, collision, grounding	3	0	2	0	2	6	No unauthorized access Use magnetic compass in case of failure Only authorized technician for repair	2NO
Speed Log	Loss of speed information	2	0	2	0	2	4	No unauthorized access Only authorized technician for repair	2NO

Communication systems (IT)	**Failure consequence/ HSE harm (1-4)**		**Likelihood of failure (1-4)**				**Risk factor= (Consequence x Exposure)**	**Protection/Control measures**	**Person responsible to implement the control measures**
Communication system Business Network (Server)	Impact	1 to 4	Web exposure No=0 Yes=2	USB/Removable media exposure No=0 Yes=2	Other media (external signal) No=0 Yes=2	**Total** (Not less than 1 and not more than 4)			
Echo Sounder	Unavailability of depth information, grounding	2	0	2	0	2	4	No unauthorized access Only authorized technician for repair	2NO
Navtex	Unavailability of nav warnings	2	0	2	0	2	4	No unauthorized access Only authorized technician for repair	2NO
VHF Radio	Nav/Distress/ Safety communication failure	3	0	2	0	2	6	No unauthorized access Only authorized technician for repair	2NO
AIS	Loss of navigational data/ information	2	0	2	2	4	8	No unauthorized access Only authorized technician for repair and service	2NO
VDR	Loss of ship's events record	2	0	2	0	4	8	No unauthorized access Only authorized technician for repair and service	2NO
Auto pilot system / Heading controller	Loss of steering	3	0	2	0	2	6	No unauthorized access Only authorized technician for repair and service	2NO
Rudder angle signal transmission system	Loss of steering	4	0	2	0	2	8	No unauthorized access Only authorized technician for repair and service	2NO

Communication systems (IT)	**Failure consequence/ HSE harm (1-4)**		**Likelihood of failure (1-4)**				**Risk factor= (Consequence x Exposure)**	**Protection/Control measures**	**Person responsible to implement the control measures**
Communication system Business Network (Server)	Impact	1 to 4	Web exposure No=0 Yes=2	USB/Removable media exposure No=0 Yes=2	Other media (external signal) No=0 Yes=2	**Total** (Not less than 1 and not more than 4)			
Bridge PC ((Digital publications and Nautical & ENC update system)	Unavailability of Nautical publications and corrections	3	2	2	0	4	12	PC protected by password Duplication of the digital publications on master's laptop Use of dedicated USB for updates by authorized personnel only Installation of authorized software only	2NO
GMDSS Equipment	Distress/ Safety communication failure	3	0	2	2	4	12	Duplicate equipment No unauthorized access Only authorized technicians for repair	2NO
CARGO HANDLING AND MANAGEMENT SYSTEMS (OT)									
Loading computer	Loss of hull stresses and stability calculations data, disruption to cargo operation	3	0	2	0	2	6	Protected by password Use of dedicated USB No unauthorized access Installation of authorized software only	CNO
Gas detection system (Fixed and portable meters)	Enclosed space atmosphere not known	3	0	0	0	1	3	Duplicate equipment No unauthorized access Only authorized technician for repair	CNO

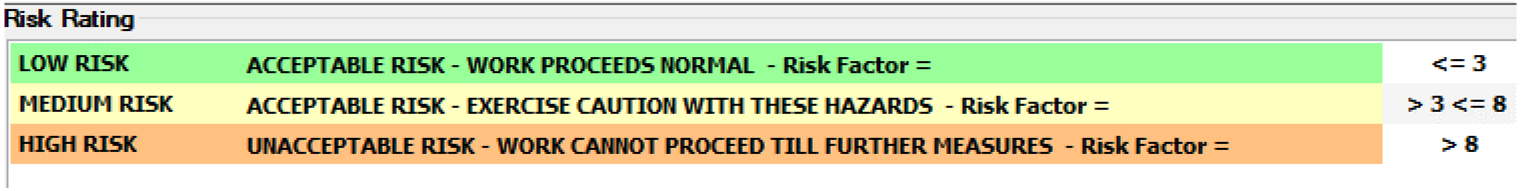
Communication systems (IT)	**Failure consequence/ HSE harm (1-4)**		**Likelihood of failure (1-4)**				**Risk factor= (Consequence x Exposure)**	**Protection/Control measures**	**Person responsible to implement the control measures**
Communication system Business Network (Server)	Impact	1 to 4	Web exposure No=0 Yes=2	USB/Removable media exposure No=0 Yes=2	Other media (external signal) No=0 Yes=2	**Total** (Not less than 1 and not more than 4)			
Water Ingress Alarm system	Flooding, property damage	3	0	0	0	1	3	No unauthorized access Only maker's authorized technician for repair	CNO
Cargo monitoring and control system – Level/Pressure/Temp/Valve/Alarms (Krone)	Cargo overflow, Harm to environment	4	0	2	0	2	6	Protected by password No unauthorized access Installation of authorized software only Only maker's authorized technician for repair	CNO
Cargo pump speed control system (ABB VSD)	Pipe ruptures, Harm to environment	4	0	2	0	2	6	Protected by password No unauthorized access Installation of authorized software only Only maker's authorized technician for repair	CEO
ODME (applicable for tanker)	Environmental pollution	3	0	2	0	2	6	No unauthorized access Password protection	CNO
PROPULSION AND MACHINERY MANAGEMENT AND POWER CONTROL SYSTEMS (OT)									
A/Es Power Management systems	Environmental pollution, Harm to people, Loss of property	3	0	2	0	2	6	No unauthorized access Password protection	CEO

