THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

Produced and supported by
BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL

BIMCO

CLIA

International Chamber of Shipping
Shaping the Future of Shipping

INTERCARGO
International Association of Dry Cargo Shipowners

InterManager

INTERTANKO

IUMI
International Union of Marine Insurance

OCIMF

WORLD SHIPPING COUNCIL
PARTNERS IN TRADE

The Guidelines on Cyber Security Onboard Ships

Version 3

Terms of use

Contents

Introduction 1

1 Cyber security and safety management 3
1.1 Differences between IT and OT systems 5
1.2 Plans and procedures 6
1.3 Relationship between ship manager and shipowner 7
1.4 The relationship between the shipowner and the agent 7
1.5 Relationship with vendors 8
2 Identify threats 9
3 Identify vulnerabilities 13
3.1 Ship to shore interface 14
4 Assess risk exposure 16
4.1 Risk assessment made by the company 21
4.2 Third-party risk assessments 21
4.3 Risk assessment process 22
5 Develop protection and detection measures 24
5.1 Defence in depth and in breadth 24
5.2 Technical protection measures 25
5.3 Procedural protection measures 29
6 Establish contingency plans 34
7 Respond to and recover from cyber security incidents 36
7.1 Effective response 36
7.2 Recovery plan 37
7.3 Investigating cyber incidents 38
7.4 Losses arising from a cyber incident 38

Annex 1 Target systems, equipment and technologies 40
Annex 2 Cyber risk management and the safety management system 42
Annex 3 Onboard networks 46
Annex 4 Glossary 50
Annex 5 Contributors to version 3 of the guidelines 53

Introduction

Ships are increasingly using systems that rely on digitisation, digitalisation, integration, and automation, which call for cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the internet.

This brings the greater risk of unauthorised access or malicious attacks to ships' systems and networks. Risks may also occur from personnel accessing systems on board, for example by introducing malware via removable media.

To mitigate the potential safety, environmental and commercial consequences of a cyber incident, a group of international shipping organisations, with support from a wide range of stakeholders (please refer to annex 5 for more details), have participated in the development of these guidelines, which are designed to assist companies in formulating their own approaches to cyber risk management onboard ships.

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. These guidelines provide a risk-based approach to identifying and responding to cyber threats. An important aspect is the benefit that relevant personnel would obtain from training in identifying the typical modus operandi of cyber attacks.

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

The commitment of senior management to cyber risk management is a central assumption, on which the Guidelines on Cyber Security Onboard Ships have been developed.

The Guidelines on Cyber Security Onboard Ships are aligned with IMO resolution MSC.428(98) and IMO's guidelines and provide practical recommendations on maritime cyber risk management covering both cyber security and cyber safety. (See chapter 1 for this distinction).

The aim of this document is to offer guidance to shipowners and operators on procedures and actions to maintain the security of cyber systems in the company and onboard the ships. The guidelines are not intended to provide a basis for, and should not be interpreted as, calling for external auditing or vetting the individual company's and ship's approach to cyber risk management.

Like the IMO guidelines, the US National Institute of Standards and Technology (NIST) framework has also been accounted for in the development of these guidelines. The NIST framework assists companies with their risk assessments by helping them understand, manage and express the

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

potential cyber risk threat both internally and externally. As a result of this assessment, 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 approaches to manage the risks. Sample framework profiles are publicly available for maritime bulk liquid transfer, offshore, and passenger ship operations[2]. These profiles were created by the United States Coast Guard and NIST's National Cybersecurity Center of Excellence with input from industry stakeholders. The profiles are considered to be complimentary to these guidelines and can be used together to assist industry in assessing, prioritizing, and mitigating their cyber risks.

[2] The NIST Framework Profiles for maritime bulk liquid transfer, offshore, and passenger operations can be accessed here: **http://mariners.coastguard.dodlive.mil/2018/01/12/1-12-2018-release-of-offshore-operations-and-passenger-vessel-cybersecurity-framework-profiles**.

1 Cyber security and safety management

Both cyber security and cyber safety are important because of their potential effect on personnel, the ship, environment, company and cargo. Cyber security is concerned with the protection of IT, OT, information and data from unauthorised access, manipulation and disruption. Cyber safety covers the risks from the loss of availability or integrity of safety critical data and OT.

Cyber safety incidents can arise as the result of:

- a cyber security incident, which affects the availability and integrity of OT, for example corruption of chart data held in an Electronic Chart Display and Information System (ECDIS)
- a failure occurring during software maintenance and patching
- loss of or manipulation of external sensor data, critical for the operation of a ship – this includes but is not limited to Global Navigation Satellite Systems (GNSS).

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

Incident: Unrecognised virus in an ECDIS delays sailing

A new-build 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 recognized as a cyber issue by the ship's master and officers. A producer 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).

Cyber risk management should:

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

Some aspects of cyber risk management may include commercially sensitive or confidential information. Companies should, therefore, consider protecting this information appropriately, and as far as possible, not include sensitive information in their Safety Management System (SMS).

