THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

version 5

Produced and supported by:
BIMCO, Class NK, Columbia Shipmanagement Cyprus, Chamber of Shipping of America, Cygnus Technologies, Digital Container Shipping Association (DCSA), INTERMANAGER, International Association of Dry Cargo Shipowners (INTERCARGO), International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Marine Contractors Association (IMCA), International Union of Marine Insurance (IUMI), Maersk, Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC), Nordic Maritime Cyber Resilience Centre (NORMA Cyber), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass), Templar Executives, World Shipping Council.
(see Annex 5)

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

version 5

Terms of use
The advice and information given in this publication is intended purely as guidance to be used at the user's own risk. No warranties or representations are given, nor is any duty of care or responsibility accepted by the authors, their membership or employees of any person, firm, corporation or organisation (who or which has been in any way concerned with the furnishing of information or data, or the compilation or any translation, publishing or supply of this publication) for the accuracy of any information or advice given in this publication; or any omission from the guidelines or for any consequence whatsoever resulting directly or indirectly from compliance with adoption of or reliance on guidance contained in this publication, even if caused by a failure to exercise reasonable care on the part of any of the aforementioned parties.

Contents

Contents 3

Introduction 7

1 Cyber security and risk management 9

1.1 Cyber security characteristics of the maritime industry 9

1.2 Senior management involvement 12

1.3 Roles, responsibilities and tasks 13

1.4 Differences between IT and OT systems 14

1.5 Plans and procedures 15

1.6 Relationship between shipowner and ship manager 16

1.7 Relationship between the shipowner and the agent 17

1.8 Relationship with vendors and other external parties 18

2 Identify threats 20

2.1 Threat actors 20

2.2 Types of cyber threats 21

2.3 Stages of a cyber incident 22

2.4 Quantifying the threat 23

General considerations 23

Threats against OT systems 24

Threats against IT systems 24

3 Identify vulnerabilities 25

3.1 Common vulnerabilities 25

3.2 IT and OT systems' documentation 25

3.3 Typical vulnerable systems 26

3.4 Ship to shore interface 28

3.5 Ship visits 29

3.6 Remote access 29

3.7 System and software maintenance 30

4 Assessing the likelihood 31

4.1 Likelihood as the product of threat and vulnerability 31

4.2 Quantifying the likelihood 31

5 Impact assessment 33

5.1 The CIA model 33

5.2 Quantifying the impact 33
5.3 "Critical" equipment and technical systems 35

6 Risk assessment 37
6.1 Relationship between factors influencing risk 37
6.2 The four phases of a risk assessment 37
Phase 1: Pre-assessment activities 37
Phase 2: Ship assessment 38
Phase 3: Debrief and reporting 40
Phase 4: Manufacturer's debrief 40
6.3 Third party risk assessments 41

7 Develop protection measures 42
7.1 Defence in depth and in breadth 42
Defence in depth 42
Defence in breadth 43
7.2 Technical protection measures 43
Limitation to and control of network ports, protocols and services 44
Configuration of network devices such as firewalls, routers and switches 44
Physical security 45
Satellite and radio communication 46
Wireless access control 47
Secure configuration of hardware and software 47
Control administrative privileges 47
Email and web browser protection 48
Phishing: The most commonly reported cyber-attack 48
Application software security (patch management) 48
7.3 Procedural protection measures 49
Training and awareness 49
Computer access for visitors 51
Crew's personal devices 52
Upgrades and software maintenance 52
Anti-virus and anti-malware tool management 53
Remote access 53
Use of administrator privileges 53
Multi/factor authentication (MFA) and passwords 54
Physical and removable media controls 54
Equipment disposal including data destruction 55

8 Develop detection measures 56
8.1 Detection, logging, blocking and alerts 56
8.2 Malware detection 56

9 Establish contingency plans 57
Disconnecting OT from shore network connection 58

10 Respond to and recover from cyber security incidents 59
10.1 Effective response 59
10.2 The four phases of incident response 59
Phase 1, Preparation: 59
Phase 2, Detection and Analysis: 60
Phase 3, Containment and Eradication: 60
Phase 4, Post-Incident Recovery: 61
10.3 Recovery plan 62
10.4 Data recovery capability 62
10.5 Investigating cyber incidents 63
10.6 Losses arising from a cyber incident 63
Cover for property damage 64
Cover for liability 65
Cyber security clause for charter parties 65
10.7 Reporting of cyber incidents 65
ANNEX 1 – Onboard IT and OT systems, equipment and technologies 66
Communication systems 66
Bridge systems 66
Propulsion, machinery management and power control systems 66
Access control systems 67
Cargo management systems 67
Passenger or visitor servicing and management systems 67
Passenger-facing networks 67
Core infrastructure systems 68
Administrative and crew welfare systems 68
ANNEX 2 – Cyber risk management and the safety management system 69
Identify 70
Protect 71
Detect 74
Respond 75
Recover 76
ANNEX 3 – Onboard networks 77
Physical layout 77
Network management 77
Network segmentation 77
Monitoring data activity 80
Protection measures 80
ANNEX 4 – Glossary 82

ANNEX 5 – Contributors to most recent revision of this publication 85
Working Group 2024 85
Reference Group 2024 85

Introduction

The purpose of these guidelines is to improve the safety and security of seafarers, the environment, the cargo and the ships. The guidelines aim to assist in the development of a proper cyber risk management strategy in accordance with relevant regulations and best practises on board a ship with a focus on work processes, equipment, training, incident response and recovery management.

Shipping relies heavily on digital solutions for the completion of everyday tasks. The rapid developments within information technology, data availability, the speed of processing and data transfer present shipowners and other players in the maritime industry with increased possibilities for operational optimisation, cost savings, safety improvements and a more sustainable business. However, these developments to a large extent rely on increased connectivity, often via internet between servers, IT systems and OT systems[1], which increases the attack surface of potential cyber vulnerabilities.

These guidelines explain why and how cyber risks should be managed in a shipping context. The supporting documentation required to conduct a risk assessment is listed and the risk assessment process is outlined with an explanation of the part played by each component of cyber risk. This publication highlights the importance of evaluating the likelihood and threat in addition to the impact and vulnerabilities when conducting a cyber risk assessment. Finally, this publication offers advice on how to respond to and recover from cyber incidents.

Approaches to cyber risk management will be company and ship specific but should be guided by the requirements of relevant national, international and flag state regulations and guidelines. 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 consider cyber risk management in accordance with the objectives and functional requirements of the (International Safety Management) ISM Code. It further encourages administrations to ensure that cyber risks are appropriately addressed in SMS no later than the first annual verification of the company's Document of Compliance (DoC) after 1 January 2021. The same year, IMO developed guidelines[2] 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 management into all levels and departments of an organisation and ensure a holistic and flexible cyber risk governance regime, which is in continuous operation and constantly evaluated through effective feedback mechanisms.

---

[1] Operational Technology (OT) systems include hardware and software which monitor and/or control physical devices, processes, and events. Information Technology (IT) systems include hardware and software which manages data (ie IT systems do not control physical devices, processes or events).

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

In addition to the IMO resolution, the U.S. National Institute of Standards and Technology (NIST) Draft Cybersecurity Framework Version 2.0 (February 2024) has also been taken into account in the development of these guidelines. The NIST Cybersecurity Framework assists companies with their approach to risk assessments by helping them understand an effective approach to manage potential cyber risks both internally and externally. As a result of applying the Framework, a "profile" is developed, which can help to identify and prioritise actions for reducing cyber risks. The profile can also be used as a tool for aligning policy, business and technological decisions to manage the risks. Sample framework profiles are publicly available for maritime bulk liquid transfer, offshore and passenger ship operations[3]. Profiles were created by the United States Coast Guard and NIST's National Cybersecurity Center of Excellence and industry stakeholders. The NIST's profiles can be used together with these guidelines to assist industry in assessing, prioritizing and mitigating their cyber risks.

Guidelines are also available from other associations, such as the Digital Container Shipping Association's (DCSA) "DCSA Implementation Guide for Cyber Security on Vessels v1.0". The DCSA's guidelines are based on an analysis of version 3 of these guidelines and the NIST framework. While the target audience for DCSA's guidelines is the container industry, other segments of shipping may also find them worthwhile to read. In addition, the International Association of Ports and Harbors published "Cybersecurity Guidelines for Ports and Port Facilities version 1.0". Even though the intended audience for the IAPH guidelines are shoreside entities, there are consistent messages that the interdependent ship and port communities can both benefit from.

The International Association for Classification Societies (IACS) has developed revisions 1 of Unified Requirements E26 ("Cyber Resilience of Ships") and E27 ("Cyber Resilience of On-Board Systems and Equipment") which apply to newbuilds and which apply from 1 July 2024[4].

The present 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.

[3] The NIST Framework Profiles for maritime bulk liquid transfer, offshore, and passenger operations, liquefied natural gas, and the responsible use of PNT services can be accessed here: **https://www.nist.gov/cyberframework**

[4] IACS UR E26 and E27 can be accessed here: **https://iacs.org.uk/resolutions/unified-requirements/ur-e**

1 Cyber security and risk management

1.1 Cyber security characteristics of the maritime industry

Cyber security is important because of its potential effect on personnel, the ship, environment, company, cargo and reputation. Cyber security is concerned with the protection of IT, OT, information and data from unauthorised access, manipulation and disruption.

Cyber incidents can arise as the result of eg:

- An attack targeted directly against the organisation
- The organisation being impacted by an attack targeted at another organisation (eg a third-party suffers an incident that has a subsequent impact on the organisation)
- An unintended error, mistake or accident occurring.

Examples of cyber incidents include:

- A waterhole attack targeting a commonly downloaded file affecting the availability and integrity of OT, for example corruption of chart data held in an Electronic Chart Display and Information System (ECDIS)
- Unintended system failure occurring during software maintenance and patching, for example using an infected USB drive to complete the maintenance
- Crew interaction with phishing attempts, which is the most common initial attack vector by threat actors. Successful phishing attempts can lead to the loss of sensitive data and the introduction of malware to shipboard systems
- Loss of or manipulation of external sensor data, critical for the operation of a ship should not be discounted. Such sensor data includes but is not limited to Global Navigation Satellite Systems (GNSS), of which the Global Positioning System (GPS) is the most frequently used.

The maritime industry has a range of characteristics that affect its vulnerability to cyber incidents. These include:

- Involvement of multiple stakeholders in the operation and chartering of a ship potentially resulting in lack of accountability for the IT and OT system infrastructure and ship's networks
- Regular crew changes which can potentially affect accountability, continuity and proper password handling
- Use of legacy IT and OT systems that are no longer supported and/or that rely on obsolete operating systems
- Use of OT systems that cannot be patched or run anti-virus due to type approval issues
- Ships that interface online with shoreside parties and other parts of the global supply chain

- Ship equipment that is remotely monitored and accessed, eg by the manufacturers or support providers
- The sharing of business critical, data sensitive and commercially sensitive information with shore-based service providers, including marine terminals and stevedores and also, where applicable, public authorities
- The availability and use of computer controlled critical systems, which may not have the latest updates/patches installed or be properly secured, for the ship's safety and for environmental protection
- A cyber risk management culture that still has potential for improvement, eg through more formalised training, exercises and clarified roles and responsibilities
- Frequently the automation system comprises of multiple sub-systems from numerous vendors that are integrated by shipyards with minimal regard to cyber issues
- Failure to follow best practices for lifecycle management (section 7.3) and properly decommission and remove unsupported systems from the vessel, to prevent their unplanned and unauthorized use by crew.

These elements should be considered, and relevant parts incorporated into the company cyber security policies and SMS.

The growing use of comprehensive data analysis, smart ships and the "Industrial Internet of Things" (IIoT) will increase the amount of information available to threat actors and the potential attack surface to cyber criminals. This necessitates robust approaches to cyber risk management[5].

Cyber risk management should be an inherent part of a company's safety and security culture conducive to the safe and efficient operation of the ship and be implemented at various levels of the company, including senior management ashore and onboard personnel. Cyber risk management should be tailored to each company's risk profile, as well as meet flag-State regulatory requirements, and should furthermore:

- Identify the roles and responsibilities of users, key personnel, third parties (eg vendors, service providers and integrators) and management both ashore and on board
- Identify the systems, assets, data and capabilities that, if disrupted, could pose risks to the ship's operations and safety
- Implement technical and procedural measures to protect against a cyber incident, provide timely detection of incident, minimise the impact of incidents and ensure continuity of operations
- Fulfil regulatory requirements
- Ensure reporting and investigation of cyber security incidents according to the principles of the SMS
- Exercise contingency and response plans regularly.

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

Some aspects of cyber risk management may include commercially sensitive or confidential information, for example the cyber risk assessment and its associated hardware and software inventories and network maps. Companies should, therefore, consider protecting this information appropriately, and as far as possible, not include sensitive information in their SMS. Similarly, proper sanitation of equipment selected for divestment or decommissioning should be carried out.

Figure 1 – Cyber risk management approach as set out in this publication.

Development, implementation and maintenance of a cyber risk management programme in accordance with the approach in figure 1 is no small undertaking. It is, therefore, important that senior management stays engaged throughout the process to ensure that the protection and contingency planning are balanced and to manage risks within an acceptable limit. Factors such as impact, likelihood, vulnerabilities, threats, capability, opportunity and intent of malicious actors are interrelated (see figure below) and are all relevant when assessing risk. It follows that if either

of the factors is low or even zero, the same will eventually apply to the risk. It is important to emphasize that risk assessment is not a one-time activity. It must be repeated at regular intervals to assess whether threats, vulnerabilities, likelihoods, impacts and risks have changed, and if the control measures are still appropriate.

