CR

CR Classification Society

FOUNDED 1951

GUIDELINES FOR CYBER SECURITY ONBOARD SHIPS 2020

CR CLASSIFICATION SOCIETY

September 2020

REVISION HISTORY

(This version supersedes all previous ones.)

Revision No.	Editor	Date (yyyy-mm)
001	Rules Section	2020-09

GUIDELINES FOR CYBER SECURITY ONBOARD SHIPS
2020

CONTENTS

CHAPTER 1 GENERAL

1.1 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) 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.In 2017, the International Maritime Organization (IMO) adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management System (SMS). The Resolution stated that an approved SMS should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code. It further encourages administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021. The same year, IMO developed guidelines [1] that provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. As also highlighted in the IMO guidelines, effective cyber risk management should start at the senior management level.

Senior management should embed a culture of cyber risk awareness into all levels and departments of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.

1.1.1 MSC.428(98):

Recognizing the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks.

Encourages Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021

1.1.2 ISM (International Safety Management) Code 1.2.2:

Safety management objectives of the Company should, inter alia […] assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards.

1.1.3 ISPS (International Ship and Port Facility Security) Code Part B, 8.3:

A Ship Security Assessment (SSA) should address the important elements including radio and telecommunication systems, as well as computer systems and networks, on board or within the ship.

1.1.4 MSC-FAL.1/Circ.3 on Guidelines on maritime cyber risk management:

(a) Stakeholders should take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping.

[1] MSC-FAL.1/Circ.3 on Guidelines on maritime cyber risk management.

(b) Risk management is fundamental to safe and secure shipping operations. Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitization, integration, automation and network-based systems has created an increasing need for cyber risk management in the shipping industry.

(c) Effective cyber risk management should start at the senior management level. Senior management should embed a culture of cyber risk awareness into all levels of an organisation and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.

(d) Vulnerabilities created by accessing, interconnecting or networking numerous systems can lead to cyber risks which should be addressed. Vulnerable systems could include, but are not limited to systems list in 3.2.

1.1.5 More guidance on how to incorporate cyber risk management into the company's SMS can be found in Annex 3 of the Guidelines.

1.2 Application

The Guidelines on Cyber Security Onboard Ships (hereinafter referred to as the Guidelines) are intended to offer guidance to shipowners and operators on procedures and actions to maintain the security of cyber systems in the company and onboard the ships. In addition, the Guidelines are intended to help IT and industrial automation control system professionals to join their efforts towards building and maintaining cyber security resilience of the total set of the assets and processes employed to conduct the company's business.

The Guidelines are not intended to provide a basis for, and should not be interpreted as, calling for external auditing or vetting the individual company's and ship's approach to cyber risk management.

1.2.1 Approaches to cyber security will be company- and ship-specific, but should be guided by appropriate standards and the requirements of relevant national, international and flag state regulations. The Guidelines provide a risk-based approach to identifying and responding to cyber threats. Following a risk based approach, the decisions of what is critical and high priority is then left at the discretion of the organisation. An important aspect is that relevant personnel should have training in identifying the typical modus operandi of cyber attacks.

1.2.2 Different members of the management team might have different exposure and levels of responsibility towards cyber security. Depending on different needs and organization size, the security level may differ from high level management, basic capabilities to comprehensive, very technical in depth. Assessment, protection, as well as improvement activities can be scaled accordingly.

1.2.3 Class notation

For ship complying with the requirements of the Guidelines, the class notation **Cyber-S** will be assigned to the ship. Any suffix and description may be added in the curly bracket after the notation, e.g.: "**Cyber-S{...}**".

1.3 Best Practices for Implementation of Cyber Risk Management

1.3.1 The approach to cyber risk management described herein provides a foundation for better understanding and managing cyber risks, thus enabling a risk management approach to address cyber threats and vulnerabilities. For detailed guidance on cyber risk management, users of the Guidelines should also refer to Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

1.3.2 Additional guidance and standards may include, but are not limited to:

(a) NIST framework:

United States National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity. NIST aims to help understand, manage and express cyber security risks both internally and externally, for example within a ship's organisation. It can help to identify and prioritise actions for reducing cyber security risks. It is also a tool for aligning policy, business and technological approaches to manage the risks.

(b) CIS Controls:

The Center for Internet Security (CIS) Controls consist of 20 key actions, called Critical Security Controls (CSC), that organizations should take to block or mitigate known attacks. The controls are designed so that primarily automated means can be used to implement, enforce and monitor them. The security controls give no-nonsense, actionable recommendations for cyber security, written in language that's easily understood by IT personnel.

(c) ISO/IEC 27001, CNS 27001:

Standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO 27001 certification involves 114 controls which aims are a combined secure architecture, preventive, detective controls and several controls and encompass procedural, physical, technical and most importantly personnel controls.

(d) IACS Rec. No. 166:

Recommendation on Cyber Resilience, which consolidates IACS' previous 12 Recommendations related to cyber resilience (Nos. 153 to 164) and applies to the use of computer-based systems which provide control, alarm, monitoring, safety or internal communication functions, and provides:

(1) guidance for mitigating the risk related to events affecting onboard computer-based systems, and

(2) goals for design and construction, functional requirements, technical requirements and verification testing.

1.3.3 Reference should be made to the most current version of any guidance or standards utilized.

1.4 Definition

1.4.1 Access control is selective limiting of the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions.

1.4.2 Back door is a secret method of bypassing normal authentication and verification when accessing a system. A back door is sometimes created by hidden parts of the system itself or established by separate software.

1.4.3 Bring your own device (BYOD): allows employees to bring personally owned devices (laptops, tablets, and smart phones) to the ship and to use those devices to access privileged information and applications for business use.

1.4.4 Cyber attack is any type of offensive manoeuvre that targets IT and OT systems, computer networks, and/or personal computer devices attempting to compromise, destroy or access company and ship systems and data.

1.4.5 Cyber incident is an occurrence, which actually or potentially results in adverse consequences to an onboard system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences.

1.4.6 Cyber risk management means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level; taking into consideration the costs and benefits of actions taken by stakeholders.

1.4.7 Cyber system is any combination of facilities, equipment, personnel, procedures and communications integrated to provide cyber services; examples include business systems, control systems and access control systems.

1.4.8 Defence in breadth is a planned, systematic set of activities that seek to identify, manage, and reduce exploitable vulnerabilities in IT and OT systems, networks and equipment at every stage of the system, network, or sub-component life cycle. Onboard ships this approach will generally focus on network design, system integration, operations and maintenance.

1.4.9 Defence in depth is an approach which uses layers of independent technical and procedural protection measures to protect IT and OT on board.

1.4.10 Executable software includes instructions for a computer to perform specified tasks according to encoded instructions.

1.4.11 Firewall is a logical or physical break designed to prevent unauthorised access to IT infrastructure and information.

1.4.12 Firmware is software imbedded in electronic devices that provides control, monitoring and data manipulation of engineered products and systems. They are normally self-contained and not accessible to user manipulation.

1.4.13 Flaw is unintended functionality in software.

1.4.14 Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

1.4.15 Intrusion Prevention Systems (IPSs), also known as Intrusion Detection and Prevention Systems (IDPSs), are network security appliances that monitor network and/or system activities for malicious activity.

1.4.16 Information technology (IT) is the use of computers to store, retrieve, transmit, and manipulate data, or information, including all hardware, software and peripheral equipment.

1.4.17 Local Area Network (LAN) is a computer network that interconnects computers within a limited area such as a home, ship or office building, using network media.

1.4.18 Malware is a generic term for a variety of malicious software which can infect computer systems and impact on their performance.

1.4.19 Operational technology (OT) includes devices, sensors, software and associated networking that monitor and control onboard systems.

1.4.20 Patches are software designed to update software or supporting data to improve the software or address security vulnerabilities and other bugs in operating systems or applications.

1.4.21 Phishing refers to the process of deceiving recipients into sharing sensitive information with a third-party.

1.4.22 Principle of least privilege refers to the restriction of user account privileges only to those with privileges that are essential to perform its intended function.

1.4.23 Producer is the entity that manufactures the shipboard equipment and associated software.

1.4.24 Recovery refers to the activities after an incident to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.

1.4.25 Removable media is a collective term for all methods of storing and transferring data between computers. This includes laptops, USB memory sticks, CDs, DVDs and diskettes.

1.4.26 Risk assessment is the process which collects information and assigns values to risks for informing priorities, developing or comparing courses of action, and informing decision making.

1.4.27 Risk management is the process of identifying, analysing, assessing and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

1.4.28 Sandbox is an isolated environment, in which a program may be executed without affecting the underlying system (computer or operating system) and any other applications. A sandbox is often used when executing untrusted software.

1.4.29 Service provider is a company or person who provides and performs software maintenance.

1.4.30 Social engineering is a method used to gain access to systems by tricking a human into revealing confidential information.

1.4.31 Software whitelisting means specifying the software which may be present and active on an IT or OT system.

1.4.32 Virtual Local Area Network (VLAN) is the logical grouping of network nodes. A virtual LAN allows geographically dispersed network nodes to communicate as if they were physically on the same network.

1.4.33 Virtual Private Network (VPN) enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, thereby benefiting from the functionality, security and management policies of the private network.

1.4.34 Virus is a hidden, self-replicating section of computer software that maliciously infects and manipulates the operation of a computer program or system.

1.4.35 Wi-Fi is all short-range communications that use some type of electromagnetic spectrum to send and/or receive information without wires.

CHAPTER 2 CYBER SECURITY AND SAFETY MANAGEMENT

2.1 General

2.1.1 Both cyber security and cyber safety are important because of their potential effect on personnel, the ship, environment, company and cargo. Cyber security is concerned with the protection of IT, OT, information 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.

2.1.2 Cyber safety incidents can arise as the result of:

(a) 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);

(b) a failure occurring during software maintenance and patching;

(c) 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).

2.1.3 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.

2.2 Plans and Procedures

2.2.1 Company plans and procedures for cyber risk management should be complementary to the existing security and safety risk management requirements contained in the ISM Code[2] and ISPS Code[3]. Cyber security should be considered at all levels of the company, from senior management ashore to onboard personnel, as an inherent part of the safety and security culture necessary for the safe and efficient operation of the ship.

2.2.2 In accordance with chapter 8 of the ISPS Code, the ship is obliged to conduct a security assessment, which should include all operations that are important to protect. The assessment should address radio and telecommunication systems, including computer systems and networks (part B, paragraph 8.3 of the ISPS Code). This calls for controlling and monitoring “the ship to shore” path of the internet connection, which is important owing to the fast adoption of sophisticated and digitalised onboard OT systems that in many cases have not been designed to be cyber resilient.

2.2.3 The objective of the company's Safety Management System (SMS) is to provide a safe working environment by establishing appropriate safe practices and procedures based on an assessment of all identified risks to the ship, onboard personnel and the environment. In the context of ship operations, cyber incidents are anticipated to result in physical effects and potential safety and/or pollution incidents. This means that the company needs to assess risks arising from the use of IT and OT onboard ships and establish appropriate safeguards against cyber incidents.

2.2.4 The SMS should include instructions and procedures to ensure the safe operation of ships and protection of the environment in compliance with relevant international and flag state legislation. These instructions and procedures

[2] International Management Code for the Safe Operation of Ships and for Pollution Prevention (ISM Code).
[3] International Ship and Port Facility Security Code (ISPS Code).

should consider risks arising from the use of IT and OT on board, as appropriate, taking into account applicable codes, guidelines and recommended standards.

2.2.5 When incorporating cyber risk management into the company SMS, consideration should be given to whether, in addition to a generic risk assessment of the ships it operates, a particular ship needs a specific risk assessment. The company should consider the need for a specific risk assessment based on whether a particular ship is unique within their fleet. This should consider factors, including but not limited to the extent to which IT and OT is used on board, the complexity of system integration and the nature of operations.