Figure 1: Cyber risk management approach as set out in the guidelines

Development, implementation, and maintenance of a cyber security management program 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, contingency and response planning are balanced in relation to the threats, vulnerabilities, risk exposure and consequences of a potential cyber incident.

1.1 Differences between IT and OT systems

OT systems control the physical world and IT systems manage data. OT systems differ from traditional IT systems. OT is hardware and software that directly monitors/controls physical devices and processes. 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.
Typical differences between IT and OT systems can be seen in the table below.

Typical differences between IT and OT systems can be seen in the table below.

Category	IT system	OT system
Performance requirements	■ non-real-time ■ response must be consistent ■ less critical emergency interaction ■ tightly restricted access control can be implemented to the degree necessary for security	■ real-time ■ response is time-critical ■ response to human and any other emergency interaction is critical ■ access to OT should be strictly controlled, but should not hamper or interfere with human-machine interaction
Availability (reliability) requirements	■ responses such as rebooting are acceptable ■ availability deficiencies may be tolerated, depending on the system's operational requirements	■ responses such as rebooting may not be acceptable because of operational requirements ■ availability requirements may necessitate back-up systems
Risk management requirements	■ manage data ■ data confidentiality and integrity is paramount ■ fault tolerance may be less important. ■ risk impacts may cause delay of: ship's clearance, commencement of loading/ unloading, and commercial and business operations	■ control physical world ■ safety is paramount, followed by protection of the process ■ fault tolerance is essential, even momentary downtime may not be acceptable ■ risk impacts are regulatory non-compliance, as well as harm to the personnel onboard, the environment, equipment and/or cargo
System operation	■ systems are designed for use with commonly known operating systems ■ upgrades are straightforward with the availability of automated deployment tools	■ differing and possibly proprietary operating systems, often without built in security capabilities ■ software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and possible involvement of modified hardware and software
Resource constraints	■ systems are specified with enough resources to support the addition of third-party applications such as security solutions	■ systems are designed to support the intended operational process and may not have enough memory and computing resources to support the addition of security capabilities

Table 1: Differences between OT and IT[3]

[3] Based on table 2-1 in NIST Special Publication 800-82, Revision 2.

There may be important differences between who handles the purchase and management of the OT systems versus IT systems on a ship. IT departments are not usually involved in the purchase of OT systems. The purchase of such systems should involve a chief engineer, 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 the IT department to ensure that cyber risks are considered during the OT purchasing process. OT systems should be inventoried with the IT department, so as to obtain an overview of potential challenges and to help establish the necessary policy and procedures for software maintenance.

Other industry sectors have seen the barrier removed between IT and OT, with management and procurement strategies all handled under the same regime.

1.2 Plans and procedures

IMO Resolution MSC.428(98) identifies cyber risks as specific threats, which companies should try to address as far as possible in the same way as any other risk that may affect the safe operation of a ship and protection of the environment. More guidance on how to incorporate cyber risk management into the company's SMS can be found in annex 2 of these guidelines.

Cyber risk management should be an inherent part of the safety and security culture conducive to the safe and efficient operation of the ship and be considered at various levels of the company, including senior management ashore and onboard personnel. In the context of a ship's operation, cyber incidents are anticipated to result in physical effects and potential safety and/or pollution incidents. This means that the company needs to assess risks arising from the use of IT and OT onboard ships and establish appropriate safeguards against cyber incidents. Company plans and procedures for cyber risk management should be incorporated into existing security and safety risk management requirements contained in the ISM Code and ISPS Code.

The objective of the SMS is to provide a safe working environment by establishing appropriate practices and procedures based on an assessment of all identified risks to the ship, onboard personnel and the environment. The SMS should include instructions and procedures to ensure the safe operation of the ship and protection of the environment in compliance with relevant international and flag state requirements. These instructions and procedures should consider risks arising from the use of IT and OT on board, taking into account applicable codes, guidelines and recommended standards.

When incorporating cyber risk management into the company's SMS, consideration should be given as to whether, in addition to a generic risk assessment of the ships it operates, a particular ship needs a specific risk assessment. The company should consider the need for a specific risk assessment based on whether a particular ship is unique within their fleet. 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.

In accordance with chapter 8 of the ISPS Code, the ship is obliged to conduct a security assessment, which includes identification and evaluation of key shipboard operations and the associated potential threats. As recommended by Part B, paragraph 8.3.5 of the ISPS Code, the assessment should address radio and telecommunication systems, including computer systems and networks. Therefore, the ship's security plan may need to include appropriate measures for protecting both the equipment and the connection. Due to the fast adoption of sophisticated and digitalised onboard OT systems, consideration should be given to including these procedures by reference to the SMS in order to help ensure the ship's security procedures are as up-to-date as possible.

Systems like Tanker Management and Self Assessment (TMSA) also require plans and procedures to be implemented.