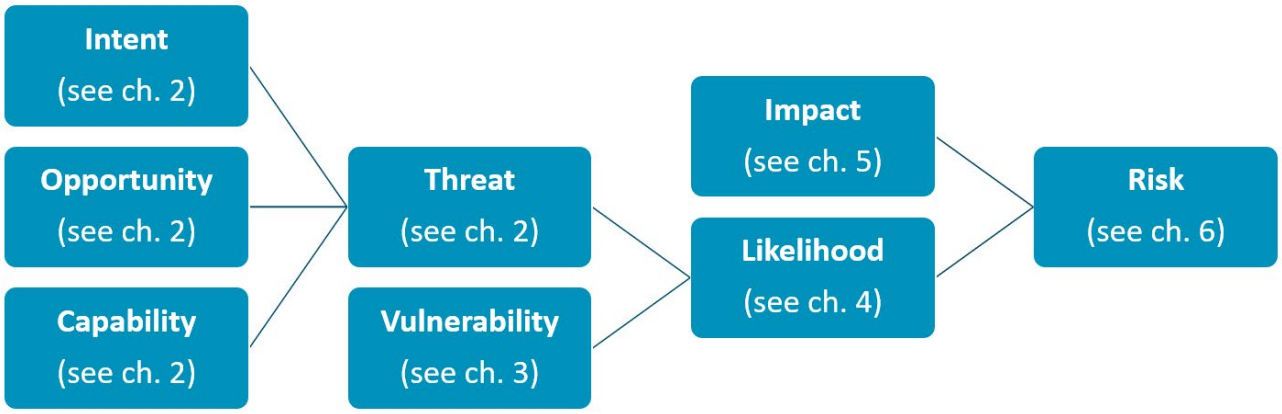

Figure 2 – The relationship between different factors influencing the risk. The lines represent multiplication, ie "Likelihood" is multiplied with "Impact" to produce "Risk".

1.2 Senior management involvement

Effective cyber risk management will involve the senior management level of a company on an ongoing basis, instead of for example, only the ship security officer or the IT manager. There are several reasons for this:

- Some cyber risks have wide-ranging destructive potential to the safety of personnel and the environment as well as the performance and reputation of the company. Cyber risks are therefore not simply security challenges, but business challenges that require leadership's involvement.
- Initiatives to heighten cyber security and safety may affect standard business procedures incl. budgeting and operations by rendering them more time consuming and/or costly. It is, therefore, a senior management decision to evaluate and allocate the necessary resources to establish risk mitigation to an acceptable level of residual risk based upon the company's risk tolerance level.
- Initiatives, which heighten cyber awareness, will likely change how the company interacts with unions, customers, suppliers and authorities, and impose new requirements on the co-operation between parties. It is a senior management decision whether to drive these changes in relationships and how best to do so.

The answers to the following questions may be used as a basis for informing and involving senior management about the importance of addressing cyber risks onboard ships:

- What is the company's risk tolerance level? What level of losses, eg magnitude, would be acceptable?
- What assets are at risk?

- What is the potential impact of a cyber incident to the business, customers, partners and stakeholders?
- Who has the final responsibility for cyber risk management?
- Are the OT systems and their working environment protected from unauthorized access and changes?
- Is there remote access to the OT systems and, if so, how is it monitored and protected?
- Are the IT systems protected and is access being appropriately managed and monitored?
- What cyber risk management best practices are being used?
- What is the cyber risk training level of the personnel operating the IT and OT systems?

Based on the answers, the company should describe and delegate authority as appropriate, and allocate the resources needed to develop and maintain suitable solutions based on the risk assessment results.

1.3 Roles, responsibilities and tasks

Effective cyber risk management relies on a clear allocation of responsibilities and tasks within the company. Cyber risk management is an integral part of ship management and ship operation, and different employees have different roles, responsibilities and tasks. Furthermore, in some companies, some roles, responsibilities and tasks are outsourced to third parties.

The various responsibilities and tasks should be mapped to the job descriptions and/or role descriptions found in the SMS. As cyber risk management planning and execution involves the whole company; it may be useful during the mapping process to clarify who is the responsible person, and who is required to support that person. For example, a ship IT manager may well be the responsible party for cyber risk management in ships, but the rely on support from other managers and staff from across the whole company, eg security staff, safety staff, training staff, procurement staff, marine HR staff, master, ship security officer, crew etc.

Often, the allocation of responsibilities and tasks will work best if it is aligned with the normal chain of command. For example, when allocating the responsibility for compliance with cyber risk management procedures on board a ship, it will often make sense to appoint the Master or the Chief Engineer, as often done for the Ship Security Officer role. Additional role-specific training should be considered.

Task Role/person	Cyber input to safety/security policy	Cyber risk assessment on ship OT systems	Cyber risk assessment on ship IT systems	Ship IT/OT infrastructure management	Crew cyber risk management training
Managing director	Responsible				
Company IT manager	Supporting		Supporting		Supporting
Ship IT manager	Supporting	Responsible	Responsible	Responsible	
Safety manager	Supporting	Supporting	Supporting	Supporting	Supporting
Procurement manager	Supporting			Supporting	
Fleet technical manager		Supporting	Supporting	Supporting	Supporting
Training manager			Supporting		Supporting
Marine HR manager			Supporting		Responsible

Figure 3 – Example (non-exhaustive) of mapping roles, responsibilities and tasks in a matrix. Job titles and associated job scope and responsibilities will vary from company to company. IT and OT responsible persons need to align and coordinate the company's cyber risk management strategy.

1.4 Differences between IT and OT systems

Whereas IT systems manage data and support business functions, OT is the hardware and software that directly monitors/controls physical devices and processes and as such are an integral part of the ship and must function independently of the IT systems onboard. The systems can, however, be connected to the IT network for performance monitoring, remote support, etc. Such systems are sometimes referred to as the Industrial Internet of Things (IIOT). In such cases, it must be ensured that the interface is sufficiently guarded by a firewall as a minimum and potential vulnerabilities in the OT systems are not exposed to the IT network. This is important because it is not always possible or feasible to ensure a proper patch level in OT systems.

IT covers the spectrum of technologies for information processing, including software, hardware and communication technologies. Traditionally OT and IT have been separated, but with the internet, OT and IT are coming closer as historically stand-alone systems are becoming integrated. Disruption of the operation of OT systems may impose significant risk to the safety of onboard

personnel, cargo, damage to the marine environment and impede the ship's operation. Likewise, failure of certain IT systems, eg lack of immediate access to dangerous goods manifest, could also result in hazardous situations. For example, in situations where a container aboard ship is on fire, information about the contents of adjacent containers is critical for proper firefighting.

There may also be important differences between who handles the purchase and management of the OT systems versus IT systems on a ship. IT managers are not usually involved in the purchase of OT systems and may or may not have a thorough understanding of cyber security. The purchase of such systems should involve someone who knows about the impact on the onboard systems but will most probably only have limited knowledge of software and cyber risk management. It is therefore important to have a dialogue with an individual knowledgeable of cyber security to ensure that cyber risks are considered during the OT purchasing process. Updating of OT software is often performed by the makers and requires management of change incl. cyber security considerations and a thorough compatibility check and class approval as opposed to IT software, which is normally updated routinely. To obtain an overview of potential challenges and to help establish the necessary policy and procedures for software maintenance, it can be an advantage for the party responsible for cyber security on board the ship to have an inventory of OT systems.

1.5 Plans and procedures

IMO Resolution MSC.428(98) identifies an urgent need to raise awareness on cyber risks, threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks. Thus, all maritime stakeholders should work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities. The resolution furthermore affirms that the SMS should consider cyber risk management in accordance with the objectives and functional requirements of the ISM Code.

The 101st session of IMO's Maritime Safety Committee (the report from this meeting is found in IMO document MSC 101/24) "… agreed that aspects of cyber risk management, including physical security aspects of cyber security, should be addressed in Ship Security Plans (SSP) under the ISPS Code; however, this should not be considered as requiring a company to establish a separate cyber security management system operating in parallel with the company Safety Management System (SMS)".

In the same meeting, IMO also "… confirmed that resolution MSC.428(98) on Maritime cyber risk management in SMS set out IMO's requirements for Administrations to ensure that cyber risks were appropriately addressed in existing SMS (as defined in the ISM Code), verified by an endorsed Document of Compliance and Safety Management Certificate, and that in the Ship Security Plan, reference should be made to cyber risk management procedures found in SMS".

For a company, a simple way of arranging procedures as required by IMO could be to reflect the following in the Ship Security Plan (SSP) or otherwise same to be incorporated in corresponding part of SMS:

- Procedures related to physical access to areas with IT and OT systems

- A reference to the SMS' cyber security procedures. Consideration should be given to wording the reference in a way that will not require it to be updated every time a cyber security related procedure in the SMS is amended, added or removed, as changes to the SSP would normally require approval from Flag State or the Recognised Organisation authorised to do so by the Flag State.

Accordingly, the remaining procedures on cyber risk management should be reflected in the SMS, whilst excluding sensitive information such as the system's documentation described in section 3.2 of the present guidelines that could be exploited by malicious actors outside the company.

The SMS already includes procedures for reporting accidents or hazardous situations and defines levels of communication and authority for decision making. If needed, such procedures should be amended to reflect communication and authority in the event of a cyber incident. The Master must have a defined resource to refer to in the event of a cyber incident and the SMS should include a well-designed response plan for cyber contingencies – see chapter 9.

Additional guidance on how to incorporate cyber risk management into the company's SMS can be found in annex 2 of these guidelines.

SMS procedures should consider risks arising from the use of IT and OT on board, taking into account applicable codes, guidelines and recommended standards. It can be considered that procedures addressing eg commercial risks are also included in the SMS rather than a separate document.

The company should consider ship-specific risk assessments based on whether particular ships or groups of ships are configured uniquely in terms of IT/OT setup within their fleet. The factors to be considered include but are not limited to the extent to which IT and OT are used on board, the complexity of system integration and the nature of operations. Similarly, consideration should be given to whether procedures in the SMS can be arranged to cover the company's fleet, or whether specific procedures are required for specific ships.

The cyber risk assessment and the IT and OT systems documentation described in section 3.2 are considered sensitive information. While there is no regulation describing how this information should be stored, the recommendation is for it to be stored and controlled, to the extent possible, in a similar manner as the Ship Security Assessment and SSP.

1.6 Relationship between shipowner and ship manager

The Document of Compliance (DoC) holder is ultimately responsible for ensuring the management of cyber risks on board. If the ship is under third party management, then the ship manager is advised to reach an agreement with the shipowner.

Emphasis should be placed by both parties on the split of responsibilities, alignment of expectations, agreement on specific instructions to the manager and possible participation in purchasing decisions as well as budgetary requirements.

Apart from ISM requirements, such an agreement should take into consideration additional applicable legislation like the EU General Data Protection Regulation (GDPR) or specific cyber regulations in other coastal states, as appropriate. Managers and owners should consider using these guidelines as a base for an open discussion on how best to implement an efficient cyber risk management regime.

Agreements between ship managers and shipowners on cyber risk management should be done in writing and signed.

1.7 Relationship between the shipowner and the agent

The importance of this relationship has placed the agent[6] as a named stakeholder, interfacing continuously and simultaneously with shipowners, operators, terminals, port services vendors and port state control authorities through the exchange of sensitive, financial and port coordination information. The relationship goes beyond that of a vendor. It can take different forms and especially in the tramp trade, shipowners require a local representative (an independent ship agent) to serve as an extension of the company.

Quality standards for agents are important because like all other businesses, agents can also be targeted by cyber criminals eg in connection with delivery of IT or OT equipment to the ship. Cyber-enabled crime, such as electronic wire fraud and false ship appointments, and cyber threats such as ransomware and hacking, call for mutual cyber strategies and cyber-enhanced relationships between shipowners and agents to mitigate such cyber risks.

INCIDENT: SHIP AGENT AND SHIPOWNER RANSOMWARE INCIDENT

A shipowner reported that the company's business networks were infected with ransomware, apparently from a phishing email attachment. The source of the ransomware was from two unwitting ship agents, in separate ports, and on separate occasions. Ships were also affected but the damage was limited to the business networks, while navigation and ship operations were unaffected. In one case, the owner paid the ransom.

The importance of this incident is that harmonized cyber security across relationships with trusted business partners and manufacturers is critical to all in the supply chain. Individual efforts to fortify one's own business can be valiant and well-intended but could also be insufficient. Parties in the supply chain should work together and share information as appropriate to mitigate cyber risk. As phishing is one of the most common techniques used in cyber-attacks, training on how to identify and report phishing should be part of mandatory cyber security training for all personnel.

[6] The party representing the ship's owner and/or charterer (the Principal) in port. If so instructed, the agent is responsible to the principal for arranging, together with the port, a berth, all relevant port and husbandry services, tending to the requirements of the Master and crew, clearing the ship with the port and other authorities (including preparation and submission of appropriate documentation) along with releasing or receiving cargo on behalf of the principal (source: Convention on Facilitation of International Maritime Traffic (FAL Convention).

1.8 Relationship with vendors and other external parties

Companies should evaluate the physical security and cyber risk management processes of their interaction with service providers, vendors and other external parties, including public authorities. Lack of physical and/or cyber security at a supplier, vendor or service provider may result in a breach of corporate IT systems and/or corruption of ship OT/IT systems. The company should therefore consider entering into supplier/vendor/service provider agreements and contracts that define cyber-related requirements and expectations, as appropriate. Companies should also evaluate the cyber risk management processes for both new and existing contracts. Broadly recognised standards exist (eg Service Organization Control (SOC) 2 Type 2 for Service-as-a-Software applications) but the company can also define its own standards.

The processes evaluated during supplier vetting and included in contract requirements may involve:

- Security management including management of sub-suppliers
- Manufacturing/operational security
- Software engineering and architecture, and the ability to constantly address new vulnerabilities arising out of threat developments and updates to operating systems
- Asset and cyber incident management
- Personnel security
- Data and information protection
- Remote service/access.

Evaluation of service providers beyond those with whom the company has a direct relation may be challenging, especially for companies with many direct suppliers. Third party providers that are collecting and managing supplier risk management data may be an option to consider.

A ship's and its company's interactions with public authorities are complex covering many issues ranging from ship arrival to crew changes to advance cargo manifest submissions. They also involve relevant challenges for the cyber risk management process. Normally, these challenges cannot be addressed in the same way as those which the company has with its commercial relationships. However, it is important that current and future communication connections with public authorities for the provision and exchange of mandatorily required information be evaluated and assessed as part of the company's cyber security position, and that any cyber security concerns arising from such connections be brought to the attention of the relevant authorities, as appropriate. Some of these issues are further discussed in section 3.4.

The following should be considered regarding manufacturers and third parties including vendors, contractors and service providers:

- Manufacturers' and service providers' will and ability to implement effective and cost-efficient cyber security best practice in their products and services, which can be demonstrated in different ways eg by following the CIRM Cyber Risk Code of Practice for Vendors of Marine Electronic Equipment and Services and the associated implementation guidelines.[7]
- Manufacturers' and service providers' cyber risk management awareness and procedures: Some companies may lack cyber awareness training and governance in their own organisations, and this may represent more sources of vulnerability, which could result in cyber incidents. Third party vendors and suppliers are increasingly being targeted by threat actors and have played a role in well publicized cyber incidents over the years. These companies should have a regularly reviewed and updated cyber risk management company policy, which is signed off by the responsible person and includes mandatory cyber security training and governance procedures for accessible IT and OT systems.
- The maturity of a third party's cyber risk management procedures: The shipowner should query the internal governance of cyber security and seek to obtain a cyber risk management 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 such as a marine terminal, stevedoring company or OT supplier for ongoing support and maintenance.