2.2.6 Cyber risk management should:

(a) identify the roles and responsibilities of users, key personnel, and management both ashore and on board;

(b) identify the systems, assets, data and capabilities, which if disrupted, could pose risks to the ship's operations and safety;

(c) implement technical measures to protect against a cyber incident and ensure continuity of operations. This may include configuration of networks, access control to networks and systems, communication and boundary defence and the use of protection and detection software

(d) implement activities and plans (procedural protection measures) to provide resilience against cyber incidents. This may include training and awareness, software maintenance, remote and local access, access privileges, use of removable media and equipment disposal;

(e) implement activities to prepare for and respond to cyber incidents.

2.2.7 In recognising that some aspects of work to include cyber risk management in safety management systems may include commercially sensitive or confidential information, companies should consider protecting this information appropriately. As far as possible, policies and procedures included in a safety management system should not include sensitive information like this.

2.3 Key Aspects of Cyber Security

The development, understanding and awareness of key aspects of cyber security and safety are list as below:

2.3.1 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.

2.3.2 Identify vulnerabilities:

Develop inventories of onboard systems with direct and indirect communications links. Understand the consequences of a cyber security threat on these systems. Understand the capabilities and limitations of existing protection measures.

2.3.3 Assess risk exposure:

Determine the likelihood of vulnerabilities being exploited by 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.

2.3.4 Develop protection and detection measures:

Reduce the likelihood of vulnerabilities being exploited through protection measures. Reduce the potential impact of a vulnerability being exploited.

2.3.5 Establish contingency plans:

Develop a response plan to reduce the impact of threats that are realised on the safety and security of the ship.

2.3.6 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 reassess threats and vulnerabilities.

2.4 Defence in Depth and in Breadth

2.4.1 Using more than one technical or procedural protection measure is recommended. It is essential to protect critical systems and data with multiple layers of protection measures which take into account the role of personnel, procedures and technology to:

(a) increase the probability that a cyber incident is detected;

(b) increase the effort and resources required to protect information, data or the availability of IT and OT systems.

2.4.2 This defence in depth approach encourages a combination of:

(a) physical security of the ship in accordance with the ship security plan (SSP);

(b) protection of networks, including effective segmentation;

(c) intrusion detection;

(d) software whitelisting;

(e) access and user controls;

(f) appropriate procedures regarding the use of removable media and password policies;

(g) personnel's awareness of the risk and familiarity with appropriate procedures.

2.4.3 Company policies and procedures should ensure that cyber security is considered within the overall approach to safety and security risk management. The complexity and potential persistence of cyber threats means that a “defence in depth” approach should be considered. Equipment and data protected by layers of protection measures are more resilient to cyber attacks.

2.4.4 However, onboard ships where levels of integration between cyber systems may be high, defence in depth only works if technical and procedural protection measures are applied in layers across all vulnerable and integrated systems.

This is “defence in breadth” and it is used to prevent any vulnerabilities in one system being used to circumvent protection measures of another system.

2.4.5 Defence in depth and defence in breadth are complementary approaches which, when implemented together, provide the foundation of a holistic response to the management of cyber risks.

CHAPTER 3 IDENTIFY THREATS

3.1 Circumstances

3.1.1 The cyber risk[4] is specific to the company, ship, operation and/or trade. When assessing the risk, companies should be aware of any specific aspects of their operations that might increase their vulnerability to cyber incidents.

3.1.2 Unlike other areas of safety and security where historic evidence is available and reporting of incidents is required, cyber security is made more challenging by the absence of any definitive information about the incidents and their impact. Until this evidence is obtained, the scale and frequency of attacks will continue to be unknown.

3.1.3 Experiences from other business sectors such as financial institutions, public administration and air transport have shown that successful cyber attacks might result in a significant loss of services, assets and even endanger human lives. Such events argue that the shipping industry should also work proactively to understand and mitigate cyber threats.

3.2 Examples of Cyber Threats

3.2.1 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 companies and the ships they operate:

Table 1 Motivation and objectives

Group	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, off vessel transportation and handling plans etc
Opportunists	• The challenge	• Getting through cyber security defences • Financial gain
States State sponsored organizations Terrorists	• Political gain • Espionage	• Gaining knowledge • Disruption to economies and critical national infrastructure

3.2.2 The groups in Table 1 are active and have the skills and resources to threaten the safety and security of ships, and a company's ability to conduct its business.

3.2.3 In addition, there is the possibility that company personnel, on board and ashore, could compromise cyber systems and data. In general, the company should be prepared that this may be unintentional and caused by human error

[4] The text in this chapter has been summarised from CESG, Common Cyber Attacks: Reducing the Impact.

when operating and managing IT and OT systems or failure to respect technical and procedural protection measures.
3.2.4 There is, however, the possibility that actions may be malicious and are a deliberate attempt to damage the company and the ship that is by a disgruntled employee.

3.3 Types of Cyber Attack[5]

3.3.1 Categories of cyber attacks:

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

(a) Untargeted attacks, where a company or a ship's systems and data are one of many potential targets;

(b) Targeted attacks, where a company or a ship's systems and data are the intended target.

3.3.2 Untargeted attacks

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. Examples of some tools and techniques that may be used in these circumstances include:

(a) 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. Ransomware encrypts data on systems until a ransom has been paid. Malware may also exploit known deficiencies and problems in outdated/unpatched business software. The term exploit usually refers to the use of a software or code, which is designed to take advantage and manipulate a problem in another computer software or hardware. This problem can, for example, be a code bug, system vulnerability, improper design, hardware malfunction, and error in protocol implementation These vulnerabilities may be exploited remotely or triggered locally. Locally, a piece of malicious code may often be executed by the user, sometimes via links distributed in email attachments or through malicious websites.

(b) Social engineering:

A non-technical technique used by potential cyber attackers to manipulate insider individuals into breaking security procedures, normally, but not exclusively, through interaction via social media.

(c) Phishing:

Sending emails to a large number of potential targets asking for particular 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.

(d) Water holing:

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

(e) Scanning:

Attacking large portions of the internet at random.

[5] In 2016, IHS Markit together with BIMCO carried out a cyber security survey. The respondent from the shipping industry had experienced the mentioned forms of attacks. Four percent of the attacks were directed at ship borne systems.

3.3.3 Targeted attacks

Targeted attacks may be more sophisticated and use tools and techniques specifically created for targeting a company or ship. Examples of tools and techniques which may be used in these circumstances include:

(a) 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.

(b) Denial of service (DoS):

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.

(c) Spear-phishing:

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

(d) Subverting the supply chain:

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

3.3.4 The above examples are not exhaustive. Other methods are evolving for example impersonating a legitimate shore based employee in a shipping company to obtain valuable information, which can be used for a further attack. The potential number and sophistication of tools and techniques used in cyber attacks continue to evolve and are limited only by the ingenuity of those organisations and individuals developing them.

3.4 Stages of a Cyber Attack

Cyber attacks are conducted in stages. The length of time taken to prepare a cyber attack can be determined by the motivations and objectives of the attacker, and the resilience of technical and procedural cyber security controls implemented by the company, including those onboard its ships. The four stages of an attack are:

3.4.1 Survey/reconnaissance:

Open/public sources used to gain information about a company, ship or seafarer, which can be used to prepare for a cyber attack. Social media, technical forums and hidden properties in websites, documents and publications may be used to identify technical, procedural and physical vulnerabilities. The use of open/public sources may be complemented by monitoring (analysing – sniffing) the actual data flowing into and from a company or a ship.

3.4.2 Delivery:

Attackers may attempt to access company and ship systems and data. This may be done from either within the company or ship or remotely through connectivity with the internet. Examples of methods used to obtain access include:

(a) company online services, including cargo or consignment tracking systems;

(b) sending emails containing malicious files or links to malicious websites to personnel;

(c) providing infected removable media, for example as part of a software update to an onboard system;

(d) creating false or misleading websites which encourage the disclosure of user account information by personnel.

3.4.3 Breach:

The extent to which an attacker can breach a company or ship system will depend on the significance of the vulnerability found by an attacker and the method chosen to deliver an attack. It should be noted that a breach might not result in any obvious changes to the status of the equipment. Depending on the significance of the breach, an attacker may be able to:

(a) make changes that affect the system's operation, for example interrupt or manipulate information used by navigation equipment;

(b) gain access to commercially sensitive data such as cargo manifests and/or crew and passenger lists;

(c) achieve full control of a system, for example a machinery management system.

3.4.4 Effect:

The motivation and objectives of the attacker will determine what effect they have on the company or ship system and data. An attacker may explore systems, expand access and/or ensure that they are able to return to the system in order to:

(a) access commercially sensitive or confidential data about cargo, crew and passengers to which they would otherwise not have access;

(b) manipulate crew or passenger lists, or cargo manifests. this may be used to allow the fraudulent transport of illegal cargo, or facilitate thefts;

(c) cause complete denial of service on business systems;

(d) enable other forms of crime for example piracy, theft and fraud;

(e) disrupt normal operation of the company and ship systems, for example by deleting critical pre-arrival information or overloading company systems.

It is crucial that users of IT systems onboard ships are aware of the potential cyber security risks, and are trained to identify and mitigate such risks.

CHAPTER 4 IDENTIFY VULNERABILITIES

4.1 Assessment of Potential Threats

4.1.1 It is recommended that a shipping company initially performs an assessment of the potential threats that may realistically be faced. This should be followed by an assessment of the systems and onboard procedures to map their robustness to handle the current level of threat. These vulnerability assessments should then serve as the foundation for a senior management level discussion/workshop. It may be facilitated by internal experts or supported by external experts with knowledge of the maritime industry and its key processes, resulting in a strategy centred around the key risks. The distinction between IT and OT systems should be considered. IT systems focus on the use of data as information whilst OT systems focus on the use of data to control or monitor physical processes.

4.1.2 Stand-alone systems will be less vulnerable to external cyber attacks compared to those attached to uncontrolled networks or directly to the internet. Network design and network segregation will be explained in more detail in Annex 2. Care should be taken to understand how critical shipboard systems might be connected to uncontrolled networks. When doing so, the human element should be taken into consideration, as many incidents are initiated by personnel's actions.

4.2 Onboard Systems

Onboard systems could include:

4.2.1 Cargo management systems:

Digital systems used for the management and control of cargo, including hazardous cargo, may interface with a variety of systems ashore. Such systems may include shipment-tracking tools available to shippers via the internet. Interfaces of this kind make cargo management systems and data in cargo manifests vulnerable to cyber attacks.

4.2.2 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. 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. A cyber incident can extend to service denial or manipulation, and therefore may affect all systems associated with navigation, including ECDIS, GNSS, AIS, VDR and Radar/ARPA.

4.2.3 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. The vulnerability of these systems can increase when they are used in conjunction with remote condition-based monitoring and/or are integrated with navigation and communications equipment on ships using integrated bridge systems.

4.2.4 Access control systems:

Digital systems used to support access control to ensure physical security and safety of a ship and its cargo, including surveillance, shipboard security alarm, and electronic “personnel-on-board” systems.

4.2.5 Passenger servicing and management systems:

Digital systems used for property management, boarding and access control may hold valuable passenger related data. Intelligent devices (tablets, handheld scanners etc.) are themselves an attack vector as ultimately the collected data is passed on to other systems.

4.2.6 Passenger facing public networks:

Fixed or wireless networks connected to the internet, installed on board for the benefit of passengers, for example guest entertainment systems. These systems should be considered uncontrolled and should not be connected to any safety critical system on board.

4.2.7 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. They can be exploited by cyber attackers to gain access to onboard systems and data. These systems should be considered uncontrolled and should not be connected to any safety critical system on board. Software provided by ship management companies or owners is also included in this category.

4.2.8 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 systems and data.