1.3 Relationship between ship manager and shipowner

The Document of Compliance 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 ship owner.

Particular emphasis should be placed by both parties on the split of responsibilities, alignment of pragmatic 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. 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 on cyber risk management should be formal and written.

1.4 The relationship between the shipowner and the agent

The importance of this relationship has placed the agent[4] 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.

Coordination of the ship's call of port is a highly complex task being simultaneously global and local. It covers updates from agents, coordinating information with all port vendors, port state control, handling ship and crew requirements, and electronic communication between the ship, port and authorities ashore. As one example, which touches cyber risk management: Often agents are required to build IT systems, which upload information real-time into owner's management information system.

Quality standards for agents are important because like all other businesses, agents are also targeted by cyber criminals. 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 owners 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 an 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[5].

The importance of this incident is that harmonized cyber security across relationships with trusted business partners and producers 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. Principals in the supply chain should work together to mitigate cyber risk.

[4] 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).

[5] Nothing in these guidelines should be taken as recommending the payment of ransom.

1.5 Relationship with vendors

Companies should evaluate and include the physical security and cyber risk management processes of service providers in supplier agreements and contracts. Processes evaluated during supplier vetting and included in contract requirements may include:

- security management including management of sub-suppliers
- manufacturing/operational security
- software engineering and architecture
- asset and cyber incident management
- personnel security
- data and information protection.

Evaluation of service providers beyond the first tier may be challenging especially for companies with a large number of tier one suppliers. Third party providers that are collecting and managing supplier risk management data may be an option to consider.

Lack of physical and/or cyber security at a supplier within their products or infrastructure may result in a breach of corporate IT systems or corruption of ship OT/IT systems.

Companies should evaluate the cyber risk management processes for both new and existing contracts. It is good practice for the company to define their own minimum set of requirements to manage supply chain or 3rd party risks. A set of cyber risk requirements that reflect the company's expectations should be clear and unambiguous to vendors. This may also help procurement practices when dealing with multiple vendors.

2 Identify threats

The cyber risk[6] is specific to the company, ship, operation and/or trade. When assessing the risk, companies should consider any specific aspects of their operations that might increase their vulnerability to cyber incidents.

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

Experiences in the shipping industry and from other business sectors such as financial institutions, public administration and air transport have shown that successful cyber attacks might result in a significant loss of services. Assets can also compromise safety.

There are motives for organisations and individuals to exploit cyber vulnerabilities. The following examples give some indication of the threats posed and the potential consequences for companies and the ships they operate:

Group	Motivation	Objective
Activists (including disgruntled employees)	■ reputational damage ■ disruption of operations	■ destruction of data ■ publication of sensitive data ■ media attention ■ denial of access to the service or system targeted
Criminals	■ financial gain ■ commercial espionage ■ industrial espionage	■ selling stolen data ■ ransoming stolen data ■ ransoming system operability ■ arranging fraudulent transportation of cargo ■ gathering intelligence for more sophisticated crime, exact cargo location, ship transportation and handling plans etc
Opportunists	■ the challenge	■ getting through cyber security defences ■ financial gain
States **State sponsored organisations** **Terrorists**	■ political gain ■ espionage	■ gaining knowledge ■ disruption to economies and critical national infrastructure

Table 2: Motivation and objectives

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

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

In addition, there is the possibility that company personnel, on board and ashore, could compromise cyber systems and data. In general, the company should realise that this may be unintentional and caused by human error when operating and managing IT and OT systems or failure to respect technical and procedural protection measures. There is, however, the possibility that actions may be malicious and are a deliberate attempt by a disgruntled employee to damage the company and the ship.

Types of cyber attack

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

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

- targeted attacks, where a company or a ship's systems and data are the intended target.

Untargeted attacks are likely to use tools and techniques available on the internet, which can be used to locate, discover and exploit widespread vulnerabilities that may also exist in a company and onboard a 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 software or hardware. This problem can, for example, be a code bug, system vulnerability, improper design, hardware malfunction and/or error in protocol implementation. These vulnerabilities may be exploited remotely or triggered locally. Locally, a piece of malicious code may often be executed by the user, sometimes via links distributed in email attachments or through malicious websites.

- **Phishing** – Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information. Such an email may also request that a person visits a fake website using a hyperlink included in the email.

- **Water holing** – Establishing a fake website or compromising a genuine website to exploit visitors.

- **Scanning** – Attacking large portions of the internet at random.

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

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

- **Brute force** – An attack trying many passwords with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords until the correct one is found.

- **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.

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

- **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. Other methods are evolving such as impersonating a legitimate shore-based employee in a shipping company to obtain valuable information, which can be used for a further attack. 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.

Stages of a cyber attack

In 2018, it took on average 140 days between time of infection of a victim's network and discovery of a cyber attack. However, intrusion can go undetected for years. This figure is down from 205 days in 2015 and continues to drop because detection is getting better[7]. Cyber attacks are conducted in stages. 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 attack are:

- **Survey/reconnaissance** – Open/public sources are used to gain information about 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.