INCIDENT: UNRECOGNISED VIRUS IN AN ECDIS DELAYS SAILING

A newbuild dry bulk ship was delayed from sailing for several days because its ECDIS was infected by a virus. The ship was designed for paperless navigation and was not carrying paper charts. The failure of the ECDIS appeared to be a technical disruption and was not recognised as a cyber issue by the ship's Master and officers. A manufacturer technician was required to visit the ship and, after spending a significant time in troubleshooting, discovered that both ECDIS networks were infected with a virus. The virus was quarantined and the ECDIS computers were restored. The source and means of infection in this case are unknown. The delay in sailing and costs in repairs totalled in the hundreds of thousands of dollars (US).

[7] The Code and the guidelines can be found at the website of Comité International Radio-Maritime (CIRM): **http://cirm.org/publications**

2 Identify threats

2.1 Threat actors

When identifying threats, companies should consider specific aspects of potential threat actors' capability, opportunity and intent to attack. Once identified, threats should be considered alongside identified vulnerabilities to evaluate the likelihood of an attack or incident taking place. Together with the impact of a given incident, the likelihood of the incident occurring produces the risk factor.

Organisations and individuals can constitute an intentional or even unintentional threat to the safety and security of a crew, the environment and the ship. The following figure lists examples of threat actors and their possible motivations and objectives. The list is non-exhaustive and may overlap. Such threat actors will have varying degrees of skills and resources to potentially threaten the safety and security of ships and a company's ability to conduct its business:

Group	Motivation
Accidental actors	Non-malicious motive but still end up causing unintended harm through bad luck, lack of knowledge, -training or -care, eg by inserting infected USB in onboard IT or OT systems.
Activists (including disgruntled employees)	• Political • Revenge • Disruption of operations • Media attention • Reputational damage.
Criminals	• Financial gain • Commercial espionage • Industrial espionage.
Opportunists	• The challenge • Reputational gain • Financial gain.
States State sponsored organisations	• Political/ideological gain eg (un)controlled disruption to economies and critical national infrastructure • Espionage • Disruption • Financial gain • Commercial espionage • Industrial espionage • Commercial gain.
Terrorists	• Political • Financial • Disruption • Recognition / media attention.

Figure 4 – Threat actors' motivation and objectives.

2.2 Types of cyber threats

In general, there are two categories of cyber threats that may affect companies and ships:

- Untargeted attacks, where a company or a ship's systems and data are one of many potential targets, is an unintended victim, or collateral damage (eg shipping was impacted by NotPetya but was not a targeted victim). Untargeted attacks are likely to use tools and techniques available on the internet, which can be used to locate, discover and exploit widespread vulnerabilities that may also exist in a company and onboard a ship.
- Targeted attacks, where a company or a ship's systems and data are the intended target or one of multiple targets. Targeted attacks may be more sophisticated and require prior reconnaissance eg via social media or web pages, and use tools and techniques specifically created for targeting a certain company or ship.

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

- **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 of and manipulate a problem in another computer's software or hardware. This problem can, for example, be a code bug, system vulnerability, improper design, hardware malfunction and/or error in protocol implementation. In some cases, spyware can be used to identify admin user credentials, allowing the malicious actor to logon as the admin user and manipulate system functions. These vulnerabilities may be exploited remotely or triggered locally eg a piece of malicious code may often be executed by the user, sometimes via links distributed in email attachments or through malicious websites.
- **Water holing.** Establishing a fake website or compromising a genuine website to exploit unsuspecting visitors.
- **Scanning.** Searching large portions of the internet at random for vulnerabilities that could be exploited.
- **Typosquatting.** Also called URL hijacking or fake URL. Relies on mistakes such as typos made by internet users when inputting a website address into a web browser or luring victims to click a website link that at a glance looks like a website they are familiar with. Should a user accidentally enter an incorrect website address, they may be led to an alternative and often malicious website.
- **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 email, social media, phone calls or in-person.
- **Brute force**. An attack trying many passwords with the hope of eventually guessing correctly to gain unauthorized access. The attacker systematically checks all possible passwords until the correct one is found.
- **Credential stuffing**. Using previously compromised credentials or specific commonly used passwords to attempt unauthorized access to a system or application.

- **Denial of service (DoS)** prevents legitimate and authorised users from accessing information, usually by flooding a network with data. A distributed denial of service (DDoS) attack takes control of multiple computers and/or servers to implement a DoS attack.
- **Phishing**. Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information. The email may also contain a malicious attachment or request that a person visits a fake website using a hyperlink included in the email.
- **Spear-phishing.** Like phishing but the individuals are targeted with personal emails, often containing malicious software or links that automatically download malicious software. In some instances, SAT-C messages have been used to establish a sense of familiarity with a malicious sender's email address.
- **Subverting the supply chain.** Attacking a company or ship by compromising equipment, software or supporting services being delivered to the company or ship.

The above examples are not exhaustive. 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.

2.3 Stages of a cyber incident

In 2019, it took on average 277 days between the time a victim's network was breached and the containment of the breach. However, intrusion can go undetected for years. Year on year, this figure has been largely unchanged since 2019[8]. The length of time to prepare a cyber-attack can be determined by the motivations and objectives of the attacker, and the resilience of technical and procedural cyber risk controls implemented by the company, including those onboard its ships. When considering targeted cyber-attacks, the generally observed stages of an incident are:

- **Survey/reconnaissance.** Open/public sources such as social media are used to gain information about a potential target (eg a company, ship or seafarer) in preparation 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.
- **Delivery**. Attackers may attempt to access the company's and ship's 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:
    - Company online services, including cargo or container tracking systems
    - Sending emails containing malicious files or links to malicious websites to personnel
    - Providing infected removable media, for example as part of a software update to an onboard system
    - Creating false or misleading websites, which encourage the disclosure of user account information by personnel.

[8] IBM Cost of a Data breach Report 2023.

- **Breach.** The extent to which an attacker can breach a company's or ship's 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:
  - Make changes that affect the system's operation, for example interrupt or manipulate information used by navigation equipment
  - Gain access to, take copies of or alter operationally important information such as loading lists or commercially sensitive data such as cargo manifests and/or crew and passenger/visitor lists
  - Achieve full control of a system, for example a machinery management system.

- **Pivot**. Pivoting is the technique of using an already compromised system to attack other systems in the same network. During this phase of an attack, an attacker uses the first compromised system to attack otherwise inaccessible systems. An attacker will usually target the most vulnerable part of the victim's system with the lowest level of security. Once access is gained then the attacker will try to exploit the rest of the system. This is why assessing risks created by integrated IT/OT systems aboard a ship is so important. Usually, in the pivot phase, the attacker may try to:
  - Upload tools, exploits and scripts in the system to support the attacker in the new attack phase
  - Execute a discovery of neighbour systems with scanning or network mapping tools
  - Install permanent tools to keep and maintain access to the system
  - Execute new attacks on the system.

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:

- Access commercially sensitive or confidential data about cargo, crew, visitors and passengers
- Manipulate crew or passenger/visitor lists, cargo manifests, stow plans or loading lists – this may subsequently be used to allow the fraudulent transport of illegal cargo or facilitate thefts
- Cause complete denial of service on business and operational systems
- Enable other forms of crime for example piracy, theft and fraud
- Disrupt normal operation of the company and ship systems, for example by deleting critical pre-arrival or discharge information or overloading company systems
- Demand a ransom for operational or personal data.

2.4 Quantifying the threat

General considerations

Threat is the product of the threat actor's capability, opportunity and intent to cause harm. The purpose of quantifying the threat is to help the quantification of the likelihood, which forms part

of the assessment of risk that is the product of likelihood and impact. In other words, if either the capability, opportunity or intent of a threat actor is zero or close to zero, the threat and thereby the risk will be small.

Threats against OT systems

Unlike other areas of safety and security, where historic evidence is available, cyber risk management is made more challenging by the scarcity of statistics about incidents and their impact.

Indications are that attacks targeted specifically against OT systems, while increasing, still remain less common in comparison to attacks against IT systems and, in many cases, not publicised. Reasons for this are likely to include:

- Many OT systems in the marine industry are still not connected to networks with external access, ie threat exposure is low and cybercriminals have no opportunity to attack. However, there are exceptions. For example, many monitoring devices (eg devices monitoring engine performance) are connected to the internet and usually have minimal cyber security controls in place, especially in comparison to other IT or even OT systems. These IIOT systems are becoming more integrated onboard ships to provide remote monitoring and connection of systems to allow for greater automation and efficiency in operations. Threat actors can scan for these systems and use them as an initial point of infiltration to a ship's network, from which they can pivot as outlined previously. Therefore, risks to these systems are important to assess and should not be overlooked.
- Attacking OT systems entail safety risks to the victims, something which may constitute a disincentive and even a deterrent to some cybercriminals.
- Basic threat intelligence and the ability to monitor anomalous activity are not readily available on OT and IIoT systems as they are on IT systems, making it difficult to detect, analyse and react to a compromise.

Despite the above, the risks to OT systems should <u>not</u> be underestimated. Threats posed by vectors such as malware introduced through software updates – either online or through manual processes such as USB sticks – or through unregulated or unauthorised access by crew can still materialise and have been known to cause disruptions and operational downtime.

Threats against IT systems

Threats against IT systems are generally easier to quantify because there is much more evidence in terms of accidents both generally and specifically for the maritime industry. Disruption of IT systems is often not considered to be the cause of physical harm to people, the environment, assets or cargo, but threats against IT systems should not be underestimated. Recent examples from the liner industry have illustrated that cyber incidents have the potential to wreak havoc on ship operations and cargo management, thus causing significant financial losses. Furthermore, such incidents can also have cascading implications for the safety of people, environment, assets, cargo or reputation, eg when disruptions of IT systems lead to lack of control of perishable cargo or dangerous goods.

3 Identify vulnerabilities

3.1 Common vulnerabilities

The following are common cyber vulnerabilities, which may be found onboard existing ships (note, newbuild ships are subjected to requirements found in IACS Unified Requirements E26 and E27):

- Obsolete and unsupported operating systems.
- Unpatched system software
- Outdated or missing antivirus software and protection from malware
- Inadequate security configurations and best practices, including ineffective network management, insufficient screening of removable media and the use of default administrator accounts and passwords, sometimes even posted for everyone to see
- Weak, generic and/or easily guessed passwords
- Shared accounts and lack of multi-factor authentication
- Shipboard computer networks, which lack boundary protection measures and segmentation of networks
- Safety critical equipment or systems always connected with the shore side
- Inadequate access controls to cyber assets, networks etc for third parties including contractors and service providers
- Staff inadequately trained and/or skilled to manage cyber risks
- Missing, inadequate or untested contingency- and incident response plans and procedures
- Failure to complete decommissioning and disposal activities as defined in the asset lifecycle policies and procedures
- Use of business networks for personal activities such as browsing or streaming
- Computers never locking when idle.

3.2 IT and OT systems' documentation

To assist every step of the risk assessment, the IT and OT systems should be clearly identified with documented governance and ownership responsibilities within an asset register, which shall be kept updated as appropriate. The asset register should include an asset valuation, with the cost of the asset and the cost of maintaining that asset. While IACS Unified Requirements E26 and E27 are applicable to newbuilds only, it may nevertheless serve as guidance for the development of documentation that may include:

- Inventory of communicating devices
- Inventory of network communication devices:

- Network Topology drawings showing interfaces between OT-OT and OT-IT equipment
- Equipment Functional Design Specification
- Switches/Firewall Configuration.

- Logical map of networks:
  - IP addresses
  - Non IP addresses
  - Non Ethernet access points
  - Endpoints
  - Connectors and communicating field devices.
- Software inventory including version information (in some cases this inventory is part of a Ship Software Logging System)
- Inventory of network services for each piece of equipment.

Tools are available to handle the inventory of an IT system but are not recommended for OT system inventory as the integrity of the OT system could be disrupted (unless handled by a well-qualified expert in close consultation with the Master, Chief Engineer etc).

3.3 Typical vulnerable systems

Identification of vulnerabilities involves an analysis of the applications, systems and procedures to uncover weaknesses that could be leveraged by potential threats. It may be facilitated by internal experts and/or supported as appropriate by external experts with knowledge of the maritime industry and its key processes.

INCIDENT: CRASH OF INTEGRATED NAVIGATION BRIDGE SYSTEM AT SEA

A ship with an integrated navigation bridge system suffered a failure of nearly all navigation systems at sea, in a high traffic area and reduced visibility. The ship had to navigate by one radar and backup paper charts for two days before arriving in port for repairs. The cause of the failure of all ECDIS computers was determined to be attributed to the outdated operating systems. During the previous port call, a manufacturer technical representative performed a navigation software update on the ship's navigation computers. However, the outdated operating systems were incapable of running the software and crashed. The ship was required to remain in port until new ECDIS computers could be installed, classification surveyors could attend, and a near-miss notification had been issued as required by the company. The costs of the delays were extensive and incurred by the shipowner.

This incident emphasizes that not all computer failures are a result of a deliberate attack and that outdated software is prone to failure. More robust testing and proactive software maintenance on the ship may have prevented this incident from occurring.

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

- Temporary exposures such as software defects, outdated or unpatched systems.
- Design such as access management or unmanaged network interconnections.
- Implementation errors for example misconfigured firewalls or failure to disable superfluous software on computers.
- Procedural or other user errors, eg insufficient password protection and authentication processes.

Stand-alone systems should be less vulnerable to external cyber incidents compared to those attached to uncontrolled networks or connected directly to the internet. Network design and network segregation will be explained in more detail in Annex 3. Care should be taken to understand how critical shipboard systems are connected to uncontrolled networks. Onboard systems could include:

- **Cargo and loading management systems**. Digital systems used for the loading, management and control of cargo, including hazardous cargo, may interface with a variety of systems ashore, including those of ports, marine terminals and stevedores. 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 and loading lists vulnerable to cyber incidents.
- **Bridge systems**. The increasing use of digital, network navigation systems, with interface to shoreside networks for update and provision of services, make such systems vulnerable to cyber incidents. 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.
- **Propulsion and machinery management and power control systems**. The use of digital systems to monitor and control onboard machinery, propulsion and steering makes such systems vulnerable to cyber incidents. The vulnerability of these systems can increase when used in conjunction with remote condition-based monitoring and/or are integrated with navigation and communications equipment on ships using integrated bridge systems.
- **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 are vulnerable to cyber incidents.
- **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.
- **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, should be considered uncontrolled and should not be connected to any safety critical system on board.
- **Administrative and crew welfare systems**. Onboard computer networks used for administration of the ship or the welfare of the crew are particularly vulnerable when

providing internet access and email. This 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.