The above-mentioned onboard systems consist of potentially vulnerable equipment which should be reviewed during the assessment. More detail can be found in Annex 1 of the Guidelines.

4.3 Ship to Shore Interface

4.3.1 Ships are becoming more and more integrated with shoreside operations because digital communication is being used to conduct business, manage operations, and stay in touch with head office. Further, critical ship systems essential to the safety of navigation, power and cargo management have been increasingly digitalised and connected to the internet to perform a wide variety of legitimate functions such as:

(a) engine performance monitoring;

(b) maintenance and spare parts management;

(c) cargo, crane and pump management;

(d) voyage performance monitoring.

4.3.2 The above list provides examples of this interface and is not exhaustive. The above systems provide data which may be of interest to cyber criminals to exploit.

4.3.3 Modern technologies can add vulnerabilities to the ships especially if there are insecure designs of networks and uncontrolled access to the internet. Additionally, shoreside and onboard personnel may be unaware how some equipment producers maintain remote access to shipboard equipment and its network system. The risks of misunderstood, unknown, and uncoordinated remote access to an operating ship should be taken into consideration as an important part of the risk assessment.

4.3.4 It is recommended that companies should fully understand the ship's OT and IT systems and how these systems connect and integrate with the shore side. This requires an understanding of all computer based onboard systems and how safety, operations, and business can be compromised by a cyber incident.

4.3.5 The following should be considered regarding producers and third parties including contractors and service providers:

(a) The producer's and service provider's cyber security awareness and procedures: Many of these companies lack cyber awareness training and governance in their own organisations and this may represent more sources of vulnerability, which could result in cyber incidents. The companies should have an updated cyber security company policy, which includes training and governance procedures for accessible IT and OT onboard systems.

(b) The maturity of a third-party's cyber security procedures: The shipowner should query the internal governance for cyber network security, and seek to obtain a cyber security assurance when considering future contracts and services. This is particularly important when covering network security if the ship is to be interfaced with the third-party.

4.4 Common Vulnerabilities

4.4.1 The following are common cyber vulnerabilities, which may be found onboard existing ships, and on some newbuild ships:

(a) Obsolete and unsupported operating systems.

(b) Outdated or missing antivirus software and protection from malware.

(c) Inadequate security configurations and best practices, including ineffective network management and the use of default administrator accounts and passwords, and ineffective network management which is not based on the principle of least privilege.

(d) Shipboard computer networks, which lack boundary protection measures and segmentation of networks.

(e) Safety critical equipment or systems always connected with the shore side.

(f) Inadequate access controls for third parties including contractors and service providers.

CHAPTER 5 ASSESS RISK EXPOSURE

5.1 Overview

5.1.1 Accountability and ownership for cyber security assessment should start at senior management level of a company, instead of being immediately delegated to the ship security officer or the head of the IT department. There are several reasons for this:

(a) Initiatives to heighten cyber security may at the same time affect standard business procedures and operations, rendering them more time consuming or costly. It is therefore a senior management level strategic responsibility to evaluate and decide on risk versus reward trade-offs.

(b) A number of initiatives which would heighten cyber security are related to business processes and training, and not to IT systems, and therefore need to be anchored organisationally outside the IT department.

(c) Initiatives which heighten cyber security awareness may change how the company interacts with customers, suppliers and authorities, and impose new requirements on the co-operation between the parties. It is a senior management level decision whether and how to drive changes in these relationships.

(d) Only when the above three aspects have been decided upon will it be possible to clearly outline what the IT requirements of the cyber security strategy will be, and this is the element which can be placed with the IT department.

(e) Based on the strategic decisions in general, and the risk versus reward trade-offs, relevant contingency plans should be established in relation to handling cyber incidents if they should occur.

Senior management should realise their leadership responsibilities by delegating authority and allocating the budget needed to carry out the risk assessment and to develop solutions that are best suit for the company and the operation of their ships.

5.1.2 The level of cyber risk will reflect the circumstances of the company, ship (its operation and trade), the IT and OT systems used, and the information and/or data stored. The maritime industry possesses a range of characteristics which affect its vulnerability to cyber incidents:

(a) the cyber controls already implemented by the company and onboard its ships;

(b) multiple stakeholders are often involved in the operation and chartering of a ship potentially resulting in lack of accountability for the IT infrastructure;

(c) the ship being online and how it interfaces with other parts of the global supply chain;

(d) ship equipment being remotely monitored eg by the producers;

(e) business-critical, data sensitive and commercially sensitive information shared with shore-based service providers;

(f) the availability and use of computer-controlled critical systems for the ship's safety and for environmental protection.

These elements should be considered, and relevant parts incorporated into the company security policies, safety management systems, and ship security plans. Users of these guidelines should refer to specific national legislation and flag state requirements as well as relevant international and industry standards and best practices when developing and implementing cyber risk management procedures.

IT and OT systems, software and maintenance can be outsourced to third-party service providers and the company itself may not possess a way of verifying the level of security supplied by these providers. 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"[6] will increase the amount of information available to cyber attackers and the potential attack surface to cyber criminals. This makes the need for robust approaches to cyber security important both now and in the future.

5.1.3 Third-party access

Visits to ships by third parties requiring a connection to one or more computers on board can also result in connecting the ship to shore. It is common for technicians, vendors, port officials, marine terminal representatives, agents, pilots, and other technicians to board the ship and plug in devices, such as laptops and tablets. Some technicians may require the use of removable media to update computers, download data and/or perform other tasks. It has also been known for customs officials and port state control officers to board a ship and request the use of a computer to “print official documents” after first inserting an unknown removable media.

Some IT and OT systems are remotely accessible and may operate with a continuous internet connection for remote monitoring, data collection, maintenance functions, safety and security. These systems can be “third-party systems”, whereby the contractor monitors and maintains the systems from a remote access. These systems could include both two-way data flow and upload-only. Systems and work stations with remote control, access or configuration functions could, for example, be:

(a) bridge and engine room computers and work stations on the ship's administrative network;

(b) cargo such as containers with reefer temperature control systems or specialised cargo that are tracked remotely;

(c) stability decision support systems;

(d) hull stress monitoring systems;

(e) navigational systems including Electronic Navigation Chart (ENC) Voyage Data Recorder (VDR), dynamic positioning (DP);

(f) cargo handling, engine, and cargo management systems;

(g) safety and security networks, such as CCTV (closed circuit television);

[6] Lloyd’s Register, Qinetiq and University of Southampton, Global Marine Technology Trends 2030.

(h) specialised systems such as drilling operations, blow out preventers, subsea installation systems, Emergency Shut Down (ESD) for gas tankers, submarine cable installation and repair.

The extent and nature of connectivity of equipment should be known by the shipowner or operator and documented as part of the risk assessment.

5.1.4 Impact assessement

The confidentiality, integrity and availability (CIA) model[7] provides a framework for assessing the impact of:

(a) unauthorised access to and disclosure of information or data about the ship, crew, cargo and passengers;

(b) loss of integrity, which would modify or destroy information and data relating to the safe and efficient operation and administration of the ship;

(c) loss of availability due to the destruction of the information and data and/or the disruption to services/ operation of ship systems.

The relative importance of confidentiality, integrity and availability (CIA) changes depending on the use of the information or data. For example, assessing the vulnerability of IT systems related to commercial operations may focus on confidentiality and integrity rather than availability. Conversely, assessing the vulnerability of OT systems onboard ships, particularly safety critical systems, may focus on availability and/or integrity instead of confidentiality.

[7] Federal Information Processing Standards, Publication 199, Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900.

Table 2 Potential impact levels when using the CIA model

Potential impact	Definition	In practice
Low	The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on company and ship, organizational assets, or individuals	A **limited** adverse effect means that a security breach might: (i) cause a degradation in ship operation to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The loss of confidentiality, integrity, or availability could be expected to have a **substantial** adverse effect on company and ship, company and ship assets, or individuals	A **substantial** adverse effect means that a security breach might: (i) cause a significant degradation in ship operation to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
High	The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on company and ship operations, company and ship assets, or individuals.	A **severe or catastrophic** adverse effect means that a security breach might: (i) cause a severe degradation in or loss of ship operation to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life- threatening injuries.

Sensitive information may include ship position, status of and readout from OT systems, cargo details, authorisations, certificates, etc. When it comes to OT systems it is important consider what impact the loss or malfunction of the system will have following a cyber incident.

5.1.5 Example

(a) Identify critical systems:

A power management system contains a supervisory control and data acquisition (SCADA) system controlling the distribution of onboard electric power. The system contains real-time sensor data which is used on board for power management. It also generates data about the power consumption, which is used by the shipping company for administrative purposes.

To determine if the information above is critical, the consequences likely to result from a compromise to the confidentiality, integrity or availability should be considered. When doing so the shipping company should determine the criticality of the information stored, processed or transmitted by the SCADA system using the most sensitive information to determine the overall impact of the system.

(b) Determine consequence:

As this OT system is using several measuring points and is integrated with other systems, the company decide to consider the effect of an operational malfunction or loss of the SCADA system due to a cyber incident. In this case, the company concludes that this will have a severe effect and thereby a high impact to the operation of the ship.

(c) Determine likelihood:

Using the confidentiality, integrity and availability (CIA) model, the shipping company can also conclude that:

(i) losing confidentiality of the sensor data acquired by the SCADA system will have a low impact as the sensors are publicly displayed on board. However, from a safety point of view, it is important that the information transmitted by the sensors can be relied upon therefore there is a high potential impact from a loss of integrity. It will also be a safety issue if the information cannot be read, and there is therefore a high potential impact from a loss of availability.

(ii) for the power consumption information being sent to the shipping company for statistical purposes, it is assessed that there is a low potential impact from a loss of confidentiality. The company does not want the data to be public, however the effect would be limited if it were to happen. There will also be a low potential impact from a loss of integrity as the data is only used for in-house considerations. There is therefore also a low potential impact from a loss of availability.

(d) Determine cyber security risks impact:

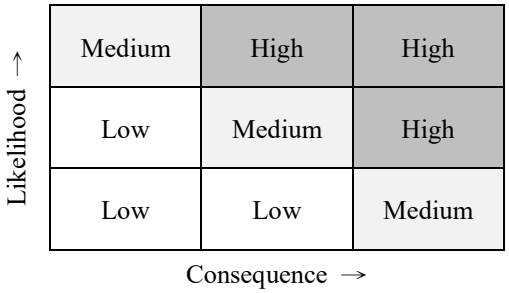
The following table shows the result of the assessment:

Table 3 Result of CIA assessment of SCADA system

SCADA system	Confidentiality	Integrity	Availability	Overall impact
Sensor data	Low	High	High	High
Statistical data	Low	Low	Low	Low

(e) Establishing the prioritised action plan:

Risk value = Assets value (impact, consequence) x Threats likelihood x Difficulty of use of vulnerabilities
Assets value = confidentiality + integrity + availability, and the impact and consequence of loss of assets



5.1.6 Bring your own device (BYOD)

It is recognised that personnel may be allowed to bring their own devices (BYOD) on board to access the ships' system or network. Although this may be both beneficial and economical for ships, because these devices may be unmanaged, it significantly increases the possibility of vulnerabilities being exposed. Policies and procedures should address their control, use, and how to protect vulnerable data, such as through network segregation.

5.2 Risk Assessment Made by the Company

5.2.1 As mentioned above, the risk assessment process starts by assessing the systems on board, in order to map their robustness to handle the current level of cyber threats. Elements of a ship security assessment[8] can be used when performing the risk assessment, which should physically test and assess the IT and OT systems on board including:

[8] The assessment described is based on regulation 8 of the ISPS Code.