- **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, or alter operationally important information such as loading lists
  - gain access to commercially sensitive data such as cargo manifests and/or crew and passenger/visitor lists

[7] The Microsoft Cybercrime Center.

- achieve full control of a system, for example a machinery management system.

- **Pivot** – Pivoting is the technique of using an instance already exploited to be able to "move" and perform other activities. 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. 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 or a key logger 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/visitors lists, cargo manifests 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 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.

3 Identify vulnerabilities

It is recommended that a shipping company initially performs an assessment of the potential threats that may realistically be faced. This should be followed by an assessment of the systems and onboard procedures to map their robustness to handle the current level of threat. It may be facilitated by internal experts or supported by external experts with knowledge of the maritime industry and its key processes. The result should be a strategy centred around the key risks.

Incident: Crash of integrated navigation bridge at sea

A ship with an integrated navigation bridge 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 producer 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 proactive software maintenance to the ship may have prevented this incident from occurring.

Stand-alone systems will be less vulnerable to external cyber attacks compared to those attached to uncontrolled networks or directly to the internet. Network design and network segregation will be explained in more detail in annex 3. Care should be taken to understand how critical shipboard systems might be connected to uncontrolled networks. When doing so, the human element should be taken into consideration, as many incidents are initiated by personnel's actions. Onboard systems could include:

- **Cargo 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 ports, marine terminals. Such systems may include shipment-tracking tools available to shippers via the internet. However, the tracking is usually done via the company's systems connected to the ship and not directly between the shipper and the ship. Interfaces of this kind make cargo management systems and data in cargo manifests and loading lists vulnerable to cyber attacks.

- **Bridge systems** – The increasing use of digital, network navigation systems, with interfaces to shoreside networks for update and provision of services, make such systems vulnerable to cyber attacks. Bridge systems that are not connected to other networks may be equally vulnerable, as removable media are often used to update such systems from other controlled or uncontrolled networks. A cyber incident can extend to service denial or manipulation and, therefore, may affect all systems associated with navigation, including ECDIS, GNSS, AIS, VDR and Radar/ARPA.

- **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 attacks. 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 attacks.

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

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

3.1 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 office. 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

- maintenance and spare parts management

- cargo, loading and unloading, crane, pump management and stow planning

- voyage performance monitoring.

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

Modern technologies can add vulnerabilities to the ships especially if there are insecure designs of networks and uncontrolled access to the internet. Additionally, shoreside and onboard personnel may be unaware how some equipment producers maintain remote access to shipboard equipment and its network system. 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 should fully understand the ship's OT and IT systems and how these systems connect and integrate with the shore side, including public authorities, marine terminals and stevedores. This requires an understanding of all computer based onboard systems and how safety, operations, and business can be compromised by a cyber incident.

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

1. The producer's and service provider's cyber risk management awareness and procedures: Such 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. These companies should have an updated cyber risk management company policy, which includes training and governance procedures for accessible IT and OT onboard systems.

2. The maturity of a third-party's cyber risk management procedures: The shipowner should query the internal governance of cyber network 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 or stevedoring company.

Common vulnerabilities

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

- obsolete and unsupported operating systems
- outdated or missing antivirus software and protection from malware
- inadequate security configurations and best practices, including ineffective network management and the use of default administrator accounts and passwords,
- 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 for third parties including contractors and service providers.

Incident: Navigation computer crash during pilotage

A ship was under the conduct of a pilot 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 Assess risk exposure

Cyber risk assessment should start at senior management level of a company, instead of being immediately delegated to the ship security officer or the head of the IT department. There are several reasons for this.

1. Initiatives to heighten cyber security and safety may at the same time affect standard business procedures and operations, rendering them more time consuming and/or costly. It is, therefore, a senior management level decision to evaluate and decide on risk mitigation.

2. A number of initiatives, which would improve cyber risk management, are related to business processes, training, the safety of the ship and the environment and not to IT systems, and therefore need to be anchored organisationally outside the IT department.

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

The following questions may be used as a basis for a risk assessment when addressing cyber risks onboard ships:

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

Based on the answers, the company should delegate authority and allocate the budget needed to carry out a full risk assessment and develop solutions that are best suited for the company and the operation of their ships. The following should be addressed:

- identify systems that are important to operation, safety and environmental protection
- assign the persons responsible for setting cyber policies, procedures and enforce monitoring
- determine where secure remote access should use multiple defence layers and where protection of networks should be disconnected from the internet
- identification of needs for training of personnel.

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

- the cyber controls already implemented by the company onboard its ships
- multiple stakeholders are often involved in the operation and chartering of a ship potentially resulting in lack of accountability for the IT infrastructure
- the ship being online and how it interfaces with other parts of the global supply chain
- ship equipment being remotely monitored, eg by the producers
- business-critical, data sensitive and commercially sensitive information shared 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 for the ship's safety and for environmental protection.