- **Communication systems**. Availability of internet connectivity via satellite and/or other wireless communication increases the vulnerability of ships, and recent developments indicate that for example VSAT signals are vulnerable to exploitation using low-cost, off-the-shelf products. Communication systems with encryption should be considered. The cyber defence mechanisms implemented by the service provider should be carefully considered but should not be solely relied upon to secure every shipboard system and data. Included in these systems are communication links to public authorities for transmission of required ship and cargo reporting information. Applicable authentication and access control management requirements by these authorities should be strictly complied with. Also included are shipboard capabilities to collect data from and interrogate devices and data loggers affixed to containers for onward transmission to designated recipients ashore (see also section below on ship to shore interface).

The abovementioned onboard systems consist of potentially vulnerable equipment, which should be reviewed during the assessment. The vulnerability assessment can be assisted by answering the below questions for each system:

- Is the system stand-alone or is it connected to other systems?
- Is the system connected externally, either directly or via other systems?
- Does the system have effective, built-in risk mitigation measures such as eg encryption?
- Does the system require regular software updates?
- Does operating the system allow connecting removable devices, for example to obtain diagnostic information?
- Is the system easy to physically access?

3.4 Ship to shore interface

Ships are becoming more and more integrated with shoreside operations because digital communication is being used to conduct business, manage operations and retain contact with head offices. Furthermore, critical ship systems essential to the safety of navigation, power and cargo management have become increasingly digitalised and connected to the internet to perform a wide variety of legitimate functions such as:

- Engine performance monitoring
- Remote diagnostics
- Temperature monitoring (eg reefers, LNG, etc)
- Maintenance and spare parts management
- Cargo and container tracking and management, loading and unloading and stowage planning

- Crane and pump management
- Monitoring of systems for adherence to environmental regulations and reporting
- Voyage performance monitoring.

The above list provides examples of this interface and is not exhaustive. The above systems contain, process and exchange data, which may be of interest to cyber criminals to exploit.

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

It is recommended that companies fully understand and document, as appropriate, the ship's OT and IT systems and how these systems connect and integrate with the shore side, including eg public authorities, marine terminals, manufacturers, vendors and stevedores. This requires an understanding of all computer-based onboard systems and how safety, operations and business, including cargo and load management, can be compromised by a cyber incident.

3.5 Ship visits

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 and other 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 having inserted an unknown removable media.

Sometimes there is no control as to who has access to the onboard systems, eg 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, and at the very least there should be a back-up of critical data and configurations made prior to entering a drydock or layup period. Where possible, systems should be scanned for malware prior to use following these events. OT systems should be tested to confirm they are functioning correctly.

3.6 Remote access

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 remotely monitors and

maintains the systems. These systems could include a two-way data flow and/or upload-only. Systems and workstations with remote control, access or configuration functions could, for example, be:

- Bridge and engine room computers and workstations on the ship's administrative network
- Cargo such as containers with reefer temperature control systems or specialised cargo that are tracked remotely
- Stability decision support systems
- Hull stress monitoring systems
- Bridge systems including Electronic Navigation Chart (ENC), Voyage Data Recorder (VDR) and dynamic positioning (DP)
- Load planning, stowage and cargo management
- Engine monitoring and control
- Safety and security networks, such as CCTV (closed circuit television)
- 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 considered as an important part of the risk assessment.

3.7 System and software maintenance

IT and OT systems, software and maintenance can be outsourced to third party service providers and the company itself may not be able to verify the level of security supplied by these providers. Some companies use different providers responsible for software and cyber security checks. In such cases, the suppliers should be requested to provide details of the updates.

INCIDENT: NAVIGATION COMPUTER CRASH DURING PILOTAGE

A ship was under pilotage when the ECDIS and voyage performance computers crashed. A pilot was on the bridge. The computer failures briefly created a distraction to the watch officers; however, the pilot and the Master worked together to focus the bridge team on safe navigation by visual means and radar. When the computers were rebooted, it was apparent that the operating systems were outdated and unsupported. The Master reported that these computer problems were frequent (referred to the issues as "gremlins") and that repeated requests for servicing from the shipowner had been ignored.

It is a clear case of how simple servicing and attention to the ship by management can prevent mishaps.

4 Assessing the likelihood

4.1 Likelihood as the product of threat and vulnerability

There is a tendency to assess risks alone based only on potential impacts and existing vulnerabilities. However, as previously accounted for, the likelihood of a cyber security event happening is the product of the threat and the vulnerability. This also means that if either of these two factors is close to non-existent, so will the likelihood be, and this should be considered when quantifying the likelihood.

4.2 Quantifying the likelihood

A company's SMS will normally contain a risk assessment matrix, where the likelihood of a given event is measured on a five-step scale. Using the SMS's existing likelihood scale can be an advantage because using existing language and concepts to describe cyber-related risks will ease the understanding and ability to measure effectiveness throughout the company. An aligned enterprise risk management strategy and understanding is critical to ensuring senior leadership's support for effective cyber risk management strategies based on the outcomes of the risk assessment. One example of such a scale can be found below:

Level	Likelihood description
1	Never heard of in industry. Close to being something unimaginable
2	Heard of in industry, but only extremely rarely and as the result of a chain of many unfortunate events
3	Incident has probably occurred in own company, but in the context of faulty equipment or by surprising mistakes made by people involved
4	Happens occasionally in own company, typically in the context of faulty equipment or by mistakes by people involved (the kind of mistakes that tend to happen on board from time to time)
5	Happens frequently when undertaking the work in question

Figure 5 – Example of likelihood scale from an SMS.

In an ideal world, quantifying the likelihood would be substantiated by access to shipping-specific industry-wide threat intelligence based on identified threat activity targeting the sector and incident reports. Such threat intelligence is available from various sources, such as the International Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC) or nationally focused efforts including NORMA Cyber and France Cyber Maritime. These sources

can provide companies with the situational awareness eg which threat actors are actively targeting the sector, threat indicators of current campaigns, vulnerabilities being targeted, etc. that is needed to help determine the likelihood of a cyber-attack as well as the potential impacts. Furthermore, it will often be worthwhile to look closer at the threat factors capability, opportunity and intent. Looking especially at intent can be useful, as zero intent will quantify a given potential threat as theoretical, and therefore produce only a small likelihood when juxtaposed against (or multiplied with) the vulnerability.

5 Impact assessment

5.1 The CIA model

The confidentiality, integrity and availability (CIA) model[9] provides a framework for assessing the impact of:

- Loss of confidentiality of information, eg unauthorised access to and disclosure of systems, information or data about the ship, crew, cargo and passengers
- Loss of integrity, which would modify systems, information and data relating to the safe and efficient operation and management of the ship
- 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 depends on the use of the systems, information or data and whether one is focused more on IT or OT systems. IT systems typically place more importance on confidentiality. Conversely, assessing the impact to OT systems onboard ships, particularly safety critical systems, may focus on availability and/or integrity instead of confidentiality.

5.2 Quantifying the impact

An SMS will normally contain a risk assessment matrix, where the impact of a given event is measured on a five-step scale of increasingly serious impacts to different categories eg safety of personnel, safety of environment, cargo safety, asset safety, business continuity, financial impact and company's reputation. Using the SMS's existing impact scale to describe cyber-related risks will ease the understanding throughout the company. Similarly, if the company uses a business impact analysis (BIA) model, that too could be applied and should be easily adoptable by the various business units. If either model has not been used to describe impacts arising out of cyber risks, it will be necessary to modify the verbal description of each of the impact levels. Using such a scale, also allows the company to distinguish between different ships in the fleet according to their criticality to the company's overall activities. An example of such a scale can be found below:

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

Level	Impact description
1	No health effect/injuries. No damage to operations, environment, assets, finances or company's reputation
2	Very slight health effect/injuries. Very slight damage to operations, environment, assets, finances or to company's reputation
3	Some health effect/minor injuries. Minor damage to operations, environment, assets, finances or to company's reputation
4	Major health effect/relatively serious injuries. Local but major damage to operations, environment, assets, finances or to company's reputation
5	Fatality or permanent disabilities. Widespread, significant damage to operations, environment, assets, finances or company's reputation.

Figure 6 – Example of an SMS's verbal description of impact levels.

There are also several other assessment methodologies that can help define the magnitude of the impact from a cyber incident, for example below:[10]

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, organisational assets or individuals	A **limited** adverse effect means that a security breach might: (i) result in minor harm to individuals; (ii) result in minor financial loss; (iii) result in minor damage to organisational assets; or (iv) cause a degradation in ship operation to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced.
Moderate	The loss of confidentiality, integrity or availability could be expected to have a **substantial** adverse effect on company and ship, assets or individuals	A **substantial** adverse effect means that a security breach might: (i) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries; (ii) result in significant financial loss; (iii) result in significant damage to organisational assets; or (iv) cause a significant degradation in ship operation to an extent and duration that the organisation is able to perform its

[10] Methodologies include, and are not limited to, ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management, COSO Enterprise Risk Management Framework, and ISO 31000:2018 Risk management – Guidelines.

		primary functions, but the effectiveness of the functions is significantly reduced.
High	The loss of confidentiality, integrity or availability could be expected to have a **severe or catastrophic** adverse effect on company and ship operations, assets, environment or individuals.	A **severe or catastrophic** adverse effect means that a security breach might: (i) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries; (ii) result in major financial loss; (iii) result in major damage to environment and/or organisational assets; or (iv) cause a severe degradation in or loss of ship operation to an extent and duration that the organisation is not able to perform one or more of its primary functions.

Figure 7 – Potential impact levels when using the CIA model.

5.3 "Critical" equipment and technical systems

The impact assessment should be carried out for every system on board. For OT systems, such an impact assessment also forms part of the list of equipment and technical systems, the sudden operational failure of which may more or less promptly result in hazardous situations, which is required by paragraph 10.4 of the ISM Code (often referred to as "critical" equipment and technical systems).

The potential impact for IT systems should also be assessed and will normally require input from the primary users, and depending on the functionality of the system this could be eg stowage staff, operations staff, commercial and finance staff etc. Consequences of a degrading or loss of IT systems can be very disruptive to the ship's operations, regulatory compliance and even safety performance and should not be underestimated.

EXAMPLE

A ship is equipped with a complex power management system. It consists of switchboards and generators controlling systems for auto load sharing, power control and auto synchronizing. On top of the power management system, a supervisory control and data acquisition (SCADA) system provides output and makes it possible for the crew to control the distribution of onboard electric power.

Power management is important to the safety of the crew, ship and cargo. It also has a clear environmental and financial impact as power is generated by use of fuel either by the ship's main engine (shaft generator) and/or auxiliary engines. Therefore, a cyber incident that disables or causes the power management system to malfunction can place the operation and safety of the ship at risk. To lower the risk, the company should add protection measures that minimize the possibility of such a cyber incident taking place.

The SCADA 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 potential impact of data and information is being breached, the CIA model should be used. When doing so, the shipping company should determine the potential impact of the most sensitive information stored, processed or transmitted by the SCADA system.

Using the CIA model, the shipping company can conclude that:

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 potential high impact from a loss of integrity. It will also be a safety issue if the information cannot be read. So, there is a potential high impact from a loss of availability.

a loss of confidentiality regarding the power consumption information being sent to the shipping company for statistical purposes is assessed as a potential low impact. There will also be a potential low impact from a loss of integrity and availability as the data is only used for non-critical, in-house considerations.

The following figure shows the result of the assessment:

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

Figure 8 – Result of CIA assessment of SCADA system.

6 Risk assessment

6.1 Relationship between factors influencing risk

Only after having established an overview of threats (intent, capability and opportunity), vulnerabilities, impacts and likelihood, is it then possible to conduct the risk assessment. A risk assessment is not a one-off activity but part of a ongoing, proactive approach to risk management which entails regularly reassessing risks and implementing appropriate and up-to-date mitigation measures.

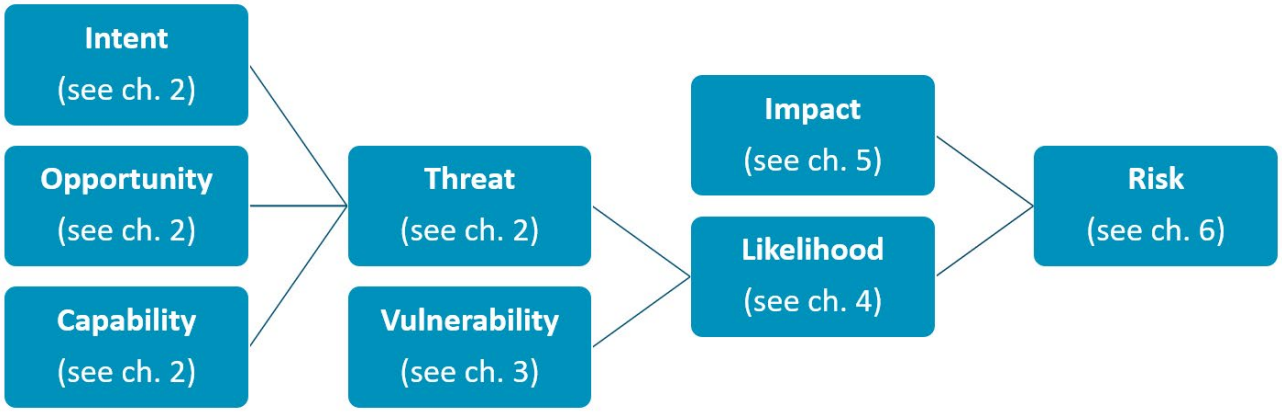

Figure 9 – The relationship between different factors influencing the risk. The lines represent multiplication, ie "Likelihood" is multiplied with "Impact" to produce "Risk".

6.2 The four phases of a risk assessment

Phase 1: Pre-assessment activities

Risk assessments apply to existing ships, newbuilds and second-hand ships, and second-hand ships entering the fleet should be given additional attention. Assessment of cyber risks is a complex undertaking, which requires detailed knowledge about cyber risk management, and third-party support to the risk assessment process is likely to be required.

Prior to starting a cyber risk assessment on board, the following activities should be performed:

- Review the documentation of IT and OT systems as described in 3.2 and assess potential impact levels, for example using the CIA model (see 5.1.).
- Identify main manufacturers of critical shipboard IT and OT equipment (a risk-based approach should be used in this identification process).
- Identify cyber security points-of-contact with the most important manufacturers and establish a working relationship with them.