(a) identification of existing technical and procedural controls to protect the onboard IT and OT systems (more information can be found with the Critical Security Controls[9]);

(b) identification of IT and OT systems that are vulnerable including human factors, and the policies and procedures governing the use of these systems (the identification should include searches for known vulnerabilities relevant to the equipment, the current level of patching and firmware updates)

(c) identification and evaluation of key ship board operations that are vulnerable to cyber attacks;

(d) identification of possible cyber incidents and their impact on key ship board operations, and the likelihood of their occurrence to establish and prioritise protection measures.

5.2.2 Companies may consult with the producers and service providers of onboard equipment and systems to understand the technical and procedural controls that may already be in place to address cyber security. Furthermore, any identified cyber vulnerability in the factory standard configuration of a critical system or component should be disclosed to facilitate better protection of the equipment in the future.

5.3 Third-Party Risk Assessments

Self-assessments can serve as a good start, but may be complemented by third-party risk assessments to drill deeper, and identify the risks and the gaps that may not be found during the self-assessment. Penetration tests of critical IT and OT infrastructure can also be performed to identify whether the actual defence level matches the desired level set forth in the cyber security strategy for the company. Such tests can be performed by external experts simulating attacks using both IT-systems, social engineering and, if desired, even physical penetration of a facility's security perimeter. These tests are referred to as active tests because they involve accessing and inserting software into a system. This may only be appropriate for IT systems. Where risk to OT systems during penetration testing is unacceptable, passive testing approaches should be considered. Passive methods rely on scanning data transmitted by a system to identify vulnerabilities. In general, no attempt is made to actively access or insert software into the system.

5.4 Risk Assessment Process

5.4.1 Phase 1: Pre-assessment activities

Prior to starting a cyber security assessment on board[10], the following activities should be performed:

(a) map the ship's key functions and systems and their potential impact levels, for example using the CIA model, taking into consideration the operation of OT systems;

(b) identify main producers of critical shipboard IT and OT equipment;

(c) review detailed documentation of critical OT and IT systems including their network architecture, interfaces and interconnections;

(d) identify cyber security points-of-contact at each of the producers and establish working relationships with them;

[9] www.cisecurity.org/critical-controls.cfm.

[10] Based on a third-party risk assessment method described by NCC Group.

(e) review detailed documentation on the ship's maintenance and support of its IT and OT systems;

(f) establish contractual requirements and obligations that the shipowner/ship operator may have for maintenance and support of shipboard networks and equipment;

(g) support, if necessary, the risk assessment with an external expert to develop detailed plans and include producers and service providers.

5.4.2 Phase 2: Ship assessment

The goal of the assessment of a ship's network and its systems and devices is to identify any vulnerabilities that could compromise or result in either loss of confidentiality, loss of integrity or result in a loss of operation of the equipment, system, network, or even the ship. These vulnerabilities and weaknesses could fall into one of the following categories:

(a) technical such as software defects or outdated or unpatched systems;

(b) design such as access management, unmanaged network interconnections;

(c) implementation errors for example misconfigured firewalls;

(d) procedural or other user errors.

The activities performed during an assessment would include reviewing the configuration of all computers, servers, routers, and cyber security technologies including firewalls. It should also include reviews of all available cyber security documentation and procedures for connected IT and OT systems and devices.

5.4.3 Phase 3: Debrief and vulnerability review/reporting

Following the assessment, each identified vulnerability should be evaluated for its potential impact and the probability of its exploitation. Recommended technical and/or procedural corrective actions should be identified for each vulnerability in a final report.

Ideally, the cyber security assessment report should include:

(a) executive summary – a high-level summary of results, recommendations and the overall security profile of the assessed environment, facility or ship;

(b) technical findings – a detailed, tabular breakdown of discovered vulnerabilities, their probability of exploitation, the resulting impact, and appropriate technical fix and mitigation advice;

(c) prioritised list of actions – the priorities allocated should reflect the effectiveness of the measure, the cost, the applicability, etc. It is important that this list does not represent a list of services and products the third-party risk assessor would like to sell, instead of being a complete list of options available;

(d) supplementary data – a supplement containing the technical details of all key findings and comprehensive analysis of critical flaws. This section should also include sample data recovered during the penetration testing of critical or high-risk vulnerabilities;

(e) appendices – detailed records of all activities conducted by the cyber security assessment team and the tools used during the engagement.

5.4.4 Phase 4: Producer debrief

Once the shipowner has had an opportunity to review, discuss and assess the findings, a subset of the findings may need to be sent to the producers of the affected systems. Any findings, which are approved by the shipowner for disclosure to the producers, could further be analysed with support from external experts, who should work with the producer's cyber security point of contact to ensure that a full risk and technical understanding of the problem is achieved. This supporting activity is intended to ensure that any remediation plan developed by the producer is comprehensive in nature and the correct solution to eliminate the vulnerabilities identified.

CHAPTER 6 DEVELOP PROTECTION AND DETECTION MEASURES

6.1 General

6.1.1 The outcome of the senior management's risk assessment and subsequent company's cyber security strategy should be a reduction in risk, if needed. At a technical level, this would include the necessary actions to be implemented to establish and maintain an agreed level of cyber security.

6.1.2 Special attention should be given when there has been no control over who has access to the onboard systems. This could, for example, happen during drydocking, layups or when taking over a new or existing ship. In such cases, it is difficult to know if malicious software has been left in the onboard systems. It is recommended that sensitive data is removed from the ship and reinstalled on returning to the ship. Where possible, systems should be scanned for malware before prior to use. OT systems should be tested to check that the functionalities are still intact.

6.1.3 It is critical to identify how to manage cyber security on board and to delegate responsibilities to the master, responsible officers and maybe the company security officer.

6.1.4 Cyber security protection measures may be technical and focused on ensuring that onboard systems are designed and configured to be resilient to cyber attacks. Protection measures may also be procedural and should be covered by company policies, safety management procedures, security procedures and access controls. Both technical and procedural controls should be compatible with the confidentiality, integrity and availability (CIA) model for protecting data and information.

6.1.5 It is recognised that technical cyber security controls may be more straightforward to implement on a new ship than on an existing ship. Consideration needs be given to only implement technical controls that are practical and cost effective, particularly on existing ships.

6.1.6 Consideration should be given in

(a) increased cost due to multiple technical controls and/or duplication;

(b) increased complexity to manage an ever increasing technology base;

(c) security can get in the way of the business; and

(d) maintenance is challenging.

Implementation of cyber security controls should be prioritised, focusing first on those measures, or combinations of measures, which offer the greatest benefit. Then expanded from basic to foundational and advanced, if applicable.

6.1.7 A wide range of options to enhance the technical aspects of cyber security exists and will often be employed by or in close cooperation with the providers of the respective critical system. Below 6.2 to 6.4 respectively introduce the widely used cyber security controls related measures and standards. Organizations may choose from, but not limited to these two measures according to their need.

6.2 CIS Technical Protection Measures

6.2.1 The Centre for Internet Security (CIS) provides guidance on measures[11] that can be used to address cyber security vulnerabilities. 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 companies to assess and improve their defences. The CSCs include both technical and procedural aspects. CSC Version 7 has 20 controls and 171 subcontrols. The subcontrols were noted as being foundational or advanced.

6.2.2 The below mentioned examples of CSCs have been selected as particularly relevant to equipment and data onboard ships[12].

(a) Limitation to and control of network ports, protocols and services

Access lists to network systems can be used to implement the company's security policy. This ensures that only appropriate traffic will be allowed via a controlled network or subnet, based on the control policy of that network or subnet.

It should be a requirement that routers are secured against attacks and unused ports should be closed to prevent unauthorised access to systems or data.

(b) Configuration of network devices such as firewalls, routers and switches

It should be determined which systems should be attached to controlled or uncontrolled[13] networks. Controlled networks are designed to prevent any security risks from connected devices by use of firewalls, security gateways, routers and switches. Uncontrolled networks may pose risks due to lack of data traffic control and they should be isolated from controlled networks, as direct internet connection makes them highly prone to infiltration by malware. For example:

(i) Networks that are critical to the operation of a ship itself, should be controlled. It is imperative that these systems - have a high level of security.

(ii) Networks that provide suppliers with remote access to navigation and other OT system software on onboard equipment, should also be controlled. These networks may be necessary for suppliers to allow upload of system upgrades or perform remote servicing. Shoreside external access points of such connections should be secured to prevent unauthorised access.

(iii) Other networks, such as guest access networks, may be uncontrolled, for instance those related to passenger recreational activities or private internet access for crew. Normally, any wireless network should be considered uncontrolled.

Onboard networks should be partitioned by firewalls to create safe zones. The fewer communications links and devices in a zone, the more secure the systems and data are in that zone. Confidential and safety critical systems should be in the most protected zone. See Annex 2 of the Guidelines for more information on shipboard networks and also refer to ISO/IEC 62443.

(c) Physical security

Security and safety critical equipment and cable runs should be protected from unauthorised access. Physical security is a central aspect of cyber security[14].

(d) Detection, blocking and alerts

---

11 CIS, Critical Security Controls for Effective Cyber Security, available at www.cisecurity.org/critical-controls.cfm.

12 Stephenson Harwood (2015), Cyber Risk.

13 In accordance with EC 61162-460:2015: Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 460: Multiple talkers and multiple listeners - Ethernet interconnection - Safety and security.

14 See also the ISPS Code.

Identifying intrusions and infections is a vital part of the controls. A baseline of network operations and expected data flows for users and systems should be established and managed so that cyber incident alert thresholds can be established. Key to this will be the definition of roles and responsibilities for detection to ensure accountability. Additionally, a company may choose to incorporate an Intrusion Detection System (IDS) system or an Intrusion Prevention System (IPS) into the network or as part of the firewall. Some of their main functions include identifying threats/malicious activity and code, and then logging, reporting and attempting to block the activity. Further details concerning IDS and IPS can be found in annex 2 of these guidelines. Ensure that dedicated onboard personnel can understand the alerts and their implications. Incidents detected should be directed to an individual or service provider, who is responsible for acting on this type of alert.

(e) Satellite and radio communication

Cyber security of the radio and satellite connection should be considered in collaboration with the service provider. In this connection, the specification of the satellite link should be considered when establishing the requirements for onboard network protection.

When establishing an uplink connection for ships' navigation and control systems to shore-based service providers, consideration should be given in how to prevent illegitimate connections gaining access to the onboard systems.

The access interconnect is the distribution partner's responsibility. The final routing of user traffic from the internet access point to its ultimate destination onboard (“last mile”) is the responsibility of the shipowner. User traffic is routed through the communication equipment for onward transmission on board. At the access point for this traffic, it is necessary to provide data security, firewalling and a dedicated “last-mile” connection.

When using a Virtual Private Network (VPN), the data traffic should be encrypted to an acceptable international standard. Furthermore, a firewall in front of the servers and computers connected to the networks (ashore or on board) should be deployed. The distribution partner should advise on the routing and type of connection most suited for specific traffic. Onshore filtering (inspection/blocking) of traffic is also a matter between a shipowner and the distribution partner. However, it is not sufficient to have either onshore filtering of traffic or firewalls/security inspection/blocking gateways on the ship, because both types are needed and supplement each other to achieve a sufficient level of protection.

Producers of satellite communication terminals and other communication equipment may provide management interfaces with security control software that are accessible over the network. This is primarily provided in the form of web-based user interfaces. Protection of such interfaces should be considered when assessing the security of a ship's installation.

(f) Wireless access control

It should be ensured that wireless access to networks on the ship is limited to appropriate authorised devices and secured using a strong encryption key, which is changed regularly.

(g) Malware detection

Scanning software that can automatically detect and address the presence of malware in systems onboard should be regularly updated.

As a general guideline, onboard computers should be protected to the same level as office computers ashore. Anti-virus and anti-malware software should be installed, maintained and updated on all personal work-related computers onboard. This will reduce the risk of these computers acting as attack vectors towards servers and other computers on the ship's network. The decision on whether to rely on these defence methods should take into consideration how regularly the scanning software will be able to be updated.