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

IT and OT systems, software and maintenance can be outsourced to third-party service providers and the company, itself, may not possess a way of verifying the level of security supplied by these providers. Some companies use different providers responsible for software and cyber security checks.

The growing use of big data, smart ships and the "internet of things"[8] will increase the amount of information available to cyber attackers and the potential attack surface to cyber criminals. This makes the need for robust approaches to cyber risk management important both now and in the future.

Incident: Worm attack 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 performed 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 producer 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 program into the memory. This program was designed to communicate with its command and control server to receive its next set of instructions. It could

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

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.

Third-party access

Visits to ships by third parties requiring a connection to one or more computers on board can also result in connecting the ship to shore. It is common for technicians, vendors, port officials, marine terminal representatives, agents, pilots, and other technicians to board the ship and plug in devices, such as laptops and tablets. Some technicians may require the use of removable media to update computers, download data and/or perform other tasks. It has also been known for customs officials and port state control officers to board a ship and request the use of a computer to "print official documents" after 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. Where possible, systems should be scanned for malware prior to use. OT systems should be tested to check that they are functioning correctly.

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

- bridge and engine room computers and work stations 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
- navigational systems including Electronic Navigation Chart (ENC) Voyage Data Recorder (VDR), dynamic positioning (DP)
- cargo handling and stowage, engine, and cargo management and load planning systems
- 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.

Impact assessment

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

- unauthorised access to and disclosure of information or data about the ship, crew, cargo and passengers
- loss of integrity, which would modify or destroy information and data relating to the safe and efficient operation and administration 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 information or data. For example, assessing the vulnerability of IT systems related to commercial operations may focus on confidentiality and integrity rather than availability. Conversely, assessing the vulnerability of OT systems onboard ships, particularly safety critical systems, may focus on availability and/or integrity instead of confidentiality.

Potential impacts could be safety-related, operational, environmental-related, financial, reputational and compliance-related. Several assessment methodologies offer criteria and techniques that can help define the magnitude of the impact from a cyber attack[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) 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; (ii) result in minor damage to organisational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The loss of confidentiality, integrity, or availability could be expected to have a substantial adverse effect on company and ship, assets or individuals	A substantial adverse effect means that a security breach might: (i) cause a significant degradation in ship operation to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organisational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
High	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on company and ship operations, assets, environment or individuals.	A severe or catastrophic adverse effect means that a security breach might: (i) cause a severe degradation in or loss of ship operation to an extent and duration that the organisation is not able to perform one or more of its primary functions; (ii) result in major damage to environment and/or organisational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

Table 3: Potential impact levels when using the CIA model

When it comes to OT systems, an extra dimension must be added to the CIA model.

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

[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.

A risk assessment of OT systems needs to be based on an inventory overview of equipment and/or computer-based systems and a map of the networks' connections. Further, access points and communication devices should be part of this overview. As the impact of an onboard OT system's cyber incident may include physical effects, risk assessments should include:

- impacts on the safety of onboard personnel, the ship and cargo
- physical impact on an OT system, including the environment surrounding it on board; the effect on the process that is being controlled and the physical effect on the OT system itself
- the consequences for risk assessments of non-digital control components within an OT system.

The implementation of protection measures based on risk assessments is well established on all ships via the ISM code and the ship's SMS. Safety assessments are concerned primarily with the physical world bearing in mind that the physical and the digital worlds are now intertwined. Assessing the potential physical damage from a cyber incident should include:

1. how an incident could manipulate the operation of sensors and actuators to impact the physical environment
2. what redundant controls and manual overriding possibilities exist in the OT system to prevent an incident
3. how a physical incident could emerge.
4. how to evaluate potential effects to the physical process performed by the OT system.

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 in-house considerations.

The following table 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

Table 4: Result of CIA assessment of SCADA system

Bring your own device (BYOD)

It is recognised that personnel may be allowed to bring their own devices (BYOD) on board to access the ship's system or network. Although this may be both beneficial and economical for ships, it significantly increases the level of vulnerability because these devices may be unmanaged. Policies and procedures should address the control and use of BYODs, as well as how to protect vulnerable data, by using network segregation for example.

4.1 Risk assessment made by the company

As mentioned above, the risk assessment process starts by assessing the systems on board, in order to map their robustness to handle the current level of cyber threats. The assessment should assess the IT and OT systems on board. When conducting the assessment, the company should consider the outcomes of the ship security assessment as well as the following:

1. identification of existing technical and procedural controls to protect the onboard IT and OT systems
2. identification of IT and OT systems that are vulnerable including the human factor, and the policies and procedures governing the use of these systems. The identification should include searches for known vulnerabilities relevant to the equipment as well as the current level of patching and firmware updates
3. identification and evaluation of key ship board operations that are vulnerable to cyber attacks
4. identification of possible cyber incidents and their impact on key ship board operations, and the likelihood of their occurrence to establish and prioritise protection measures.