- Review detailed documentation on the ship's maintenance and support of the IT and OT systems.
- Establish contractual requirements and obligations that the shipowner/ship operator may have for maintenance and support of shipboard networks and equipment.

Phase 2: Ship assessment

When all risk factors (threats, vulnerabilities, likelihood and impact) are assessed, the risk assessment and associated risk mitigation can be carried out. The risk assessment is a systematic consideration of relevant risk factors.

The risk assessment is carried out system by system and is therefore based on the system documentation described in 5.2. To be accurate, the risk assessment relies on knowledge of the functionality of the systems, data flows to and from the system, and precisely how each system is connected to other systems either by cable or wireless connection. For the same reason, the risk assessment will most likely require input from a broad range of company staff, equipment makers and external cyber security experts, when appropriate. Every connection is a potential vulnerability. For example, a connection to an internet accessible shared network printer entails a risk that cyber criminals can use the printer as a gateway to other systems connected to the printer.

The identification and implementation of mitigation measures based on risk assessments is well established on all ships via the ISM code and the company SMS. However, cyber risk assessments should not be confused with the operational risk assessments normally carried out by the crew as per the SMS. Cyber risk assessments require different knowledge and experience sets that will quite likely require the involvement of office staff and possibly even third-party consultants depending on the level of complexity.

To calculate the risk for a given system, the likelihood and the impact should be assessed.

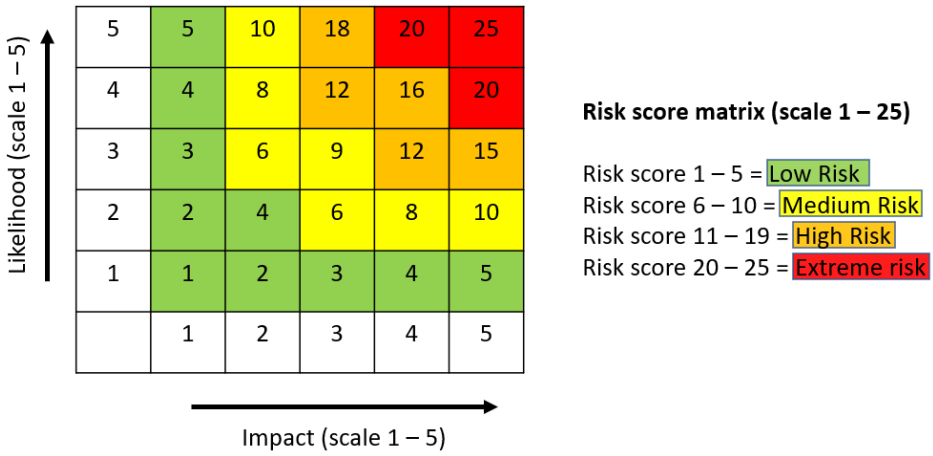

Figure 10 – Example of a company's risk score matrix.

If the calculated initial risk for a given system is above what is acceptable in accordance with the company's risk acceptance criteria, the risk must be mitigated for the residual risk to reach an acceptable level (as demonstrated in the example below):

System	Impact	Likelihood	Initial Risk	Mitigation	Residual risk
ECDIS	Score 5 due to risk of catastrophic events like grounding and collision	Score 4 due to active USB ports, computer used for other purposes, connection to admin network for access to shared printer, connection to automatic chart updates via satellite via trusted vendor	Risk = 5 x 4 = 20	Password protect and restrict PC use to ECDIS only	Risk = 5 x 3 = 15
				Disconnect from admin network	Risk = 5 x 2 = 10
				Blind off USB ports	Risk = 5 x 1 = 5

Figure 11 – Example of risk assessment and identification of mitigation measures.

Although carried out system by system, the risk assessment for the ship will require a holistic approach cognisant of the fact that some potential risk mitigation measures suggested for one system may impact on the risk assessment of other systems that are often connected and, of course, their cost-effectiveness. Different risk mitigation measures are described in more detail in the subsequent chapters of the present guidelines.

The activities performed during an assessment could include reviewing the configuration of all computers, servers, routers and cyber security technologies including firewalls to ensure needed functionality and services are configured to the company standard. It could also include reviews of all available cyber security documentation and procedures for connected IT and OT systems and devices.

An aspect of the onboard ship assessment is the involvement of crew of all levels; particularly the Master, Chief Engineer and Chief Officer. This process assists them in understanding the implementation of the IT and OT systems onboard, and how they may vary from stated design documentation, and to understand the level of cyber training to be delivered to the ship's crew.

For obvious reasons selection of mitigation measures depends on the resources available and the nature of the risk. Some mitigation measures which can include eg procedural changes may be equally as effective as expensive technical solutions by reducing the likelihood, frequency or impact of events. Especially for existing ships with legacy systems, technical solutions can be difficult and expensive to implement.

Assessing the effectiveness of different risk mitigation measures should be an integral part of the risk assessment and change management processes.

It can also be considered when categorising different risk mitigation measures, so it becomes easier to understand and provide guidelines on which controls to use, and where.

Phase 3: Debrief and reporting

To satisfy the requirements of the ISM Code, the risk assessment should be a coherent and up-to-date document which reflect how risks are assessed and mitigated. Producing such a risk assessment will often be an iterative process where different mitigation measures are considered in different combinations, until a decision can be made to the optimal composition of the risk mitigation measured in terms of legal requirements, risk appetite, feasibility, effectiveness and cost.

If the risk assessment is carried out by an external party (eg if sufficient expertise is unavailable in-house) the initial report of the external party is likely to be an interim account of the risks, in which recommendations are made. Once recommendations have been considered and a final decision has been taken, this should be reflected in the final risk assessment.

An initial third-party cyber risk assessment could for example include the following:

- Executive summary – a high-level summary of results, recommendations and the overall security profile of the assessed ship
- Technical findings – breakdown of discovered vulnerabilities, their probability of exploitation, the monetary cost of exploitation, the resulting impact on the crew, ship and environment and appropriate technical fix and/or mitigation advice
- Prioritised list of actions – the priorities should reflect the effectiveness of the measure, the cost, the applicability, etc. It is important that this list includes a complete list of options available and not represent a list of services and products, which the third-party risk assessor, if applicable, would like to sell
- Supplementary data – a supplement document containing the technical details of all key findings and comprehensive analysis of critical flaws used to inform the report should be provided. This section should also include data recovered during the penetration testing, if any, of critical or high-risk vulnerabilities
- Appendices – record of activities conducted and tools used by the cyber risk assessment team.

Phase 4: Manufacturer's 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 manufacturers of the effected systems for them to provide a means of reducing or mitigating the risks. Any findings, eg any identified cyber vulnerability in the factory standard configuration of a critical system or component, could be further analysed with support from external experts, who should work with the manufacturer'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 manufacturer is comprehensive in nature and identifies the correct solution to eliminate the vulnerabilities.

6.3 Third party risk assessments

Depending on the capabilities of the company to perform accurate risk assessments, assistance by third parties can be considered.

Third party risk assessments can also include penetration tests of critical IT and OT infrastructure to identify whether the actual defence level matches the desired level set forth in the cyber security strategy for the company. Such tests can simulate incidents 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 potentially inserting software into a system. This may only be appropriate for IT systems or as part of a dry dock activities for OT systems where risks to the crew or vessel would be minimal. Alternatively, 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 should be made to actively access or insert software into the system.

Third party risk assessments are a valuable way of integrating specialized skills and field expertise to perform varying tasks in the overall effort of managing and remediating cyber risk. These assessments can also be beneficial to companies with limited personnel resources to perform objective and transparent cyber risk assessments. Choosing third parties to assist in these activities also allows stakeholders to learn from multiple perspectives and perform due diligence, empowering them to make informed and confident choices.

While penetration testing has been viewed as a way of determining if networks and software systems can be compromised, there are numerous other ways of building the foundation of understanding of one's own organisation's and fleet's environments that can also be performed. These services could include asset discovery and inventory on networks to assist shipowners and operators with understanding what is connected, where and with whom. Third parties may also perform network architecture reviews and design to understand and audit current design as well as spot where improvements can be made in cost effective and sensible ways. Vulnerability assessments can be performed as a deeper dive and a broader look, to even include passive network scanning. Regardless of the service, it is important for the supervising officers and shoreside staff to coordinate these activities for safety purposes, and to choose third party services with fleet awareness, competency and experience.

7 Develop protection measures

7.1 Defence in depth and in breadth

Defence in depth

It is important to protect critical systems and data with multiple layers of protection measures, which combine the role of personnel, procedures and technology to:

- Increase the probability that a cyber incident is detected
- Make the best use of resources required to protect confidentiality, integrity and availability of data in IT and OT systems
- Institute system level measures that further isolate and secure systems against unauthorized use.

Connected OT systems on board should require more than one technical and/or procedural protection measure. Perimeter defences such as firewalls are important for preventing unwelcomed entry into the systems, but this may not be sufficient to cope with insider threats.

This defence in depth approach encourages a combination of:

- Physical security of the ship in accordance with the ship security plan (SSP)
- Protection of networks, including effective segmentation
- Intrusion detection
- Use of firewalls
- Periodic vulnerability scanning and testing
- Software patching/updating and software whitelisting
- Access and user controls
- Configuration and change management controls
- Appropriate procedures regarding the use of removable media and password policies
- Personnel's cyber security awareness and understanding of the risk to themselves and the industry
- Understanding and familiarity with appropriate procedures, including incident response.

Company policies and procedures should help 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 incidents.

Defence in breadth

When developing integration between systems, either zero trust or a trust boundary model should be considered, whereby systems are grouped into those between which trust is implicit (for example user workstations), and those between which trust should be explicit (between bridge computers and corporate networks). For large or complex networks, threat modelling should be considered as an activity to understand where technical controls should be implemented between systems in order to support a defence in breadth approach.

However, onboard ships where levels of integration between IT and OT 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. Therefore, "defence in breadth" is used to prevent any vulnerabilities in one system being used to circumvent protection measures of another system.

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

Implementation of cyber security controls should be prioritised, focusing first on those measures, or combinations of measures, which offer the greatest benefit. Of course, all systems can be protected but, in some cases, the outlay in time and money is far greater than the risk of infection itself.

7.2 Technical protection measures

Cyber risk protection measures are often technical and focused on ensuring that onboard systems are designed and configured to be resilient to cyber incidents. Consideration needs to be given to implementing technical controls that are practical and cost effective, particularly on existing ships. It should be noted that implementation of technical control measures is not a one-off activity, they must be kept up to date to avoid risk of failure.

The Centre for Internet Security (CIS) provides guidance on measures[11] that can be used to address cyber security vulnerabilities. The protection measures are a list of Critical Security Controls (CSC) that are prioritised and vetted to help ensure that they provide an effective approach for companies to assess and improve their defences. The CSCs include both technical and procedural aspects.

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

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

[12] Stephenson Harwood (2015), Cyber Risk.

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 helps ensure that only appropriate traffic will be allowed via a controlled network or subnet, based on the control policy of that network or subnet.

The most common attacks are generally against host systems such as web servers, mail servers, file and printer servers, workstations, etc. and organisations should ensure that only those ports, protocols and services with a valid business requirement are open/running on each system. It is recommended that only managed routers be used and secured by disabling unused ports, protocols and services to reduce unauthorised access to systems or data.

Configuration of network devices such as firewalls, routers and switches

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

- Networks that are critical to the operation of a ship itself, should be controlled. It is important that these systems have a high level of security.
- Networks that provide suppliers with remote access to navigation and other OT systems' software on board, should also be controlled. It may be necessary to allow suppliers to upload system upgrades or perform remote servicing on these networks. Shoreside external access points of such connections should be secured to prevent unauthorised access.
- Cargo stowage, load planning and cargo and container management systems should be controlled. So, should those systems that perform mandatory ship reporting to public authorities.
- 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.

Effective segregation of systems/zones, based on necessary access and trust levels, is one of the most successful strategies for the prevention of cyber incidents. Effectively segregating networks can significantly impede an attacker's access to a ship's systems and is one of the most effective techniques for preventing the spread of malware. Onboard networks should be partitioned by firewalls to create trusted zones. Firewall configurations should be reviewed regularly to detect unauthorised changes. 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 3 of these guidelines for more information on shipboard networks and also refer to ISO/IEC 62443 as well as IACS Recommendation no. 166 on Cyber Resilience.

[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.

INCIDENT: WORM INCIDENT ON MARITIME IT AND OT

A ship was equipped with a power management system that could be connected to the internet for software updates and patching, remote diagnostics, data collection and remote operation. The ship was built recently, but this system was not connected to the internet by design.

The company's IT department made the decision to visit the ship and perform vulnerability scans to determine if the system had evidence of infection and to determine if it was safe to connect. The team discovered a dormant worm that could have activated itself once the system was connected to the internet and this would have had severe consequences. The incident emphasizes that even air gapped systems can be compromised and underlines the value of proactive cyber risk management.

The shipowner advised the manufacturer about the discovery and requested procedures on how to erase the worm. The shipowner stated that before the discovery, a service technician had been aboard the ship. It was believed that the infection could potentially have been caused by the technician.

The worm spread via USB devices into a running process, which executes a programme into the memory. This programme was designed to communicate with its command and control server to receive its next set of instructions. It could even create files and folders.

The company asked cyber security professionals to conduct forensic analysis and remediation. It was determined that all servers associated with the equipment were infected and that the virus had been in the system undiscovered for 875 days. Scanning tools removed the virus. An analysis proved that the service provider was indeed the source and that the worm had introduced the malware into the ship's system via a USB flash drive during a software installation.

Analysis also proved that this worm operated in the system memory and actively called out to the internet from the server. Since the worm was loaded into memory, it could affect the performance of the server and systems connected to the internet.

Physical security

Physical security[14] is sometimes the simplest, cheapest and most obvious form of cyber defence. It is a central aspect of cyber risk management and an effective defence in depth strategy should aim to ensure that physical control measures cannot be circumvented. Areas containing sensitive OT or IT control components should be securely locked. Security and safety critical equipment and cable runs should be protected from unauthorised access, and physical access to sensitive user equipment (such as exposed USB ports on bridge systems) should be secured. In the Ship Security Plan such areas will be defined as Restricted Areas as required by the ISPS Code Part A section 9.4.1 considering the guidance in the Code's part B. This is particularly relevant to places that are normally unmanned in port, such as the bridge.

[14] See also the ISPS Code.