(h) Secure configuration for hardware and software

Only senior officers should be given administrator profiles so that they can control the set up and disabling of normal user profiles. User profiles should be restricted to only allow the computers, workstations or servers

to be used for the purposes for which they are required. User profiles should not allow the user to alter the systems or install and execute new programs.

(i) Email and web browser protection

Email communication between ship and shore is a vital part of a ship's operation. Appropriate email and web browser protection serves to:

(i) protect shoreside and onboard personnel from potential social engineering

(ii) prevent email being used as a method of obtaining sensitive information

(iii) ensure that the exchange of sensitive information via email or by voice is appropriately protected to ensure confidentiality and integrity of data, for example protecting by encryption

(iv) prevent web browsers and email clients from executing malicious scripts.

Some best practices for safe email transfer are: email as zip or encrypted file when necessary, disable hyperlinks on email system, and avoid using generic email addresses and ensure the system has configured user accounts.

(j) Data recovery capability

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. Essential information and software-adequate backup facilities should be available to ensure it can be recovered following a cyber incident.

Retention periods and restore scenarios should be established to prioritise which critical systems need quick restore capabilities to reduce the impact. Systems that have high data availability requirements should be made resilient. OT systems, which are vital to the safe navigation and operation of the ship, should have backup systems to enable the ship to quickly and safely regain navigational and operational capabilities after a cyber incident. More detail on recovery can be found in chapter 7 of the Guidelines.

(k) Application software security (patch management)

Critical safety and security updates should be provided to onboard systems. These updates or patches should be applied correctly and in a timely manner to ensure that any flaws in a system are addressed before they are exploited by a cyber attack.

6.3 ISO/IEC 27001

6.3.1 Many organisations find it worthwhile to establish an information security management system (ISMS) according to the international standard ISO/IEC 27001. The standard is fully aligned with recent editions of the other commonly used ISO management system standards, such as ISO 9001 and ISO 14001, allowing for easy integration of the ISMS into the wider scope of a company's integrated management system if so desired. At time of the Guidelines publishing, ISO/IEC 27001:2013 is the current edition of the standard. ISO/IEC 27001 requires continuous cyber security management, through implementing an information security management system (ISMS). The ISMS shall be established, implemented, maintained and continually improved in accordance with the requirements of ISO/IEC 27001, covering the organisation, responsibilities and management of IT & OT systems. The typical PDCA management system cycle also applies to the ISMS. The guidelines deals with the operational aspects of cyber security management, focusing on the ship in operation. The ISO/IEC 27001 approach complements the Guidelines' approach with an organisation-centric approach, putting much emphasis on planning, resources, and continuous improvement.

6.3.2 ISO/IEC 27001:2013 is divided into ten clauses and an annex; the management system controls (clause 4 to 10) and annexure controls (14 sections, 35 control objectives and 114 detail controls). Clauses 1 to 3 contain the scope of the standard, normative references, and a reference to ISO 27000 for terms and definitions. Clauses 4 to 10 contain the following requirements:

(a) Clause 4: Context of the organisation
- 4.1 Understanding the organisation and its context
- 4.2 Understanding the needs and expectations of interested parties
- 4.3 Determining the scope of the information security management system
- 4.4 Information security management system established

(b) Clause 5: Leadership
- 5.1 Leadership and commitment
- 5.2 Policy
- 5.3 Organisational roles, responsibilities and authorities

(c) Clause 6: Planning
- 6.1 Actions to address risks and opportunities
- 6.2 Information security objectives and planning to achieve them

(d) Clause 7: Support
- 7.1 Resources
- 7.2 Competence
- 7.3 Awareness
- 7.4 Communication
- 7.5 Documented Information

(e) Clause 8: Operation
- 8.1 Operational planning and control
- 8.2 Information security risk assessment
- 8.3 Information security risk treatment

(f) Clause 9: Performance evaluation
- 9.1 Monitoring, measurement, analysis and evaluation
- 9.2 Internal Audit
- 9.3 Management Review

(g) Clause 10: Improvement
- 10.1 Nonconformity and corrective action
- 10.2 Continual improvement

(h) Annex A (normative): Reference control objectives and controls

Lists in detail controls to be used for the main clauses of the standard. The organisation's controls must be checked against this list to ensure no necessary controls are overlooked.

The typical PDCA management system cycle

6.3.3 Overview of ISO 27001:2013 Annex A

Ref.	Section	Controls	Content
A.5	Information security policies	2	Management direction
A.6	Organization of information security	7	Internal organization, Mobile devices and teleworking
A.7	Human resource security	6	Prior to, during employment, termination and change of employment
A.8	Asset management	10	Responsibility for assets, information classification, media handling
A.9	Access Control	14	Business requirements, user access management and responsibilities, system and application access control
A.10	Cryptography	2	Cryptographic controls

A.11	Physical and environmental security	15	Secure areas, equipment
A.12	Operations security	14	Procedures and responsibilities, malware protection , backup process, Logging and monitoring, operational software, technical vulnerabilities, system audits
A.13	Communications security	7	Network security, Information transfer
A.14	System acquisition, development and maintenance	13	Security requirements, development and support, test data
A.15	Supplier relationships	5	Information security in supplier relationships, service delivery
A.16	Information security incident management	7	Management of information security incidents and improvements
A.17	Information security aspects of business continuity management	4	Continuity, redundancy
A.18	Compliance	8	Legal and contractual compliance, reviews

6.3.4 Mandatory documents corresponding to ISO 27001:2013

Mandatory documents	Check
Scope of the ISMS (clause 4.3)	
Information security policy and objectives (clauses 5.2 and 6.2)	
Risk assessment and risk treatment methodology (clause 6.1.2)	
Statement of Applicability (clause 6.1.3 d)	
Risk treatment plan (clauses 6.1.3 e and 6.2)	
Risk assessment report (clause 8.2)	
Definition of security roles and responsibilities (clauses A.7.1.2 and A.13.2.4)	
Inventory of assets (clause A.8.1.1)	
Acceptable use of assets (clause A.8.1.3)	
Access control policy (clause A.9.1.1)	
Operating procedures for IT/OT management (clause A.12.1.1)	
Secure system engineering principles (clause A.14.2.5)	
Supplier security policy (clause A.15.1.1)	
Incident management procedure (clause A.16.1.5)	
Business continuity procedures (clause A.17.1.2)	
Statutory, regulatory, and contractual requirements (clause A.18.1.1)	

6.3.5 Mandatory records corresponding to ISO 27001:2013

Mandatory records	Check
Records of training, skills, experience and qualifications (clause 7.2)	
Monitoring and measurement results (clause 9.1)	
Internal audit program (clause 9.2)	
Results of internal audits (clause 9.2)	
Results of the management review (clause 9.3)	
Results of corrective actions (clause 10.1)	
Logs of user activities, exceptions, and security events (clauses A.12.4.1 and A.12.4.3)	

6.3.6 Non-mandatory documents corresponding to ISO 27001:2013

Non-mandatory records	Check
Procedure for document control (clause 7.5)	
Controls for managing records (clause 7.5)	
Procedure for internal audit (clause 9.2)	

Procedure for corrective action (clause 10.1)	
Bring your own device (BYOD) policy (clause A.6.2.1)	
Mobile device and teleworking policy (clause A.6.2.1)	
Information classification policy (clauses A.8.2.1, A.8.2.2, and A.8.2.3)	
Password policy (clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, and A.9.4.3)	
Disposal and destruction policy (clauses A.8.3.2 and A.11.2.7)	
Procedures for working in secure areas (clause A.11.1.5)	
Clear desk and clear screen policy (clause A.11.2.9)	
Change management policy (clauses A.12.1.2 and A.14.2.4)	
Backup policy (clause A.12.3.1)	
Information transfer policy (clauses A.13.2.1, A.13.2.2, and A.13.2.3)	
Business impact analysis (clause A.17.1.1)	
Exercising and testing plan (clause A.17.1.3)	
Maintenance and review plan (clause A.17.1.3)	
Business continuity strategy (clause A.17.2.1)	

6.4 IACS Rec. No. 166

Refer to IACS announced publication of its Recommendation on Cyber Resilience (No. 166) which provides technical requirments for cyber resilient ships throughout their service lifes. See also 1.3.2(d).

6.5 Procedural Protection Measures

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:

6.5.1 Training and awareness

Training and awareness is the key supporting element to an effective approach to cyber safety and security as described in these guidelines and summarised in 2.3.

The internal cyber threat is considerable and should not be underestimated. Personnel have a key role in protecting IT and OT systems but can also be careless, for example by using removable media to transfer data between systems without taking precautions against the transfer of malware. Training and awareness should be tailored to the appropriate levels for:

- onboard personnel including the master, officers and crew;
- shoreside personnel, who support the management and operation of the ship.

The guidelines assume that other major stakeholders in the supply chain, such as charterers, classification societies and service providers, will carry out their own best-practice cyber security protection and training. It is advised that owners and operators ascertain the status of cyber security preparedness of their third-party providers as part of their sourcing procedures for such services.

An awareness programme should be in place for all onboard personnel, covering at least the following:

- risks related to emails and how to behave in a safe manner (examples are phishing attacks where the user clicks on a link to a malicious site);

- risks related to internet usage, including social media, chat forums and cloud-based file storage where data movement is less controlled and monitored;
- risks related to the use of own devices (these devices may be missing security patches and controls, such as anti-virus, and may transfer the risk to the environment to which they are connected);
- risks related to installing and maintaining software on company hardware using infected hardware (removable media) or software (infected package);
- risks related to poor software and data security practices where no anti-virus checks or authenticity verifications are performed;
- safeguarding user information, passwords and digital certificates;
- cyber risks in relation to the physical presence of non-company personnel, eg, where third-party technicians are left to work on equipment without supervision;
- detecting suspicious activity or devices and how to report if a possible cyber incident is in progress (examples of this are strange connections that are not normally seen or someone plugging in an unknown device on the ship network);
- awareness of the consequences or impact of cyber incidents to the safety and operations of the ship;
- understanding how to implement preventative maintenance routines such as anti-virus and anti-malware, patching, backups, and incident-response planning and testing;
- procedures for protection against risks from service providers' removable media before connecting to the ship's systems.

In addition, personnel need to be made aware that the presence of anti-malware software does not remove the requirement for robust security procedures, for example controlling the use of all removable media.

Further, applicable personnel should know the signs when a computer has been compromised. This may include the following:

- an unresponsive or slow to respond system;
- unexpected password changes or authorised users being locked out of a system;
- unexpected errors in programs, including failure to run correctly or programs running unexpectedly;
- unexpected or sudden changes in available disk space or memory;
- emails being returned unexpectedly;
- unexpected network connectivity difficulties;

- frequent system crashes;
- abnormal hard drive or processor activity;
- unexpected changes to browser, software or user settings, including permissions.

And, nominated personnel should be able to understand reports from IDS systems, if used. This list is not comprehensive and is intended to raise awareness of potential signs, which should be treated as possible cyber incidents.

6.5.2 Access for visitors

Visitors such as authorities, technicians, agents, port officials, and owner representatives should be restricted with regard to computer access whilst on board. Unauthorised access to sensitive OT network computers should be prohibited through clearly marked physical barriers. If access to a network by a visitor is required and allowed, then it should be restricted in terms of user privileges. Access to certain networks for maintenance reasons should be approved and co-ordinated following appropriate procedures as outlined by the company/ship operator.

If a visitor requires computer and printer access, an independent computer, which is air-gapped from all controlled networks, should be used. To avoid unauthorised access, removable media blockers should be used on all other physically accessible computers and network ports.

6.5.3 Upgrades and software maintenance

Hardware or software that is no longer supported by its producer or software developer will not receive updates to address potential vulnerabilities. For this reason, the use of hardware and software, which is no longer supported, should be carefully evaluated by the company as part of the cyber risk assessment.