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

4.2 Third-party risk assessments

Self-assessments can serve as a good start but may be complemented by third-party risk assessments to drill deeper and identify the risks and the gaps that may not be found during the self-assessment. Penetration tests of critical IT and OT infrastructure can also be performed to identify whether the actual defence level matches the desired level set forth in the cyber security strategy for the company. Such tests can be performed by external experts simulating attacks using both IT-systems, social

engineering and, if desired, even physical penetration of a facility's security perimeter. These tests are referred to as active tests because they involve accessing and inserting software into a system. This may only be appropriate for IT systems. Where risk to OT systems during penetration testing is unacceptable, passive testing approaches should be considered. Passive methods rely on scanning data transmitted by a system to identify vulnerabilities. In general, no attempt is made to actively access or insert software into the system.

4.3 Risk assessment process

Phase 1: Pre-assessment activities

Prior to starting a cyber risk assessment on board[11], the following activities should be performed:

- map the ship's key functions and systems and their potential impact levels, for example using the CIA model, taking into consideration the operation of OT systems
- identify main producers of critical shipboard IT and OT equipment
- review detailed documentation of critical OT and IT systems including their network architecture, interfaces and interconnections
- identify cyber security points-of-contact with each of the producers 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
- support, if necessary, the risk assessment with an external expert to develop detailed plans and include producers and service providers.

Phase 2: Ship assessment

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

- technical such as software defects or outdated or unpatched systems
- design such as access management, unmanaged network interconnections
- implementation errors for example misconfigured firewalls
- procedural or other user errors.

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

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

An aspect of on-ship assessment is involvement of crew of all levels; particularly the master, chief engineer and first mate. This process assists to understand the implementation of the IT and OT systems onboard, and how they may vary from stated design documentation, and also to understand the level of cyber training delivered to the ship's crew.

Phase 3: Debrief and vulnerability review/reporting

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

Ideally, the cyber risk assessment should include:

- 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 resulting impact, and appropriate technical fix and mitigation advice
- prioritised list of actions – the priorities allocated should reflect the effectiveness of the measure, the cost, the applicability, etc. It is important that this list should be a complete list of options available and not represent a list of services and products the third-party risk assessor, if applicable, would like to sell.
- supplementary data – a supplement containing the technical details of all key findings and comprehensive analysis of critical flaws. This section should also include sample data recovered during the penetration testing, if any, of critical or high-risk vulnerabilities
- appendices – records of activities conducted by the cyber risk assessment team and the tools used during the engagement.

Consideration should be given as to whether parts of the cyber risk assessment should be treated as confidential.

Whilst cyber risk management policies and procedures should be included in the company safety management system, these should not contain information, which if made available outside the company could become a vulnerability.

Phase 4: Producer debrief

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

5 Develop protection and detection measures

The outcome of the company's risk assessment and subsequent cyber security strategy should be a reduction in risk to be as low as reasonably practicable. At a technical level, this would include the necessary actions to be implemented to establish and maintain an agreed level of cyber security.

It is important to identify how to manage cyber security on board and to delegate responsibilities to the master, responsible officers and when appropriate the company security officer.

5.1 Defence in depth and in breadth

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

- increase the probability that a cyber incident is detected
- increase the effort and resources required to protect information, data or the availability of IT and OT systems.

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
- periodic vulnerability scanning and testing
- software whitelisting
- access and user controls
- appropriate procedures regarding the use of removable media and password policies
- personnel's awareness of the risk and familiarity with appropriate procedures.

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 attacks.

When developing integration between systems, 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. This is “defence in breadth” and it is used to prevent any vulnerabilities in one system being used to circumvent protection measures of another system.

Cyber risk protection measures may be either technical or procedural in nature, with technical controls implemented to enforce procedural controls; a combination approach using appropriate measures provides the most effective level of protection.

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

Cyber risk protection measures may be technical and focused on ensuring that onboard systems are designed and configured to be resilient to cyber attacks. Protection measures may also be procedural and should be covered by company policies, safety management procedures, security procedures and access controls.

Consideration needs to be given to implementing technical controls that are practical and cost effective, particularly on existing ships.

Implementation of cyber security controls should be prioritised, focusing first on those measures, or combinations of measures, which offer the greatest benefit.

5.2 Technical protection measures

The Centre for Internet Security (CIS) provides guidance on measures[12] 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[13].

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.

It is recommended that routers are secured against attacks and unused ports should be closed to prevent 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 controlled or uncontrolled[14] networks. Controlled networks are designed to prevent any security risks from connected devices by use of

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

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

[14] 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.

firewalls, security gateways, routers and switches. Uncontrolled networks may pose 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. These networks may be necessary to allow suppliers to upload system upgrades or perform remote servicing. Shoreside external access points of such connections should be secured to prevent unauthorised access
- cargo stowage, load planning and 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, based on necessary access and trust levels, is one of the most successful strategies for the prevention of cyber incidents. Effectively segregated 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 safe zones. The fewer communications links and devices in a zone, the more secure the systems and data are in that zone. Confidential and safety critical systems should be in the most protected zone. See annex 3 of these guidelines for more information on shipboard networks and also refer to ISO/IEC 62443.