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.
A satellite terminal normally has an unprotected LAN port for connection to the ship's networks, which leaves different options open for protection depending on the threat.

Protection against eavesdropping when unencrypted device communications is used is typically done by means of Virtual Private Network (VPN) connection or encrypted protocols. While protection against hacking, piercing and other types of attack can be achieved by other means such as a security arrangement with the service provider, connection through a secure server ashore owned by the company, or an onboard firewall.

One important aspect of cyber security is to make the satellite terminal invisible. This can be achieved by deactivating functions such as the "remote administration page" and "port forwarding" in the terminal settings menu. Deactivation can typically be done in the terminal's settings menu.

When establishing a connection for a ship's navigation and control systems to shore-based service providers, consideration should be given on how to prevent illegitimate connections gaining access to the onboard systems. It is advised that an IP address should not be published and routable (ie public) directly to a ship from the internet. Connections from the internet should route through a shoreside network and firewall for routing and access control. A second consideration is the close monitoring of outbound connections originating from ship networks, control networks or networks that have a connection to control networks (ie reverse tunnel connections).

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 onboard. At the access point for this traffic, it is necessary to provide data security, firewalling and a dedicated "last-mile" connection.

When using a VPN, the data traffic should be encrypted to the highest allowable international standard. Furthermore, a firewall in front of the servers and computers connected to the networks (ashore and 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. Both onshore filtering of traffic and firewalls/security inspection/blocking gateways on the ship are needed and supplement each other to achieve a sufficient level of protection.

Manufacturers 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. Examples of protection of administrative interfaces include limiting networks that can access such interfaces through whitelisting whether they are web-based or command line or entirely disabling

unnecessary interfaces that are only used during initial configuration. As for other systems, the passwords should be managed appropriately eg default passwords, which are often well-known to criminals, should be changed. Multi-factor authentication can also be leveraged to further enhance security.

Wireless access control

Wireless access to networks on the ship should be limited to appropriate authorised devices and secured using a strong encryption key, which is changed regularly. The following should be considered for controlling wireless access:

- The use of enterprise authentication systems using asymmetric encryption and isolating networks with appropriate wireless dedicated access points (eg guest networks isolated from administrative networks)
- The adoption of systems, such as wireless intrusion prevention system (WIPS), that can intercept non-authorized wireless access points or rogue devices. Using network access control (NAC) to profile devices (corporate versus personal) and control wireless network access is effective at managing access
- The protection of the physical interconnection between wireless access devices and the network, such as network plugs, secured network racks, etc to avoid unauthorized access by rogue devices.

Secure configuration of hardware and software

All endpoints, to include servers, workstations, laptops and company issued mobile devices, used on ships should have secure baseline configurations for the operating system and other software before being placed into production status. Once in production, baseline configuration changes should follow a change management process, and regular patching of these systems as part of a vulnerability management program should occur. Having standardized baselines in place across a fleet of vessels makes it easier to monitor these systems and identify when suspicious or abnormal activity has occurred. User profiles should be restricted to only allow computers, workstations or servers to be used for the purposes for which they are required.

Control administrative privileges

User profiles should leverage the principles of least privilege to limit what activities the user is allowed to take and not allow the user to alter the systems or install and execute new programmes. The use of administrative accounts should be limited to key personnel and normal user privileges should be limited so that if an attacker compromises an account, the actions they can take with those credentials are more limited.

Email and web browser protection

Any email and web browser protection should:

- Protect shoreside and onboard personnel from potential social engineering, eg phishing attacks
- Help prevent email being used as a method of obtaining sensitive information
- Ensure that the exchange of sensitive information via email or by voice is appropriately protected to ensure confidentiality and integrity of data, eg encryption protection
- Prevent web browsers and email clients from executing malicious scripts.

Some best practices for safe email transfer are encrypting emails and files when necessary, disabling hyperlinks, avoiding using generic email addresses and ensuring the system has configured user accounts.

In addition, implementing Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication Reporting and Conformance (DMARC) security controls helps authenticate the validity of emails and protect against phishing attacks. Companies should also consider leveraging email security focused tools and services that can further protect against phishing attacks.

There are several security controls that can be easily implemented for the web browsers on ship systems that have legitimate requirements to reach the internet. First, browsers can easily be configured to a more secure setting to limit features and create a more secure environment. This includes blocking pop-up windows and plugins, disabling JavaScript and cookies and isolating the browser processes to run in a sandbox environment. Additionally, browsers should be regularly patched as part of the other software vulnerability management efforts for the onboard computers.

Phishing: The most commonly reported cyber-attack

Because it is an inexpensive, easy to conduct and low risk effort, phishing is the most common cyber-attack used by a wide range of the attackers outlined previously. In addition to the phishing campaigns that many critical infrastructure stakeholders receive that include subjects related to online shopping sales, prizes being awarded or impersonating requirements for account validation (eg Microsoft, Amazon, etc accounts), there are also frequent phishing campaigns that target the maritime industry. A common campaign theme is to impersonate port state control in an email to the Master or ship officers, or the inverse where an email to shoreside personnel spoofs the ship's crew as the sender. This highlights the need for email security to be a focus for every company.

Application software security (patch management)

Security updates should be provided to onboard systems and it is recommended to develop a software and hardware patching plan. Security patches should be included in the periodic maintenance cycle, and it is recommended to pay special attention to equipment utilized to do virtual network segregation (VLAN) and firewalling. These updates or patches should be applied

only by authorised personnel and in a timely manner to ensure that any vulnerabilities in a system are addressed before they are exploited and available to hackers. Patching of the IT systems onboard the ship should be a regular, eg monthly, practice.

It can be complicated and expensive to patch some OT systems, because all software and hardware firmware needs to be aligned and thorough tests must be conducted post installation to validate the integrity, and class may need to certify the systems afterwards. In other cases, security patches may not be applicable without upgrading system hardware partly or completely. For those reasons, OT systems are not updated so frequently or not at all. And it is important to assess the compatibility and potential operational impact on the OT systems prior to any patches being installed. If a critical patch cannot be installed, alternative measures should be evaluated to ensure the vulnerabilities are not exposed in larger IT networks or ultimately to the internet. This could be a combination of physical protection, limiting network access and implementation of virtual patching techniques.

7.3 Procedural protection measures

Protection measures may also be procedural and should be covered by company policies, safety management procedures, security procedures and access controls. As with all other control measures, only procedural controls that are practical and cost effective should be implemented. Procedural controls are focused on how personnel use the onboard systems. Plans and procedures that contain security sensitive information (for example vulnerability assessments, analysis/decisions made from information gained from assessments, physical and operational security plans, proprietary information, etc) should be kept confidential and handled according to company policies. Examples for procedural actions can be:

Training and awareness

Training and awareness are the key supporting elements to an effective approach to cyber risk management as described in these guidelines.

The internal cyber threat should be considered. 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, loading, stowage and operation of the ship.

The STCW Convention[15] requires companies to ensure that seafarers are familiarized with *"[…] all ship arrangements, installations, equipment, procedures and ships characteristics that are relevant*

[15] The International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers, 1978, as amended.

to their routine or emergency duties;" and that *"[…] the ship's compliment can effectively coordinate their activities in an emergency situation and in performing functions vital to safety or to the protection or mitigation of pollution."* The managing, as appropriate, of cyber risks fall within the scope of the STCW convention.

In addition to the familiarization training of seafarers required by the STCW convention, an awareness programme should be in place for all onboard personnel according to their role, covering for example some of 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 or opens a malicious attachment. One way of training this aspect is through specially crafted campaigns including phishing simulation tests, which is a proven method of increasing awareness and stimulate level of commitment
- 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 geolocation data for personnel and the ship that is publicly available
- Risks related to the use of personal 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 a possible cyber incident. Examples of this are systems randomly rebooting, 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
- Training and familiarization on how to handle remote maintenance sessions on OT equipment and associated risks and impact.

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, relevant personnel should be aware of 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 programmes, including failure to run correctly or programmes 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.

Designated personnel should be able to understand reports from Intrusion Detection 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.

To reinforce user awareness training and procedures, cyber security focused scenarios should be incorporated with security drills and exercises. The Master and senior officers should be able to demonstrate proficiency in understanding how to properly respond to a cyber incident onboard the ship, and drills and exercises help to reinforce and improve this proficiency.

These 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 advisable for owners and operators to ascertain the status of cyber security preparedness of their third-party providers, including marine terminals and stevedores, as part of their sourcing procedures for such services.

Computer access for visitors

Visitors such as authorities, technicians, agents, port and terminal officials, and owner representatives should be restricted regarding computer access whilst on board. Unauthorised access to sensitive computers should be prohibited. If access to a network by a visitor is required and allowed, then it should be restricted in terms of user privileges and conducted under supervision. 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 isolated from all controlled networks, should be used. Where possible a Wi-Fi Direct or Wireless Direct enabled printer can be provided for document printing. Wi-Fi Direct or Wireless Direct allows the printer to behave as an access point so the mobile device or PC connects directly without a Wi-Fi access point/router. To avoid unauthorised access, removable media blockers should be used on all other physically accessible computers and network ports.

INCIDENT: BUNKER SURVEYOR'S ACCESS TO A SHIP'S ADMINISTRATIVE NETWORK

A dry bulk ship in port had just completed bunkering operations. The bunker surveyor boarded the ship and requested permission to access a computer in the engine control room to print documents for signature. The surveyor inserted a USB drive into the computer and unwittingly introduced malware onto the ship's administrative network. The malware went undetected until a cyber assessment was conducted on the ship later, and after the crew had reported a "computer issue" affecting the business networks.

This emphasises the need for procedures to prevent or restrict the use of USB devices onboard, including those belonging to visitors.

Crew's personal devices

Procedures must be in place to provide instructions to crew about the use of IT devices for personal and leisure purposes. This should include how to utilise the ship's communication networks for personal means such as audio/visual communications services, social media, emails, gaming, video streaming without endangering critical IT or OT systems.

Upgrades and software maintenance

Hardware or software that is no longer supported by its manufacturer 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 help maintain a sufficient level of security. Procedures for timely updating of software may need to be put in place considering the ship type, speed of internet connectivity, sea time, etc. Software includes computer operating systems, which should also be kept up to date. Additionally, routers, switches and firewalls, and various OT devices will be running their own firmware, which may require regular updates that 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[16] to help 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.

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

Anti-virus and anti-malware tool management

Scanning software tools used to detect and deal with malware, should be kept up to date and managed. 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.

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, and when-, how- and what they can access. Remote access should also be done via established and secure means, such as through VPN connection and be explicitly approved by security. Any procedures for remote access should include close co-ordination with the ship's Master and other key senior ship personnel. Furthermore, a risk assessment should be performed including identification of fall-back options in case remote maintenance is not successful.

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.

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 onto systems with administrator privileges may enable existing vulnerabilities to be more easily exploited. Administrator privileges should only be given to appropriately trained personnel, who as part of their role in the company or onboard, need to log onto systems using these privileges. In any case, use of administrator privileges should always be limited to functions requiring such access.

Ideally, user privileges should be removed when the person concerned is no longer onboard. 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 users change roles 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 full access to systems.

Multi/factor authentication (MFA) and passwords

To protect access to confidential data and safety critical systems, a robust password policy in conjunction with MFA should be developed[17]. MFA should be used as widely as reasonably possible, ie for all appropriate levels. To reduce the chances of a brute force attack, passwords[18] should be strong and can be either user or machine generated. The company policy should address the fact that over complicated passwords that are difficult to remember, which must be changed too frequently, are at risk of being written on a piece of paper and kept near the computer.

It is recommended eg, to use passphrases, which is a sequence of mixed words, that are easier to remember than complex passwords. Passwords or passphrases on administrative systems should be supplemented with the use of MFA, which is based on something that you have, eg a token, or device, and something that you know, eg a password and something "you are", eg a fingerprint passcode on a phone. Where MFA is implemented, the risk of a breach is greatly reduced, as the token or device will not be in the possession of the threat actor, who manages to obtain the password. A warning should be included so as seafarers and office personnel to be reminded that systems' passwords shall never been posted in public areas.

INCIDENT: MAIN APPLICATION SERVER INFECTED BY RANSOMWARE

A ransomware infection on the main application server of the ship caused complete disruption of the IT infrastructure. The ransomware encrypted every critical file on the server and as a result, sensitive data was lost, and applications needed for ship's administrative operations were unusable. The incident was reoccurring even after complete restoration of the application server.

The root cause of the infection was poor password policy that allowed attackers to successfully brute force remote management services. The company's IT department deactivated the undocumented user and enforced a strong password policy on the ship's systems to remediate the incident.

Physical and removable media controls

When transferring data from uncontrolled systems to controlled systems, there is a risk of introducing malware. Removable media can be used to bypass layers of defences and attack systems that are otherwise not connected to the internet. A clear policy for the use of such media devices is important. The policy must help ensure that media devices are not normally used to transfer information between uncontrolled 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 check

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

[18] https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

removable media for malware and/or validate 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. 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 files for example:

- Cargo files and loading plans, eg container ship BAPLIE files
- National, customs and port authority forms
- Bunkering and lubrication oil forms
- Ship's stores and provisions list
- Software update files
- Engineering maintenance files.

This list represents examples and should not be seen as exhaustive. Wherever possible, the files and forms should be transferred electronically or be downloaded directly from a trusted source without using removable media.

Equipment disposal including data destruction

Obsolete equipment can contain data, which is commercially sensitive or confidential. Prior to disposal of the equipment, the company should have a procedure in place to ensure that the data held in obsolete equipment is properly destroyed and cannot be retrieved, eg by means of a degaussing tool in accordance with manufacturer's instructions.

8 Develop detection measures

8.1 Detection, logging, blocking and alerts

Detecting intrusions and infections is a central part of cyber risk management. A baseline of system, application, account and network operations and expected data flows for users and systems should be established and managed, so that cyber incident alert thresholds can be established. This requires the collection and normalization of multiple log sources from onboard the ship. Key to this will be the definition of roles and responsibilities for detection to help ensure accountability. A dedicated Security Information and Event Management (SIEM) system should be considered. SIEM systems collect logs from every possible source, parse them and correlate them in a manner that suspicious activities can be detected that would otherwise go unnoticed. Effective deployment of SIEM systems is a complex undertaking and is offered as a service by some cyber security providers.

Additionally, a company may choose to incorporate an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS) into the network, as part of a vessel communications solution, 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 3 of these guidelines. Relevant onboard or shoreside personnel should be able to understand the alerts and their implications and carry out the agreed response and recovery activities. Knowledge of incidents detected should be directed to an individual or service provider, who is responsible for acting on this type of alert.