Relevant hardware and software installations on board should be updated to maintain a sufficient security level. Procedures for timely updating of software may need to be put in place taking into account the ship type, speed of internet connectivity, sea time, etc. Software includes computer operating systems, which should also be kept up to date.

Additionally, a number of routers, switches and firewalls, and various OT devices will be running their own firmware, which may require regular updates and so should be addressed in the procedural requirements.

Effective maintenance of software depends on the identification, planning and execution of measures necessary to support maintenance activities throughout the full software lifecycle. An industry standard[15] to ensure safe and secure software maintenance has been developed. It specifies requirements for all stakeholders involved in software maintenance of shipboard equipment and associated integrated systems. The standard covers on board, on shore and remote software maintenance.

6.5.4 Anti-virus and anti-malware tool updates

In order for scanning software tools to detect and deal with malware, they need to be updated. Procedural requirements should be established to ensure updates are distributed to ships on a timely basis and that all relevant computers on board are updated.

6.5.5 Remote access

Policy and procedures should be established for control over remote access to onboard IT and OT systems. Clear guidelines should establish who has permission to access, when they can access, and what they can access. Any procedures for remote access should include close co-ordination with the ship's master and other key senior ship personnel.

All remote access occurrences should be recorded for review in case of a disruption to an IT or OT system. Systems, which require remote access, should be clearly defined, monitored and reviewed periodically.

[15] See: Industry standard on software maintenance of shipboard equipment by BIMCO and CIRM (Comité International Radio-Maritime).

6.5.6 Use of administrator privileges

Access to information should only be allowed to relevant authorised personnel.

Administrator privileges allow full access to system configuration settings and all data. Users logging into systems with administrator privileges may enable existing vulnerabilities to be more easily exploited. Administrator privileges should only be given to appropriately trained personnel who have a need, as part of their role in the company or on board, to log into systems using these privileges. In any case, use of administrator privileges should always be limited to functions requiring such access.

User privileges should be removed when the people concerned are no longer on board. User accounts should not be passed on from one user to the next using generic usernames. Similar rules should be applied to any onshore personnel with remote access to systems on ships when they change role and no longer need access.

In a business environment, such as shipping, access to onboard systems is granted to various stakeholders. Suppliers and contractors are a risk because they often have both intimate knowledge of a ship's operations and often full access to systems.

To protect access to confidential data and safety critical systems, a robust password policy should be developed[16]. Passwords should be strong and changed periodically. The company policy should address the fact that over-complicated passwords, which must be changed too frequently, are at risk of being written on a piece of paper and kept near the computer.

6.5.7 Physical and removable media controls

Transferring data from uncontrolled systems to controlled systems represents a major risk of introducing malware. Removable media can be used to bypass layers of defences and can be used to attack systems that are otherwise not connected to the internet. A clear policy for the use of such media devices is essential; it must ensure that media devices are not normally used to transfer information between un-controlled and controlled systems.

There are, however, situations where it is unavoidable to use these media devices, for example during software maintenance. In such cases, there should be a procedure in place to require checking of removable media for malware and/or validating legitimate software by digital signatures and watermarks.

Policies and procedures relating to the use of removable media should include a requirement to scan any removable media device in a computer that is not connected to the ship's controlled networks. If it is not possible to scan the removable media on board, eg the laptop of a maintenance technician, then the scan could be done prior to boarding with the result and timing duly documented. Companies should consider notifying ports and terminals about the requirement to scan removable media prior to permitting the uploading of files onto a ship's system. This scanning should be carried out when transferring the following file types:

(a) cargo files and loading plans eg container ship BAPLIE files;

(b) national, customs, and port authority forms;

(c) bunkering and lubrication oil forms;

(d) ship's stores and provisions lists;

(e) engineering maintenance files.

This list represents examples and should not be seen as exhaustive.

6.5.8 Equipment disposal, including data destruction

[16] More information can be found in NIST publication SP 800-63-3 Digital Identity Guidelines.

Obsolete equipment can contain data which is commercially sensitive or confidential. The company should have a procedure in place to ensure that the data held in obsolete equipment is properly destroyed prior to disposing of the equipment, ensuring that vital information cannot be retrieved.

6.5.9 Obtaining support from ashore and contingency plans

Ships should have access to technical support in the event of a cyber attack. Details of this support and associated procedures should be available on board. Please refer to Chapter 6 of these guidelines for more information about contingency planning.

CHAPTER 7 ESTABLISH CONTINGENCY PLANS

7.1 Attention of Developing The Plan

7.1.1 When developing contingency plans for implementation onboard ships, it is important to understand the significance of any cyber incident, particularly for IT and OT systems and prioritise response actions accordingly.

7.1.2 Any cyber incident should be assessed in accordance with the CIA model (see chapter 5) 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. In the event of a cyber incident affecting IT systems only, the priority may be the immediate implementation of an investigation and recovery plan.

7.1.3 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 and protection of the marine environment. In general, appropriate contingency plans for cyber incidents, including the loss of critical systems and the need to use alternative modes of operation, should be addressed by appropriate operational and emergency procedures included in the safety management system. Some of the existing procedures in the ship's safety management system will already cover such cyber incidents.

7.1.4 The safety management system will already include procedures for reporting accidents or hazardous situations and define levels of communication and authority for decision making. Where appropriate, such procedures should be amended to reflect communication and authority in the event of a cyber incident.

7.1.5 The following is a non-exhaustive list of the actions in response to the type of cyber incidents, which should be addressed in contingency plans on board:

(a) loss of availability of electronic navigational equipment or loss of integrity of navigation related data;

(b) loss of availability or integrity of external data sources, including but not limited to GNSS

(c) loss of essential connectivity with the shore, including but not limited to the availability of Global Maritime Distress and Safety System (GMDSS) communications

(d) loss of availability of industrial control systems, including propulsion, auxiliary systems and other critical systems, as well as loss of integrity of data management and control

(e) the event of a ransomware or denial or service incident.

7.1.6 It is important that onboard personnel understand that the loss of OT systems due to a cyber incident must be treated like any other equipment failure. Furthermore, it is important to ensure that a loss of equipment or reliable information due to a cyber incident does not make existing emergency plans and procedures redundant. It is crucial that contingency plans, and related information, are available in a non-electronic form as some types of cyber incidents can include the deletion of data and shutdown of communication links.

7.1.7 There may be occasions when responding to a cyber incident may be beyond the competencies on board or at head office due to the complexity or severity of such incidents. In these cases, external expert assistance may be required (for example post event forensic analysis and clean-up).

CHAPTER 8

RESPOND TO AND RECOVER FROM CYBER SECURITY INCIDENTS

8.1 General

It is important to understand that cyber incidents may not disappear by themselves. If for example the ECDIS has been infected with malware, starting up the back-up ECDIS may cause another cyber incident. It is, therefore, recommended to plan how to carry out the cleaning and restoring of infected systems.

Knowledge about previous identified cyber incidents should be used to improve the response plans of all ships in the company's fleet and an information strategy for such incidents may be considered.

8.2 Effective Response

8.2.1 A team, which may include a combination of onboard and shore-based personnel and/or external experts, should be established to take the appropriate action to restore the IT and/or OT systems so that the ship can resume normal operations. The team should be capable of performing all aspects of the response.

8.2.2 An effective response should at least consist of the following steps:

(a) Initial assessment: To ensure an appropriate response, it is essential that the response team find out:
  (i) how the incident occurred;
  (ii) which IT and/or OT systems were affected and how;
  (iii) the extent to which the commercial and/or operational data is affected;
  (iv) to what extent any threat to IT and OT remains.

(b) 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. The content of a recovery plan is covered in 8.3.

(c) 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. Investigations into cyber incidents are covered in 8.4.

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

8.2.3 When a cyber incident is complex, for example if IT and/or OT systems cannot be returned to normal operation, it may be necessary to initiate the recovery plan alongside onboard contingency plans. When this is the case, the response team should be able to provide advice to the ship on:

(a) whether IT or OT systems should be shut down or kept running to protect data

(b) whether certain ship communication links with the shore should be shut down

(c) the appropriate use of any advanced tools provided in pre-installed security software

(d) the extent to which the incident has compromised IT or OT systems beyond the capabilities of existing recovery plans.

8.3 Recovery Plan

8.3.1 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 ensure the safety of onboard personnel, the operation and navigation of the ship should be prioritised in the plan. The recovery plan should be understood by personnel responsible for cyber security. The detail and complexity of a recovery plan will depend on the type of ship and the IT, OT and other systems installed on board.

8.3.2 As explained in section 6.2, a data recovery capability is a valuable technical protection measure. Data recovery capabilities are normally in the form of software backup for IT data. The availability of a software backup, either on board or ashore, should enable recovery of IT to an operational condition following a cyber incident.

8.3.3 Recovery of OT may be more complex especially if there are no backup systems available and recovery may involve 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.

8.3.4 If qualified personnel are available on board, more extensive diagnostic and recovery actions may be performed. Otherwise, the recovery plan will be limited to obtaining quick access to technical support.

8.4 Investigating Cyber Incidents

8.4.1 Investigating a cyber incident can provide valuable information about the way in which a vulnerability was exploited. Companies should, wherever possible, investigate cyber incidents affecting IT and OT on board in accordance with company procedures. A detailed investigation may require external expert support.

8.4.2 The information from an investigation can be used to improve the technical and procedural protection measures on board and ashore. It will also provide the wider maritime industry with a better understanding of maritime cyber risks. Any investigation should result in[17]:

(a) a better understanding of the potential cyber risks facing the maritime industry both on board and ashore;

(b) identification of lessons learned, including improvements in training to increase awareness;

(c) updates to technical and procedural protection measures to prevent a recurrence.

[17] Based on CREST, Cyber Security Incident Response Guide, Version 1.

8.5 Losses Arising From a Cyber Incident

8.5.1 Insurance issue

For insurers, the term “cyber” includes many different aspects and it is important to distinguish between them and their effects on insurance cover. Also, it is important to note that according to the general understanding of insurers, there is no systemic risk to ships arising from a cyber incident and the impact of an incident is expected to be most likely confined to a single ship.

Companies will be aware that specific non-marine insurance cover may be available to cover data loss and the resulting fines and penalties resulting from equipment failure.

Companies should be able to demonstrate that they are acting with reasonable care in their approach to managing cyber risk and protecting the ship from any damage that may arise from a cyber incident.

8.5.2 Cover for property damage

Generally, in many markets offering marine property insurance, the policy may cover loss or damage to the ship and its equipment caused by a shipping incident such as grounding, collision, fire or flood, even when the underlying cause of the incident is a cyber incident. It may be noted that currently in some markets exclusion clauses for cyber attacks exist. If the marine policy contains an exclusion clause for cyber attacks, the loss or damage will not be covered.

Companies are recommended to check with their insurers / brokers in advance whether their policy covers claims caused by cyber incidents and/or by cyber attacks.

Guidelines for the market have been published, in which marine insurers are recommended to ask questions about company cyber security awareness and non-technical procedures. Companies should, therefore, expect a request for non-technical information regarding their approach to cyber security from insurers.

The limited data on the frequency, severity of loss or probability of physical damage resulting from a cyber incident, represents a challenge and means that standard pricing is not available.

8.5.3 Cover for liability

It is recommended to contact the P&I (Protection and Indemnity) Club for detailed information about cover provided to shipowners and charterers in respect of liability to third parties (and related expenses) arising from the operation of ships.

An incident caused, for example by malfunction of a ship's navigation or mechanical systems because of a criminal act or accidental cyber attack, does not in itself give rise to any exclusion of normal P&I cover.

It should be noted that many losses, which could arise from a cyber incident are not in the nature of third-party liabilities arising from the operation of the ship. For example, financial loss caused by ransomware, or costs of rebuilding scrambled data would not be identified in the coverage.