Communication systems (IT)	**Failure consequence/ HSE harm (1-4)**		**Likelihood of failure (1-4)**				**Risk factor= (Consequence x Exposure)**	**Protection/Control measures**	**Person responsible to implement the control measures**
Communication system Business Network (Server)	Impact	1 to 4	Web exposure No=0 Yes=2	USB/Removable media exposure No=0 Yes=2	Other media (external signal) No=0 Yes=2	**Total** (Not less than 1 and not more than 4)			
M/E, A/Es & other machinery alarm system	Environmental pollution, Harm to people, Loss of property		0	2	0	2	6	No unauthorized access Password protection	CEO
M/E online monitoring system (MAN B&W 6G50ME-B9.3)	Loss of data monitoring	2	2	2	0	4	8	Installed with Enginevault (Cyber security hardware/software system) Access protected by password No unauthorized access Only maker's authorized technician for guidance/repair	CEO
Power control system – VFD (DESMI)	Harm to environment	2	2	2	0	4	8	Manual override provided Web access is password protected No unauthorized access Installation of authorized software only Only maker's authorized technician for repair	CEO
PROPULSION AND MACHINERY MANAGEMENT AND POWER CONTROL SYSTEMS (OT)									
A/Es Power Management systems	Environmental pollution, Harm to people, Loss of property	3	0	2	0	2	6	No unauthorized access Password protection	CEO

Communication systems (IT)	**Failure consequence/ HSE harm (1-4)**		**Likelihood of failure (1-4)**				**Risk factor= (Consequence x Exposure)**	**Protection/Control measures**	**Person responsible to implement the control measures**
Communication system Business Network (Server)	Impact	1 to 4	Web exposure No=0 Yes=2	USB/Removable media exposure No=0 Yes=2	Other media (external signal) No=0 Yes=2	**Total** (Not less than 1 and not more than 4)			
M/E, A/Es & other machinery alarm system	Environmental pollution, Harm to people, Loss of property		0	2	0	2	6	No unauthorized access Password protection	CEO
M/E online monitoring system (MAN B&W 6G50ME-B9.3)	Loss of data monitoring	2	2	2	0	4	8	Installed with Engine vault (Cyber security hardware/software system) Access protected by password No unauthorized access Only maker's authorized technician for guidance/repair	CEO
Power control system – VFD (DESMI)	Harm to environment	2	2	2	0	4	8	Manual override provided Web access is password protected No unauthorized access Installation of authorized software only Only maker's authorized technician for repair	CEO
Incinerator	Harm to environment		0	2	0	2	4	No unauthorized access Only authorized technician for repair	CEO
Inert Gas system	Fire and explosion	2	0	2	0	2	4	No unauthorized access Only authorized technician for repair	CEO

Communication systems (IT)	**Failure consequence/ HSE harm (1-4)**		**Likelihood of failure (1-4)**				**Risk factor= (Consequence x Exposure)**	**Protection/Control measures**	**Person responsible to implement the control measures**
Communication system Business Network (Server)	Impact	1 to 4	Web exposure No=0 Yes=2	USB/Removable media exposure No=0 Yes=2	Other media (external signal) No=0 Yes=2	**Total** (Not less than 1 and not more than 4)			
OWS	Harm to environment	3	0	2	0	2	6	No unauthorized access Only authorized technician for repair	CEO
BWTS	Harm to environment	3	0	2	0	2	6	No unauthorized access Only authorized technician for repair	CEO
Ballast Water control system	Delays, unstable ship								
ACCESS CONTROL SYSTEMS (OT)									
Bridge Navigational Watch Alarm System (BNWAS)	Loss of alerting system	3	0	2	0	2	6	No unauthorized access Only authorized technician for repair Compliance with the bridge manning level	Master
Ship Security Alarm Systems (SSAS)/Polestar	Loss of Security breach communication	2	2	0	2	4	8	No unauthorized access Only authorized technician for repair Other means of communication available	Master
Ship Security Alarm Systems (SSAS)/Inmarsat-C	Loss of Security breach communication	2	0	2	0	2	4	No unauthorized access Only authorized technician for repair Other means of communication available	Master

Communication systems (IT)	**Failure consequence/ HSE harm (1-4)**		**Likelihood of failure (1-4)**				**Risk factor= (Consequence x Exposure)**	**Protection/Control measures**	**Person responsible to implement the control measures**
Communication system Business Network (Server)	Impact	1 to 4	Web exposure No=0 Yes=2	USB/Removable media exposure No=0 Yes=2	Other media (external signal) No=0 Yes=2	**Total** (Not less than 1 and not more than 4)			
CCTV network	Loss of pictorial data	1	2	2	0	4	4	No unauthorized access Only authorized technician for repair	Master
ADMINISTRATIVE SYSTEMS (IT)									
PMS system - Mespas[30]	Regulatory non-compliance	2	2	2	0	4	8	Anti-virus and Firewall in place No unauthorized access Password protection	Master
Work/Rest hours system – ISF Watchkeeper	Regulatory non-compliance	2	2	2	0	4	8	Anti-virus and Firewall in place No unauthorized access Password protection	Master
Crew training system - Karko	Harm to people	2	2	2	0	4	8	Anti-virus and Firewall in place No unauthorized access Password protection	2NO
SHEQ System	Regulatory non-compliance	2	2	2	0	4	8	Anti-virus and Firewall in place No unauthorized access Password protection	Master



Risk Rating

LOW RISK	ACCEPTABLE RISK - WORK PROCEEDS NORMAL - Risk Factor =	<= 3
MEDIUM RISK	ACCEPTABLE RISK - EXERCISE CAUTION WITH THESE HAZARDS - Risk Factor =	> 3 <= 8
HIGH RISK	UNACCEPTABLE RISK - WORK CANNOT PROCEED TILL FURTHER MEASURES - Risk Factor =	> 8

[30] W 30 / 2024