8.2 Malware detection

Endpoint protection and scanning software that can automatically detect and address the presence of malware in systems onboard should be kept up to date and managed.

As a general guideline, computers on board 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 and work-related computers and devices onboard. This will reduce the risk of these computers acting as attack vectors towards servers and other computers on the ship's network. How regularly the scanning software will be updated must be taken into consideration when deciding whether to rely on these defence methods.

9 Establish contingency plans

A response plan should be developed covering relevant contingencies, and all plans should be kept in hard copy in the event of complete loss of electronic access to them. When developing contingency plans for implementation onboard ships, it is important to understand the significance of any cyber incident as a safety matter and prioritise response actions accordingly. This can only be accomplished together with a team from shoreside management.

Any cyber incident should be assessed to estimate the impact on operations, assets etc. In most cases, and with the exception of load planning and management systems, a loss of IT systems on board, including a data breach of confidential information, will be a security issue and would normally not have immediate, significant impact on the safe operation of the ship. In the event of a cyber incident affecting IT systems only, the priority may be to notify designated persons within the shipowner or operating company for immediate response, and the immediate implementation of an investigation and recovery plan. These designated personnel should be available to the Master in the event of such an incident.

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 help ensure the immediate safety of the crew, ship, cargo 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 the relevant operational and emergency procedures included in the SMS. Ideally, some of the existing procedures in the ship's SMS will already cover such cyber incidents. However, cyber incidents may result in multiple failures causing more systems to shut down at the same time. The contingency planning should take such incidents into consideration.

The following is a sample non-exhaustive list of cyber incidents, which should be addressed in plans for onboard contingencies. Arguably, most of these incidents are probably already addressed in the company's procedures for dealing with shipboard emergencies as required by the ISM Code's chapter 8 (Emergency preparedness).

- Loss of availability of electronic navigational equipment or loss of integrity of navigation related data
- Loss of availability or integrity of external data sources, including but not limited to GNSS
- Loss of essential connectivity with the shore, including but not limited to the availability of Global Maritime Distress and Safety System (GMDSS) communications
- 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
- The event of a ransomware or denial of service incident.

Furthermore, it is important to help ensure that a loss of equipment or reliable information due to a cyber incident does not make existing emergency plans and procedures ineffective. Contingency

plans and related information should include communications and escalation management to ensure that the correct shore-based support can be accessed, and should be available in a non-electronic form as some types of cyber incidents can include the deletion of data and shutdown of communication links.

Contingency plans should be carefully designed, and simple and designated personnel ashore should be integrated with the ship in the event of a cyber incident. The Master and designated officers should be provided with this plan to enable training and periodic review for familiarity.

Disconnecting OT from shore network connection

Connections between shore and OT systems can be relevant in a wide range of applications like performance monitoring, predictive maintenance and remote support just to mention a few. Common for these systems are that they are not strictly necessary for operating the ship safely. However, they represent a potential attack vector to the systems that are needed for the ship's safe operation. Therefore, it is relevant to assess when these connections are allowed and under what circumstances. Plans should be established specifying when such OT systems should be temporarily separated from the shore network connection to protect the ship's safe operation or prevent a shipside infection from reaching shoreside systems. Disconnecting will help prevent the attacker from being able to manipulate safety critical systems or take direct control of the system or spread back to the shore and potentially back out to other ships. Disconnecting could also take place to avoid malware spreading between network segments.

To effectively shut down shore connections, it is important to have the network and connectivity services designed and documented in a way (eg a list or drawing clearly showing such cables, switches/firewalls) that the networks can be physically isolated quickly by removing a single network cable (eg marked in an odd colour) or powering off the firewall. This design and procedure should be provided by the responsible shoreside staff to the Master. Training should also be provided to aid the Master and officers with understanding cyber threats. The crew should also be trained to operate the ship should there be a disconnection of OT. These impacts should be known in advance, tested and procedures developed for each ship.

10 Respond to and recover from cyber security incidents

10.1 Effective response

The starting point for effective response is the response plan covering relevant contingencies. However, it is unlikely that response plans will eventually match a cyber incident scenario as it unfolds, which is why the incident response plans (IRP) should be supplemented with specific playbooks for eg malware, data leaks, denial of service or system unavailability, etc based on likely to be encountered scenarios. This is why it is important to regularly drill the response plan and playbooks and develop contingencies according to lessons learned about the threats, vulnerabilities and impacts. For ships, the contingency shall already be in place in the emergency procedures required by the ISM Code 1.4.5.

Cyber incidents will require an active response to return the ship to operation. If for example, the ECDIS has been infected with malware, starting the backup ECDIS may cause another cyber incident. It is, therefore, recommended to build and rehearse an incident response plan, detailing roles and responsibilities, communications paths and core activities.

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 addition, the insurer may require that the company use an external services provider as part of the incident response. In these cases, external expert assistance should be available to assist with multiple functions, such as network activity, anomalous behaviour of connected devices or the detection of non-inventoried devices, unauthorized or uncoordinated accesses by vendors to critical systems, and aspects of response and recovery (such as post event forensic analysis and clean-up).

To the extent available, knowledge about previously identified cyber incidents (in own fleet as well as in other fleets) 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.

10.2 The four phases of incident response

As determined by NIST, there are four key phases to incident response:

1. Preparation
2. Detection and analysis
3. Containment and eradication
4. Post-incident recovery.

Phase 1, Preparation:

In accordance with previous advice in this guidance:

- Identify roles and responsibilities of personnel
- Determine the critical components on the ship, their prioritization and location
- Ensure regular back-up as appropriate of all relevant data
- Identify single points of failure and define contingencies as necessary
- Create an incident response plan and rehearse it regularly. The plan should include the roles and responsibilities of crew and personnel ashore as well as guidance on clear communication. The plan should also detail critical network and data recovery processes, as necessary.

Phase 2, Detection and Analysis:

Monitoring of the ship's IT, OT and IoT environments is fundamental to early detection of a cyber security event and is the only consistent way to proactively identify the early signs of a cyber incident. For example, by identifying that a system onboard is trying to communicate with an attacker's command and control server to initiate a malware download. Otherwise, organisations will often only identify a cyber incident after the impact has become known, as in the previous example where ECDIS is no longer working. As such, it is important that a variety of logs from the ship are actively collected and monitored for signs of a security event, including:

- Suspicious activity or unauthorized access to systems, data and/or networks
- Suspicious activity or unauthorized or inappropriate use of systems, networks or accounts
- Failure to follow management of change or other security procedures
- Loss or disruption to the availability of critical systems or data.

To help ensure an appropriate response, the response team should perform triage on the detected security events to find out wherever possible:

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

Phase 3, Containment and Eradication:

Containing the outbreak of an incident is a time-critical exercise. Based on the established playbooks, the organisation can then systematically and effectively work to contain the situation. Based upon the IRP and playbooks, this may require where possible, removing the device from the network. Where this is not possible, then it is important to quarantine the device from its VLAN or LAN and to ensure that boundary controls are operational between networks. Furthermore, the IRP and playbooks should include steps to:

- Check the firewall rules have not changed. A sophisticated attacker can open up network ports. Where systems are internet / VSAT facing, consider shutting down remote access management ports.
- Ensure that anti-virus and anti-malware definitions are up to date.

- Take a full disk image of any impacted systems. Store this securely in accordance with the Chain of Custody for forensic investigation ashore. A chain of custody process involves the identification, labelling, recording, handling, transportation, access control and secure storage of the disk image.
- Consider taking memory dumps (RAM image) as this is important for forensics purposes. Note, that restarting or powering off a computer will destroy volatile data like RAM so expert advice should be considered when dealing with threat eradication.

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:

- Whether IT or OT systems should be shut down or kept running to protect data
- Whether certain ship communication links with the shore should be shut down and what the implications of such steps may be
- The appropriate use of any recovery tools provided in pre-installed security software.

Phase 4, Post-Incident Recovery:

After the incident is contained and remediation efforts are underway, there are additional steps which need to continue, including:

- 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 section 10.3.
- Investigate the incident: To understand the causes and consequences of a cyber incident, an investigation should be undertaken by the company, with support from an external expert, if appropriate. The information from the investigation will play a significant role in preventing a potential recurrence by determining the root cause of the incident. Investigations into cyber incidents are covered in section 10.5.
- 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.

It may be necessary to initiate the long-term recovery plan to return the ship to an operational state. When this is the case, the response team should be able to provide advice to the ship on:

- The extent to which the incident has compromised IT or OT systems beyond the capabilities of existing recovery plans
- The systems and networks that will need to be rebuilt and/or replaced in a layup or dry dock environment.

As explained in section 7.3, training and awareness are the key supporting elements to an effective approach to cyber risk management. It is therefore important for relevant personnel aboard ship and ashore to execute regular cyber security exercises.

10.3 Recovery plan

Recovery plans in hard copy onboard and ashore should be available to personnel responsible for cyber security and who are tasked with assisting in cyber incidents. The purpose of the plan, which should be a part of the organisation's overall business continuity plan, is to support the recovery of systems and data necessary to restore IT and OT to an operational state. To help ensure the safety of onboard personnel, the operation and navigation of the ship should be prioritised in the plan. The detail and complexity of a recovery plan will depend on the type of ship and the IT, OT and other systems installed onboard.

The incident response team should carefully consider the implications of recovery actions (such as wiping of drives), which may result in the destruction of evidence that could provide valuable information on the causes of an incident. Where appropriate, professional cyber incident response support should be obtained to assist in preservation of evidence whilst restoring operational capability.

As explained in section 7.2 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. Because ransomware and worms have historically also spread to backup appliances, the use of offline backups should also be considered.

Recovery of OT may be more complex especially if there are no backup systems available and may require assistance from ashore. Details of where this assistance is available and by whom, should be part of the recovery plan, for example by proceeding to a port to obtain assistance from a service engineer.

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.

Incident response plans, contingency plans and business continuity plans should all be complementary to each other and include roles and responsibilities across the company. It is important that companies often test their recovery procedures and the whole ship-to-shore collaboration on responding to a cyber incident.

10.4 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. Governance must be in place to keep backup images up to date and also to ensure they are functional. Essential information and software-adequate backup facilities should be available to help ensure recovery 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 regain navigational and operational capabilities quickly and safely after a cyber incident.

10.5 Investigating cyber incidents

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.

Where external support is required, the full disk image taken during the containment phase can be shared with the investigating team. By ensuring that the Chain of Custody has been securely maintained, any forensic evidence obtained will be permissible in court as the process demonstrates that evidence has not been tampered with. A best practice for incident response, especially when a significant incident has occurred, is to assume that a court case could materialise and legal evidence would then be required.

The information from an investigation can be used to improve the technical and procedural protection measures on board and ashore. It may also help the wider maritime industry with a better understanding of maritime cyber risks. Any investigation should result in[19]:

- A better understanding of the potential cyber risks facing the maritime industry both on board and ashore
- Identification of lessons learned, including improvements in training to increase awareness
- Updates to technical and procedural protection measures to prevent a recurrence.

10.6 Losses arising from a cyber incident

As cyber related risks become a part of the overall risk landscape, marine insurers also face an increasing demand for insurance products and services against these cyber related risks. Risk assessment and risk mitigation is first and paramount and a precondition for granting insurance cover. In addition, the number of details underwriters are requesting related to cybersecurity programs before providing quotes and cover are increasing on an annual basis as they seek to better understand the maturity and efficacy of programs.

Cyber incidents may result in economic loss or costs of rebuilding lost data. These are not generally insured, but stand-alone ransomware insurance products are now available both within the marine and non-marine insurance markets to protect against this risk. The limited data on the frequency, severity of loss or probability of physical damage and the potential of facing a systemic risk is still a challenge to underwriters.

A successful cyber incident can have several implications relevant to insurance: Loss of life, personal injury, pollution, loss/damage to cargo, cargo handling equipment or of property, business interruption, liabilities, loss of production, loss of data, loss of reputation and probably any consequential damages. Studies show that cyber incident related risks are rapidly evolving and can become a systemic risk, and as such there is not necessarily a one-size-fits-all approach to the monitoring and quantification of these risks. Cyber incident exposures are hence regularly

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

underwritten with appropriate controls in place, and aggregate exposures and limits monitored appropriately.

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

Cover for property damage

Insurance solutions covering damages arising from cyber risks in general and cyber incidents have to be developed within each individual company. The status may be summarized as follows:

- Some local insurance markets still issue unbinding recommendations for certain lines of business excluding cyber related damages. Historically, the most widely used exclusion has been CL380 for malicious cyber incidents (Institute Cyber-attack Exclusion Clause). It is used across all marine sectors and activities (cargo, energy, excess of loss, hull, liability, specialty and war). Another widely used exclusion is the American Institute Cyber Exclusion Clause (1/06/2015).
- Other market solutions may either explicitly insure the risk or – in all risk policies – do not exclude the risk and grant "silent cover" (ie cyber risks are covered in the contract without being mentioned explicitly). However, it should be noted that the silent cover approach has increasingly come under scrutiny.[20]
- Finally, so called "buy back" solutions may include the risk under defined preconditions and against a negotiated additional premium. "Buy back" means that the risk is excluded in the contract, but there's an option to include again additional cyber coverage in the contract at certain conditions and against additional premium.

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

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

[20] In mid-2017, the **Prudential** Regulation Authority (PRA) in the UK released a supervisory statement detailing its expectations of firms to be able to identify, quantify and manage cyber insurance underwriting risk. Likewise, global ratings agencies announced they "expect companies to be proactive and forthcoming with their own evaluation and measurement of the exposure and accumulation of their cyber liability exposure." In June 2019, the International Underwriting Association (IUA) published cyber exclusion clauses IUA 09-081 and IUA 09-082. The wordings have been developed in order to address issues of non-affirmative or "silent" cover, where traditional insurance policies may unintentionally suggest protection for undefined cyber risks. In November 2019, the Lloyd's Market Association (LMA) published several new purely illustrative model clauses for the guidance of its members which shall provide clarity about cyber coverage under first-party property damage policies: LMA5400 – Property D&F Cyber Endorsement, LMA5401 – Property D&F Cyber Exclusion, LMA5402 – Marine Cyber Exclusion and LMA5403 – Marine Cyber Endorsement. The clauses relate to property direct and facultative business and marine business. The clauses shall provide a starting point for the market to address cyber risks in the property, marine and energy markets.