Normal cover, in respect of liabilities, is subject to a war risk exclusion and cyber incidents in the context of a war or terror risk, will not normally be covered.

CHAPTER 9 AUDIT

9.1 Type of Audit

The types of audit for registeration and maintenance of class notation "**Cyber-S**" are specified in the following 9.1.1 to 9.1.3:

9.1.1 Initial Audit (refer to 9.3)

9.1.2 Renewal Audit (hereinafter referred to as “Periodical Audit”)

9.1.3 Annual Audit (hereinafter referred to as “Periodical Audit”)

9.1.4 Occasional Audit

9.2 Timing of Audits

Audits are to be carried out in accordance with the following requirements given in 9.2.1 and 9.2.2.

9.2.1 Initial audits are to be carried out at the time an application for registration of "**Cyber-S**" notation is made.

9.2.2 Periodical audits are to be carried out in (a) through (c) below.
However, periodical audits may be omitted for ships where cyber security measures of the ship are effectively implemented, managed and maintained in accordance with requirements set out in other guidelines or standards, etc. considered as equivalent by the Society.

(a) Renewal Audits are to be carried out within 3 months prior to the due date of Special Survey as specified in 1.6.4 of Part I of the Rules for Steel Ship.

(b) Annual Audits are to be carried out at the intervals specified in 1.6.5(a) of Part I of the Rules for Steel Ships

(c) Occasional Audits are to be carried out at a timing when any of (i) to (iii) mentioned below takes place but does not fall within the schedules of Renewal Audits or Annual Audits.
  (i) In case where any computer based system has been damaged, repaired or renewed.
  (ii) In case where any computer based system is modified or altered.
  (iii) In case where considered necessary by the Society.

9.3 Initial Audit

An owner who intends to apply "**Cyber-S**" notation is to conduct a meeting upon building contract in which a tripartite agreement is to be made amongst owner, builder and class that the owner is to define the scope of computer based systems to which the Guidelines applies and provide information necessary for the inventory by the time of the defined date in the contract.

9.3.1 Drawing and data

Before the integrator designs detailed sytems and networks, following plans and documents are to be submitted to the Society for approval, if applicable.

(a) Inventory of onboard systems as specified in 4.2.

(b) Onboard networks (refer to Annex 2).

(c) Ship to shore interface as specified in 4.3.

(d) Company plans and procedures for cyber risk management as specified in 2.2.

(e) The results of identifing threats and vulnerabilities as specified in Chapter 3 and Chapter 4.

(f) Risk assessment report as specified in Chapter 5.

(g) Protection and detection measures as specified in Chapter 6.

(h) Established contingency plans as specified in Chapter 7.

(i) Recovery plan as specified in Chapter 8.

Upon approval of the above drawings and documents by the Society, the integrator is to develop the following plans and documents which are to be submittes for approval by the Society.

(j) Cyber security testing plans

The timing and the method of testings on cyber security features should be planned and implemented.

(g) Documents governing remote access (control procedures etc.), where the ship has remote access capabilities.

9.3.2 Testing after installation onboard

(a) The attending auditor confirms on board the ship that the measures to control the identified risks submitted by the integrator has been fully and effectively implemented onboard.

(b) Security tests is to be carried out with the attendance of the auditor. If it is difficult for the auditors to attend the security tests, they can be replaced by submission of test reports issued by a testing company with sufficient capabilities and experiences.

9.3.3 Documents to be maintained onboard

At the completion of an initial audit, the drawing and data specified in 9.3.1 should be maintained and properly managed onboard.

9.4 Renewal Audit

Following documents are to be submitted to the Society by the owner for renewal audits.

9.4.1 Results of security tests specified in 9.3.1(j)

9.4.2 Documents which indicates that the documents specified in 9.3.1 are properly maintained and managed

9.5 Annual Audit

Following documents are to be submitted to the Society by the owner for annual audits.

9.5.1 Documentation which indicates that the documents specified in 9.3.1 are properly maintained and maintained

9.6 Occasional Audits

Where an occasional audit is found necessary, the owner or the management company is to submit documents required by the Society for the examination.

ANNEX 1 TARGET SYSTEMS, EQUIPMENT AND TECHNOLOGIES

This annex provides a summary of potentially vulnerable systems and data onboard ships to assist companies with assessing their cyber risk exposure. Vulnerable systems, equipment and technologies may include:

A1.1 Communication Systems

A1.1.1 Integrated communication systems

A1.1.2 Satellite communication equipment

A1.1.3 Voice Over Internet Protocols (VOIP) equipment

A1.1.4 Wireless networks (WLANs)

A1.1.5 Public address and general alarm systems.

A1.2 Bridge Systems

A1.2.1 Integrated navigation system

A1.2.2 Positioning systems (GPS, etc.)

A1.2.3 Electronic Chart Display Information System (ECDIS)

A1.2.4 Dynamic Positioning (DP) systems

A1.2.5 Systems that interface with electronic navigation systems and propulsion/manoeuvring systems

A1.2.6 Automatic Identification System (AIS)

A1.2.7 Global Maritime Distress and Safety System (GMDSS)

A1.2.8 Radar equipment

A1.2.9 Voyage Data Recorders (VDRs)

A1.2.10 Other monitoring and data collection systems.

A1.3 Propulsion and Machinery Management and Power Control Systems

A1.3.1 Engine governor

A1.3.2 Power management

A1.3.3 Integrated control system

A1.3.4 Alarm system

A1.3.5 Emergency response system.

A1.4 Access Control Systems

A1.4.1 Surveillance systems such as CCTV network

A1.4.2 Bridge Navigational Watch Alarm System (BNWAS)

A1.4.3 Shipboard Security Alarm Systems (SSAS)

A1.4.4 Electronic “personnel-on-board” systems.

A1.5 Cargo Management Systems

A1.5.1 Cargo Control Room (CCR) and its equipment

A1.5.2 Level indication system

A1.5.3 Valve remote control system

A1.5.4 Ballast water systems

A1.5.5 Water ingress alarm system.

A1.6 Passenger Servicing and Management Systems

A1.6.1 Property Management System (PMS)

A1.6.2 Electronic health records

A1.6.3 Financial related systems

A1.6.4 Ship passenger/seafarer boarding access systems

A1.6.5 Infrastructure support systems like domain naming system (DNS) and user authentication/authorisation systems.

A1.7 Passenger-Facing Networks

A1.7.1 Passenger Wi-Fi or LAN internet access

A1.7.2 Guest entertainment systems

A1.7.3 Passenger Wi-Fi or Local Area Network (LAN) internet access, for example where onboard personnel can connect their own devices[18].

A1.7.4 Guest entertainment systems.

A1.8 Core infrastructure systems

A1.8.1 Security gateways

A1.8.2 Routers

A1.8.3 Switches

A1.8.4 Firewalls

A1.8.5 Virtual Private Network(s) (VPN)

A1.8.6 Virtual LAN(s) (VLAN)

A1.8.7 Intrusion prevention systems

A1.8.8 Security event logging systems.

A1.9 Administrative and Crew Welfare Systems

A1.9.1 Administrative systems

A1.9.2 Crew Wi-Fi or LAN internet access, for example where onboard personnel can connect their own devices.

[18] This is not considered as Bring Your Own Device (BYOD). Devices are not used to access protected information. They can only be used for an individual's personal, non-company, use.

ANNEX 2 ONBOARD NETWORKS

A secure network depends on the IT/OT set up onboard 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 security 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.

Direct communication between an uncontrolled and a controlled network should be prevented. Furthermore, several protection measures should be added:

(a) implement network separation and/or traffic management

(b) manage encryption protocols to ensure correct level of privacy and commercial communication

(c) manage use of certificates to verify origin of digitally signed documents, software or services.

In general, only equipment or systems that need to communicate with each other over the network should be able to do so. The overriding principle should be that the networking of equipment or systems is determined by operational need.

A2.1 Physical Layout

The physical layout of the network should be carefully considered. It is important to consider the physical location of essential network devices, including servers, switches, firewalls and cabling. This will help restrict access and maintain the physical security of the network installation and control of entry points to the network.

A2.2 Network Management

Any network design will need to include an infrastructure for administering and managing the network. This may include installing network management software on dedicated workstations and servers providing file sharing, email and other services to the network.

A2.3 Network Segmentation

Onboard networks should normally accommodate the following:

(a) necessary communication between OT equipment

(b) configuration and monitoring of OT equipment

(c) onboard administrative and business tasks including email and sharing business related files or folders

(d) recreational internet access for crew and/or passengers.

Effective network segmentation is a key aspect of "defence in depth". OT, IT and public networks should be separated or segmented by appropriate protection measures. The protection measures used may include, but are not limited to an appropriate combination of the following:

(a) a perimeter firewall between the onboard network and the internet

(b) network switches between each network segment

(c) internal firewalls between each network segment

(d) Virtual Local Area Networks (VLAN) to host separate segments.

In addition, each segment should have its own range of Internet Protocol (IP) addresses. Network segmentation does not remove the need for systems within each segment to be configured with appropriate network access controls and software firewalls and malware detection.

For example, the network was segmented using a perimeter firewall, which supports three VLANs.

(a) The OT Network containing equipment and systems, that performs safety critical functions.

(b) The IT network containing equipment and systems, that performs administrative or business functions.

(c) A crew and guest network, providing uncontrolled internet access.

Considerations should be made on how to maximise the security of the switches themselves. To achieve the highest level of security, each network should use a different hardware switch. This will minimise the chance of an attacker jumping between networks due to misconfiguration or by acquiring access to the configuration of a switch.

A correctly configured and appropriate firewall is an essential element of the proper segmentation of a network installation. The onboard installation should be protected by at least a perimeter firewall to control traffic between the internet and the onboard network. To prevent any unintended communication taking place, the firewall should be configured by default to deny all communication. Based on this configuration, rules should be implemented. The rules should be designed to allow passage of data traffic that is essential for the intended operation of that network.

For example, if a specific endpoint receives updates from the internet, the rule should allow the specific endpoint to connect specifically to the server handling the specific update service. Enabling general internet access to a specified endpoint for updates is bad practice.

Uncontrolled networks like a crew or passenger network should not be allowed any communication with the controlled networks. The uncontrolled network should be considered as unsafe as the internet since the devices connecting to it are unmanaged, their security status (antivirus, updates, etc.) is unknown and their users could be acting maliciously, intentionally or unintentionally.

A2.4 Monitoring Data Activity

It is essential to monitor and manage systems to be aware of the networks' status and to detect any unauthorised data traffic. Logging should be implemented in the firewall and ideally in all network-attached devices so that in case of a

breach, the responsible person can trace back the source and methodology of the attack. This will help to secure the network from any similar attacks in the future.

A network Intrusion Detection System (IDS) or Intrusion Protection System (IPS) can alert the system administrator in real-time of any attacks to the network systems. The IDS and IPS inspect data traffic, entry points or both to identify known threats or to reject traffic, which does not comply with the security policy. An IPS should comply with the latest industry best practices and guidelines.

It is recommended to place a sensor on the internet-facing segment, because the public servers are a visible target to attackers. Another sensor should be placed behind the firewall, to monitor traffic between the internet and the internal network. An lDS/IPS sensor could also be placed by a remote-access segment, for instance a Virtual Private Network (VPN).

A2.5 Secure Running Environment

Normally referred to as a sandbox, a secure running environment provides additional protection against cyber threats by isolating executable software from the underlying operating system. This prevents unauthorised access to the operating systems, on which the software is running. The sandbox enables software to be run under a specific set of rules and this adds control over processes and computer resources. Therefore, the sandbox prevents malicious, malfunctioning or untrusted software from affecting the rest of the system.