Physical security

Physical security[15] is a central aspect of cyber risk management and an effective defence in depth strategy relies on ensuring that technical controls cannot be circumvented through trivial technical means. 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.

Detection, blocking and alerts

Identifying intrusions and infections is a central part of the control procedures. A baseline of network operations and expected data flows for users and systems should be established and managed, so that cyber incident alert thresholds can be established. Key to this will be the definition of roles and responsibilities for detection to help ensure accountability. Additionally, a company may choose to incorporate an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS) into the network or as part of the firewall. Some of their main functions include identifying threats/malicious activity and code, and then logging, reporting and attempting to block the activity. Further details concerning IDS and IPS can be found in annex 3 of these guidelines. It helps to ensure that dedicated onboard personnel can understand the alerts and their implications. Incidents detected should be directed to an individual or service provider, who is responsible for acting on this type of alert.

[15] 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.

When establishing an uplink 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.

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

When using a Virtual Private Network (VPN), the data traffic should be encrypted to an acceptable international standard. Furthermore, a firewall in front of the servers and computers connected to the networks (ashore or on board) should be deployed. The distribution partner should advise on the routing and type of connection most suited for specific traffic. Onshore filtering (inspection/blocking) of traffic is also a matter between a shipowner and the distribution partner. 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.

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

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 can be considered for controlling wireless access:

- the use of enterprise authentication systems using asymmetric encryption and isolating networks with appropriate wireless dedicated access points (e.g. guest networks isolated from administrative networks)
- the adoption of systems, such as wireless IPS, that can intercept non-authorized wireless access points or rogue devices
- the protection of the physical interconnection between wireless access devices and the network, such as network plugs, network racks, etc.) to avoid unauthorized access by rogue devices.

Malware detection

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

As a general guideline, onboard computers should be protected to the same level as office computers ashore. Anti-virus and anti-malware software should be installed, maintained and updated on all

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

Secure configuration for hardware and software

Only senior officers should be given administrator profiles, so that they can control the set up and disabling of normal user profiles. User profiles should be restricted to only allow the computers, workstations or servers to be used for the purposes, for which they are required. User profiles should not allow the user to alter the systems or install and execute new programs.

Email and web browser protection

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

- protect shoreside and onboard personnel from potential social engineering
- 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: email as zip or encrypted file when necessary, disable hyperlinks on email system, avoid using generic email addresses and ensure the system has configured user accounts.

Data recovery capability

Data recovery capability is the ability to restore a system and/or data from a secure copy or image, thereby allowing the restoration of a clean system. Essential information and software-adequate backup facilities should be available to 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 quickly and safely regain navigational and operational capabilities after a cyber incident. More details on recovery can be found in chapter 7 of these guidelines.

Application software security (patch management)

Safety and security updates should be provided to onboard systems. Ordinary security patches should be included in the periodic maintenance cycle. Critical patches should be evaluated in terms of operational impact on the OT systems. These updates or patches should be applied correctly and in a timely manner to ensure that any flaws in a system are addressed before they are exploited by a cyber attack. If a critical patch cannot be installed, alternative measures should be evaluated to help implement virtual patching techniques.

5.3 Procedural protection measures

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

Training and awareness

Training and awareness are the key supporting elements to an effective approach to cyber risk management as described in these guidelines and summarised in figure 1.

The internal cyber threat should be taken into account. 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 and operation of the ship.

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.

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

- risks related to emails and how to behave in a safe manner. Examples are phishing attacks where the user clicks on a link to a malicious site
- risks related to internet usage, including social media, chat forums and cloud-based file storage where data movement is less controlled and monitored
- risks related to the use of own devices. These devices may be missing security patches and controls, such as anti-virus, and may transfer the risk to the environment, to which they are connected
- risks related to installing and maintaining software on company hardware using infected hardware (removable media) or software (infected package)
- risks related to poor software and data security practices, where no anti-virus checks or authenticity verifications are performed
- safeguarding user information, passwords and digital certificates
- cyber risks in relation to the physical presence of non-company personnel, eg, where third-party technicians are left to work on equipment without supervision
- detecting suspicious activity or devices and how to report a possible cyber incident. Examples of this are strange connections that are not normally seen or someone plugging in an unknown device on the ship network

- awareness of the consequences or impact of cyber incidents to the safety and operations of the ship
- understanding how to implement preventative maintenance routines such as anti-virus and anti-malware, patching, backups, and incident-response planning and testing
- procedures for protection against risks from service providers' removable media before connecting to the ship's systems.