Cover for liability

It is recommended to contact the P&I Club for detailed information about coverage provided to shipowners and charterers regarding 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 incident, does not in itself give rise to any exclusion of normal P&I cover. In the event of a claim involving a cyber incident, claimants may well seek to argue that the claim arose as a result of an inadequate level of cyber preparedness. This, therefore, further stresses the importance of companies being able to demonstrate that they are acting with reasonable care in their approach to managing cyber risk and to protecting the ship.

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 and are therefore not covered by P&I insurance. For example, financial loss caused by ransomware, or costs of rebuilding scrambled data would not be identified in the coverage.

It should, however, be noted that normal P&I 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. As many cyber-attacks have been linked back to various nation state threat actors, it is important to understand whether such attacks by a nation state actor would be potentially viewed as an act of war by the insurer.

Cyber security clause for charter parties

Standard cyber security clauses have been developed by shipping industry bodies and could be considered for inclusion in charter parties. The importance of sharing information about cyber incident and thereby help the other party in mitigating or preventing the effects of a cyber incident is emphasized.

10.7 Reporting of cyber incidents

Reporting cyber incidents is increasingly becoming a regulatory and/or contractual requirement for companies and can include notification to flag State and/or coastal State authorities, customers, vendors and other impacted parties. As timelines for reporting vary greatly, eg from an immediate notification to within two weeks, companies should include an appendix within their IRP that contains their specific reporting requirements. If an incident does occur and the company does not adhere to their reporting requirements, they may face a variety of penalties.

In addition, anonymously reporting incidents to an international nongovernmental organisation, such as eg, the MTS-ISAC or NORMA Cyber, can help provide early warning of attacks to the broader maritime community. This can help to limit debilitating attacks across the global maritime supply chain by helping to provide other potential, interdependent victims, such as port authorities, shipowners and terminal operators, early warning of the cyber-attack. Additionally, eg the MTS-ISAC or NORMA Cyber receives timely notifications from stakeholders regarding cyber threat activity and can be a quick source of information during incident response.

ANNEX 1 – Onboard IT and OT systems, equipment and technologies

This annex provides a non-exhaustive 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 eg:

Communication systems

- Integrated communication systems
- Satellite communication equipment
- Voice Over Internet Protocols (VOIP) equipment
- Wireless local area networks (WLANs)
- Public address and general alarm systems
- Systems used for reporting mandatory information to public authorities.

Bridge systems

- Integrated navigation system
- Positioning systems (GPS, etc)
- Electronic Chart Display Information System (ECDIS)
- Dynamic Positioning (DP) systems
- Systems that interface with electronic navigation systems and propulsion/manoeuvring systems
- Automatic Identification System (AIS)
- Long Range Identification and Tracking system (LRIT)
- Global Maritime Distress and Safety System (GMDSS)
- Radar equipment
- Voyage Data Recorders (VDRs)
- Bridge Navigational Watch Alarm System (BNWAS)
- Shipboard Security Alarm Systems (SSAS).

Propulsion, machinery management and power control systems

- Engine governor
- Power management

- Integrated control system
- Alarm system
- Bilge water control system
- Water treatment system
- Emissions monitoring
- Heating, ventilation. and air conditioning monitoring
- Damage control systems
- Other monitoring and data collection systems eg fire alarms.

Access control systems

- Surveillance systems such as CCTV network
- electronic “personnel-on-board” systems.

Cargo management systems

- Cargo Control Room (CCR) and its equipment
- Onboard loading computers and computers used for exchange of loading information and. Load plan updates with the marine terminal and stevedoring company
- Remote cargo and container tracking and sensing systems
- Level indication system
- Valve remote control system
- Ballast water systems
- Reefer monitoring systems
- Water ingress alarm system.

Passenger or visitor servicing and management systems

- Property Management System (PMS)
- Shipmanagement systems (often including electronic health records)
- Financial related systems
- Ship passenger/visitor/seafarer boarding access systems
- Infrastructure support systems like domain naming system (DNS) and user authentication/authorisation systems
- Incident management systems.

Passenger-facing networks

- Passenger Wi-Fi or Local Area Network (LAN) internet access, for example where onboard personnel can connect their own devices[21]
- Guest entertainment systems.

Core infrastructure systems

- Security gateways
- Routers
- Switches
- Firewalls
- Virtual Private Network(s) (VPN)
- Virtual LAN(s) (VLAN)
- Intrusion prevention systems
- Security event logging systems.

Administrative and crew welfare systems

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

[21] 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 – 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 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 to address cyber risk management in an approved SMS. Companies are reminded to check with their flag State and/or Recognised Organisation for implementation requirements.

Identify[22]

Roles and Responsibilities[23]	
Action	Remarks
ISM Code: 3.2 This publication: 1.1 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 This publication: 1.1 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[24] 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 This publication: 7.3 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.

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

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

[24] 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.

Protect

Implement risk control measures	
Action	Remarks
ISM Code: 1.2.2.2 This publication: 2, 3, 4, 5 and 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 the identification of authorized and removal of 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 software running on company-controlled hardware onboard, including version and update status and take actions to remove unauthorized software. 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 hardware and/or software, and deletion of such, 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 activities. ▫ 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. 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.
	• The SMS should include policies on the allocation and use of administrative privileges by ship and shore-based personnel, and third parties.
	• **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**. Maintain situational awareness of current cyber threats. 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.

Develop contingency plans	
Action	Remarks
ISM Code: 7 This publication: 1.5 and 9 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 This publication: 9	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 SMS. This is because the effect of common shipboard emergencies should be independent of the root cause. For example, a fire may be caused by

Update emergency plans to include responses to cyber incidents.	equipment malfunctioning because of a software failure or inappropriate maintenance or unexpected 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 response and recovery 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 eg, providing a step-by-step checklist for system recovery.

Detect

Develop and implement activities necessary to detect a cyber-event in a timely manner.	
Action	Remarks
ISM Code: 9.1 This publication: 1.5 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. Consider sharing the facts of a cyber related non-conformity with information sharing organisations. Examples of such non-conformities and cyber incidents: • Unauthorised access to network infrastructure • Unauthorized or inappropriate use of administrator privileges • Suspicious network activity such as large file downloads or bulk file deletions • Unauthorised access to critical systems • Unauthorised use of removable media • Unauthorised connection of personal device • 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.

Respond

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 This publication: 10.1 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 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 This publication: 10 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 This publication: 7.2 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. • As part of the management of change process a backup is performed before system updates. • 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.

Recover

Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber incident	
Action	Remarks
ISM Code: 10.4 This publication: 10.3 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.

ANNEX 3 – Onboard networks

Implementing a secure network depends on both the configuration of IT/OT systems and network 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 the physical network control on an existing ship may be limited because cyber risk management had not been considered during the ship's construction. For newbuilds, following the requirements found in IACS UR E26 is mandatory.

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

- Implement network separation and/or traffic management to restrict the level of access to sensitive data, systems and services.
- Manage encryption protocols to ensure correct level of privacy and commercial communication.
- Manage use of certificates to verify origin of digitally signed documents, software or services.

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

Physical layout

The physical layout of the network should be carefully planned, taking into consideration the physical location of essential network devices, including servers, switches, firewalls and cabling. This will inform the methods used to restrict access and maintain the physical security of the network installation and control of entry points to the network.

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.

Network segmentation

As appropriate, onboard networks should normally segment the following basic functions (it is not uncommon that networks are even further separated):

- Necessary communication between OT equipment, and configuration and monitoring of OT equipment

- Onboard administrative tasks including email and sharing files or folders related to eg ship administration, cargo operations, technical management etc (IT networks)
- Recreational internet access for crew and/or passengers/visitors
- Navigational network and machinery/cargo networks
- Wireless segment within the OT network
- Safety equipment within the OT network and the rest of the OT segments.

Effective network segmentation is a key aspect of “defence in depth”. OT, IT and public networks should be segmented by appropriate protection measures. To ensure safety, especially OT network should be physically segmented from IT and public networks. Where risks demand, further segmentation between navigation systems, engineering systems and cargo management systems can be considered. The protection measures used may include, but are not limited to an appropriate combination of the following:

- A perimeter firewall between the onboard network and the internet
- Network switches between each network segment
- Internal firewalls between each network segment
- Virtual Local Area Networks (VLAN) to host separate segments.

In addition, each physical segment and/or VLAN 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.

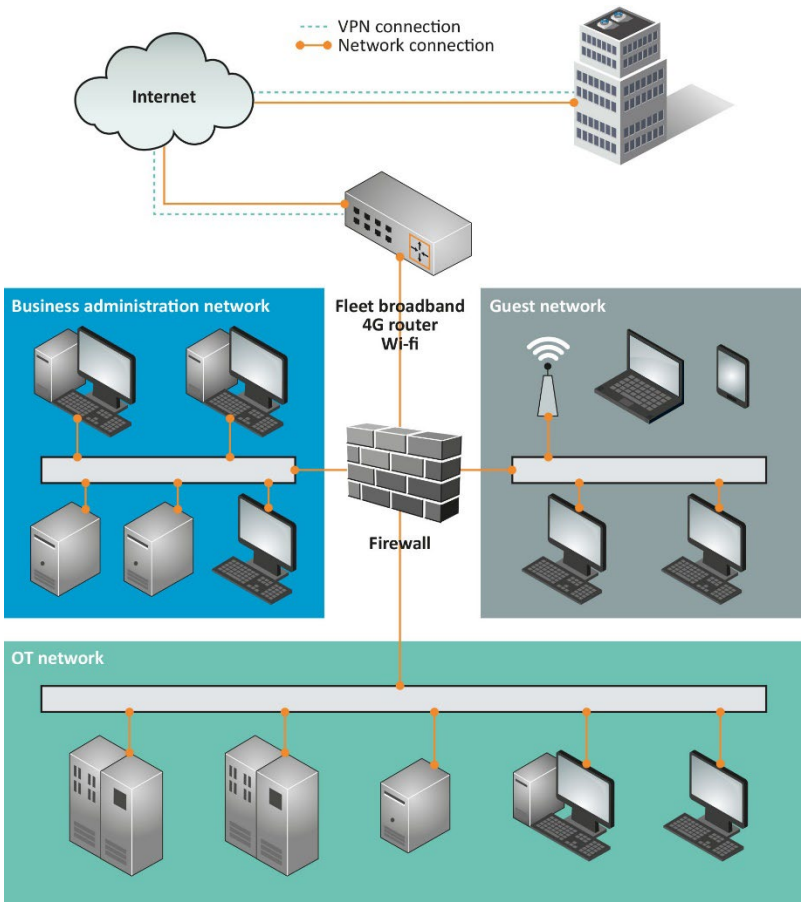

Figure 12 – Example of an onboard network.

In the example shown above, the network has been segmented using a perimeter firewall, which supports three VLANs.

1. The OT Network containing equipment and systems, that performs safety critical functions
2. The IT network containing equipment and systems, that performs administrative or business functions
3. A crew network governed by the company usage policies and procedures
4. A 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 important 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 the 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 not recommended.

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.

Monitoring data activity

It is important when monitoring and managing 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 incident. This will help to secure the network from any similar incidents in the future.

A network Intrusion Detection System (IDS) or Intrusion Protection System (IPS) can alert the system administrator in real-time of any incidents 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 IDS/IPS sensor could also be placed by a remote-access segment, for instance a VPN.

Protection measures

Protection measures should be implemented in a way that maintains the system's integrity during normal operations as well as during a cyber incident. Every network onboard has several endpoints such as workstations, servers, routers, input and output modules, transducers etc. The endpoints are very important as they control the operation and the security of the system.
A single security product, technology or solution cannot adequately protect a system by itself. A multiple layer strategy involving two (or more) different overlapping security mechanisms is desired, so that the impact of a failure in any one mechanism is minimized (see section 7.1 defence-in-depth). In addition, an effective defence-in-depth strategy requires a thorough understanding of possible attack vectors on a system. These may include:

- Back doors and holes in network perimeter and instruments
- Vulnerabilities in commonly used protocols

- Vulnerable endpoints and sensors
- Unprotected databases
- Intentional or unintentional compromise through authorised users.

A secure running environment can be established by using a testing environment isolated from networks and computers, which 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 helps prevent malicious, malfunctioning or untrusted software from affecting the rest of the system.

ANNEX 4 – Glossary

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.

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

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.

Chain of custody is the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis and disposition of physical or electronic evidence.

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

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

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 by taking into consideration the costs and benefits of actions taken by stakeholders.

Cyber security means the prevention of damage to, protection of and restoration of computers, electronic communications systems, electronic communications services, wire communication and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality and nonrepudiation.

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.

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.

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

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

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

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

Flaw is unintended functionality in software.

Industrial Internet of Things (IIoT) refers to the application of instrumentation and connected sensors and other devices to machinery and vehicles in the transport, energy and industrial sectors.

Information Technology (IT) covers the spectrum of technologies for data storing and processing, including software, hardware and communication technologies.

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.

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

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.

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

Manufacturer is the entity that manufactures the shipboard equipment and associated software.

Operational technology (OT) includes hardware and software that directly monitors/controls physical devices and processes, typically on board.

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.

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

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

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

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.

Risk assessment is the process which collects information and assigns values to risks as a base on which to make decision on priorities and developing or comparing courses of action.

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.

Sandbox is an isolated environment, in which a programme 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.

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

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

Software whitelisting means specifying the software, which is present and active on an IT or OT system.

Typosquatting. Also called URL hijacking or fake URL. Relies on mistakes such as typos made by Internet users when inputting a website address into a web browser. Should a user accidentally enter an incorrect website address, they may be led to an alternative and often malicious website.

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.

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.

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

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

ANNEX 5 – Contributors to most recent revision of this publication

The following organisations and companies have participated in the development of these guidelines[25]:

Working Group 2024

- BIMCO
- Columbia Shipmanagement Cyprus
- Chamber of Shipping of America
- Digital Container Shipping Association (DCSA)
- INTERMANAGER
- International Association of Dry Cargo Shipowners (INTERCARGO)
- International Association of Independent Tanker Owners (INTERTANKO)
- International Chamber of Shipping (ICS)
- International Marine Contractors Association (IMCA)
- International Union of Marine Insurance (IUMI)
- Maersk
- Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC)
- Nordic Maritime Cyber Resilience Centre (NORMA Cyber)
- Oil Companies International Marine Forum (OCIMF)
- Superyacht Builders Association (Sybass)
- World Shipping Council

Reference Group 2024

- Class NK
- Cygnus Technologies
- Templar Executives

[25] The following additional stakeholders have participated in previous working groups:
Anglo-Eastern Group, Cruise Lines International Association, Cyberkeel, Interferry, International Group of P & I Clubs, Moran Cyber and SOFTimpact Ltd.