ANNEX 3 CYBER RISK MANAGEMENT AND THE SAFETY MANAGEMENT SYSTEM

IMO Resolution MSC.428(98) makes clear that an approved SMS should take into account cyber risk management (CRM) when meeting the objectives and functional requirements of the ISM Code. The guidance provided in the Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3) provides high level recommendations regarding the elements of an appropriate approach to implementing cyber risk management. The guidance in this annex is designed to provide the minimum measures that all companies should consider implementing so as to address cyber risk management in an approved SMS.

A3.1 Identify[19]

A3.1.1 Roles and responsibilities[20]

Action	Remarks
ISM Code: 3.2 the Guidelines: 1.2 & Ch.2 Update the safety and environment protection policy to include reference to the risk posed by unmitigated cyber risks.	An updated safety and environment protection policy should demonstrate: ● a commitment to manage cyber risks as part of the overall approach to safety management (including safety culture) and protection of the environment ● an understanding that CRM has both safety and security aspects, but the emphasis is on managing the safety risks introduced by OT, IT and networks ● an understanding that without appropriate technical and procedural risk protection and control measures, OT is vulnerable to disruption affecting the safe operation of a ship and protection of the environment. Nothing in the updated policy should suggest that CRM is given any more or less attention than any other risks identified by the company.
ISM Code: 3.3 the Guidelines: 1.2 & Ch.2 Update the responsibility and authority information provided in the SMS to include appropriate allocation of responsibility and authority for cyber risk management (CRM).	In general, IT personnel should understand potential vulnerabilities in computer-based systems and know the appropriate technical and procedural protection measures to help ensure the availability and integrity of systems and data. Operational and technical personnel should generally understand the safety and environmental impacts of disruption to critical systems[21] onboard ships and are responsible for the SMS. Allocation of responsibility and authority may need to be updated to enable CRM. This should include: ● allocation of responsibilities and authorities which encourage cooperation between IT personnel (which may be provided by a third party) and the company's operational and technical personnel ● incorporating compliance with cyber risk management policies and procedures into the existing responsibility and authority of the Master.
ISM Code: 6.5 the Guidelines: 6.2 Using existing company procedures, identify any training which may be required to support the incorporation of cyber risk management into the SMS.	Cyber awareness training is not a mandatory requirement. Notwithstanding this, training is a protection and control measure that forms the basis of CRM. It helps to ensure that personnel understand how their actions will influence the effectiveness of the company's approach to CRM. Existing company procedures for identifying training requirements should be used to assess the benefits and need for: ● all company personnel to receive basic cyber awareness training in support of the company's CRM policies and procedures ● company personnel, who have been assigned CRM duties, to receive a type and level of cyber training appropriate to their responsibility and authority.

[19] Identify, Protect, Detect, Respond and Recover as described in the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3).

[20] Functional element from the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3).

[21] For the purpose of this annex, “critical systems” means the OT, IT, software and data the sudden operational failure or unavailability of which is identified by the company as having the potential to result in hazardous situations.

A3.1.2 Identify systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

Action	Remarks
ISM Code: 10.3 the Guidelines: Ch.4 & Ch.5 Using existing company procedures, identify equipment and technical systems (OT and IT) the sudden operational failure of which may result in hazardous situations.	An approved SMS will already identify the equipment and technical systems (including OT and IT), and capabilities, which may cause hazardous situations if they become unavailable or unreliable. The impacts should already have been documented in an approved SMS. However, an approved SMS, which incorporates CRM will also need to address data in the context of sudden operational failure. Loss of availability or integrity of data used by critical systems can have the same impact on safety and protection of the environment as the system becoming unavailable or unreliable for some other reason. Consequently, it is recommended that the list of equipment and technical systems, should be supplemented by a list of the data used by those systems and its source(s).

A3.2 Protect

A3.2.1 Implement risk control measures

Action	Remarks
ISM Code: 1.2.2.2 the Guidelines: Ch.6 & Annex 1 Assess all identified risks to ships, personnel and the environment and establish appropriate safeguards.	The full scope of risk control measures implemented by the company should be determined by a risk assessment, taking into account the information provided in these guidelines. As a baseline, the following measures should be considered before a risk assessment is undertaken. The baseline consists of the technical and procedural measures, which should be implemented in all companies to the extent appropriate. These measures are: ● Hardware inventory – Develop and maintain a register of all critical system hardware on board, including authorized and unauthorized devices on company controlled networks. The SMS should include procedures for maintaining this inventory throughout the operational life of the ship. ● Software inventory – Develop and maintain a register of all authorized and unauthorized software running on company-controlled hardware onboard, including version and update status. The SMS should be updated to include procedures for: ・ maintaining this inventory when hardware controlled by the company is replaced ・ maintaining this inventory when software controlled by the company is updated or changed ・ authorizing the installation of new or upgraded software on hardware controlled by the company ・ prevention of installation of unauthorized software, and deletion of such software if identified ・ software maintenance. ● Map data flows – Map data flows between critical systems and other equipment/technical systems on board and ashore, including those provided by third parties. Vulnerabilities identified during this process should be recorded and securely retained by the company. The SMS should be updated to include procedures for: ・ maintaining the map of data flows to reflect changes in hardware, software and/or connectivity ・ identifying and responding to vulnerabilities introduced when new data flows are created following the installation of new hardware ・ reviewing the need for connectivity between critical systems and other OT and IT systems. Such a review should be based on the principle that systems should only be connected where there is a need for the safe and efficient operation of the ship, or to enable planned maintenance ・ controlling the use of removable media, access points and the creation of ad-hoc or uncontrolled data flows. This may be achieved by restrictions on the use of removable media and disabling USB and similar ports on critical systems.

	● Implement secure configurations for all hardware controlled by the company – This should include documenting and maintaining commonly accepted security configuration standards for all authorized hardware and software. The SMS should include policies on the allocation and use of administrative privileges by ship and shore-based personnel, and third parties. However, it is not recommended that the details of secure configurations are included in the SMS. This information should be retained separately and securely by the company. ● Audit logs – Security logs should be maintained and periodically reviewed. Security logging should be enabled on all critical systems with this capability. The SMS should be updated to include procedures for: ・ policies and procedures for the maintenance of security logs and periodic review by competent personnel as part of the operational maintenance routine ・ procedures for the collation and retention of security logs by the company, if appropriate. ● Awareness and training – See line 3 above. ● Physical security – The physical security of the ship is enhanced by compliance with the security measures addressed in the ship security plan (SSP) required by the ISPS Code. Measures should be taken to restrict access and prevent unauthorized access to critical system network infrastructure onboard.

A3.2.2 Develop contingency plans

Action	Remarks
ISM Code: 7 the Guidelines: Ch.7 Update procedures, plans and instructions for key shipboard operations concerning the safety of the personnel, ship and protection of the environment which rely on OT.	An approved SMS should already address procedures, plans and instructions for key shipboard operations concerning the safety of the personnel, ship and protection of the environment. In general, these plans should be unaffected by the incorporation of CRM into the SMS. This is because the effect of the loss of availability of OT, or loss of integrity of the data used or provided by such systems, is the same as if the OT was unavailable or unreliable for some other reason. Notwithstanding this, consideration should be given to developing instructions on the actions to be taken if disruption to critical systems is suspected. This could include procedures for reverting to back-up or alternative arrangements as a precaution whilst any suspected disruption is investigated. Procedures for periodically checking the integrity of information provided by OT to operators should be considered for inclusion in operational maintenance routines.
ISM Code: 8.1 the Guidelines: Ch.7 Update emergency plans to include responses to cyber incidents.	An approved SMS should already address emergency plans for the disruption of critical systems required for the safe operation of ships and protection of the environment. In general, these plans should be unaffected by the incorporation of cyber risk management into safety management systems. This is because the effect of common shipboard emergencies should be independent of the root cause. For example, a fire may be caused by equipment malfunctioning because of a software failure or inappropriate maintenance or operation of the equipment. Notwithstanding the above, consideration should be given to the development of a cyber incident module in the integrated system of shipboard emergency plans for significant disruption to the availability of OT or the data used by them. The purpose of the module could be to provide information on the actions to be taken in the event of a simultaneous disruption to multiple OT systems required for the safe operation of the ship and protection of the environment. In this more complex situation, additional information on appropriate immediate actions to be taken in response may be necessary.

A3.3 Detect

A3.3.1 Develop and implement activities necessary to detect a cyber-event in a timely manner.

Action	Remarks
ISM Code: 9.1 the Guidelines: 2.4 & Ch.6 Update procedures for reporting non-conformities, accidents and hazardous situations to include reports relating to cyber incidents.	An approved SMS should already address procedures relating to non-conformities. When incorporating CRM into the SMS, company reporting requirements for non-conformities may need to be updated to include cyber related non-conformities. Examples of such non-conformities and cyber incidents: ● 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.

A3.4 Respond

A3.4.1 Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations and/or services impaired due to a cyber-event.

Action	Remarks
ISM Code: 3.3 the Guidelines: 8.2 Ensure that adequate resources and shore-based support are available to support the DPA in responding to the loss of critical systems.	An approved SMS should already be supported by adequate resources to support the DPA. However, the incorporation of CRM into the SMS should require that this resourcing includes appropriate IT expertise. This resource could come from within the company but may also be provided by a third party. In providing the adequate resources, the following should be considered: ● company or third party technical support should be familiar with onboard IT and OT infrastructure and systems ● any internal response team or external cyber emergency response team (CERT) should be available to provide timely support to the DPA ● provision of an alternative means of communication between the ship and the DPA, which should be able to function independently of all other shipboard systems, if and when the need arises ● internal audits should confirm that adequate resources, including third parties when appropriate, are available to provide support in a timely manner to support the DPA.
ISM Code: 9.2 the Guidelines: 8.2 Update procedures for implementing corrective actions to include cyber incidents and measures to prevent recurrence.	An approved SMS should already include procedures for responding to non-conformities. In general, these should not be affected by the incorporation of CRM in SMS. However, the procedures should help ensure that consideration of non-conformities and corrective actions involves the personnel with responsibility and authority for CRM. This should help ensure that corrective actions, including measures to prevent recurrence, are appropriate and effective.

ISM Code: 10.3 the Guidelines: 8.2 Update the specific measures aimed at promoting the reliability of OT.	An approved SMS should already include procedures for operational maintenance routines to promote the reliability of equipment on board. A SMS, which incorporates CRM, should outline procedures for: ● Software maintenance as a part of operational maintenance routines – Such procedures should ensure that application of software updates, including security patches, are applied and tested in a timely manner, by a competent person. ● Authorizing remote access, if necessary and appropriate, to critical systems for software or other maintenance tasks – This should include authorizing access in general (including verification that service providers have taken appropriate protective measures themselves) and for each specific remote access session. ● Preventing the application of software updates by service providers using uncontrolled or infected removable media. ● Periodic inspection of the information provided by critical systems to operators and confirmation of the accuracy of this information when critical systems are in a known state. ● Controlled use of administrator privileges to limit software maintenance tasks to competent personnel.

A3.5 Recovery

A3.5.1 Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber incident.

Action	Remarks
ISM Code: 10.4 the Guidelines: 2.4, Ch.6 & 8.3 Include creation and maintenance of back-ups into the ship's operational maintenance routine.	An approved SMS should already include procedures for maintaining and testing back-up arrangements for shipboard equipment. Notwithstanding this, it may not address procedures for maintaining and storing offline back-ups for data and systems required for the safe operation of the ship and protection of the environment. A SMS, which incorporates CRM, should include procedures for: ● checking back-up arrangements for critical systems, if not covered by existing procedures ● checking alternative modes of operation for critical systems, if not covered by existing procedures ● creating or obtaining back-ups, including clean images for OT to enable recovery from a cyber incident ● maintaining back-ups of data required for critical systems to operate safely ● offline storage of back-ups and clean images, if appropriate ● periodic testing of back-ups and back-up procedures.