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

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

- an unresponsive or slow to respond system
- unexpected password changes or authorised users being locked out of a system
- unexpected errors in programs, including failure to run correctly or programs running unexpectedly
- unexpected or sudden changes in available disk space or memory
- emails being returned unexpectedly
- unexpected network connectivity difficulties
- frequent system crashes
- abnormal hard drive or processor activity
- unexpected changes to browser, software or user settings, including permissions.

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

Access for visitors

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

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

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.

Upgrades and software maintenance

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

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

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

Effective maintenance of software depends on the identification, planning and execution of measures necessary to support maintenance activities throughout the full software lifecycle. An industry standard[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.

Anti-virus and anti-malware tool updates

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

Remote access

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

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

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

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 on board, need to log onto systems using these privileges. In any case, use of administrator privileges should always be limited to functions requiring such access.

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

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

To protect access to confidential data and safety critical systems, a robust password policy should be developed[17]. Passwords should be strong and changed periodically. The company policy should address the fact that over-complicated passwords, which must be changed too frequently, are at risk of being written on a piece of paper and kept near the computer.

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 were 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 brute force remote management services successfully. 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; it must help ensure that media devices are not normally used to transfer information between un-controlled and controlled systems.

There are, however, situations where it is unavoidable to use these media devices, for example during software maintenance. In such cases, there should be a procedure in place to check 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,

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

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 the following file types:

- 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 lists
- 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.

Obtaining support from ashore and contingency plans

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

6 Establish contingency plans

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

Any cyber incident should be assessed in accordance with chapter 4 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 business continuity issue and should not have any impact on the safe operation of the ship. In the event of a cyber incident affecting IT systems only, the priority may be the immediate implementation of an investigation and recovery plan.

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 safety management system.

Some of the existing procedures in the ship's safety management system 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.

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. Disconnecting will help prevent the attacker from being able to manipulate safety critical systems or take direct control of the system. 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 in such a way that the networks can be physically segregated quickly by removing a single network cable (eg marked in an odd color) or powering off the firewall.

Safety management system

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

The following is a non-exhaustive list of cyber incidents, which should be addressed in contingency plans on board:

- 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 or 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 be available in a non-electronic form as some types of cyber incidents can include the deletion of data and shutdown of communication links.

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

7 Respond to and recover from cyber security incidents

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

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

7.1 Effective response

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

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

1. Initial assessment. To help ensure an appropriate response, the response team should find out:
    - how the incident occurred
    - which IT and/or OT systems were affected and how
    - the extent to which the commercial and/or operational data is affected
    - to what extent any threat to IT and OT remains.
2. Recover systems and data. Following an initial assessment of the cyber incident, IT and OT systems and data should be cleaned, recovered and restored, so far as is possible, to an operational condition by removing threats from the system and restoring software. The content of a recovery plan is covered in section 7.2.
3. Investigate the incident. To understand the causes and consequences of a cyber incident, an investigation should be undertaken by the company, with support from an external expert, if appropriate. The information from an investigation will play a significant role in preventing a potential recurrence. Investigations into cyber incidents are covered in section 7.3.
4. Prevent a re-occurrence. Considering the outcome of the investigation mentioned above, actions to address any inadequacies in technical and/or procedural protection measures should be considered, in accordance with the company procedures for implementation of corrective action.

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
- the appropriate use of any advanced tools provided in pre-installed security software
- the extent to which the incident has compromised IT or OT systems beyond the capabilities of existing recovery plans.

It is important for relevant personnel to execute regular cyber security exercises in order to help keep the response capability effective. Cyber security exercises could, where appropriate, be inspired by real-life events and can be simulations of large-scale incidents that escalate to become cyber crises. This offers an opportunity to analyse advanced technical cyber security incidents, but also to help address business continuity and crisis management.

7.2 Recovery plan

Recovery plans should be available in hard copy on board and ashore. The purpose of the plan is to support the recovery of systems and data necessary to restore IT and OT to an operational state. To help ensure the safety of onboard personnel, the operation and navigation of the ship should be prioritised in the plan. The recovery plan should be understood by personnel responsible for cyber security. The detail and complexity of a recovery plan will depend on the type of ship and the IT, OT and other systems installed on board.

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

As explained in section 5.1, 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.

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.

7.3 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.

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[18]:

- 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.

7.4 Losses arising from a cyber incident

For insurers, the term "cyber" includes many different aspects and it is important to distinguish between them and their effects on insurance cover. Some insurers believe that there is no systemic risk to ships arising from a cyber incident and the impact of an incident will most likely be confined to a single ship.

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

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

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

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

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

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

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

Cover for liability

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

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

ANNEX 1 Target systems, equipment and technologies

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

Communication systems

- integrated communication systems
- satellite communication equipment
- Voice Over Internet Protocols (VOIP) equipment
- wireless 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)
- Global Maritime Distress and Safety System (GMDSS)
- radar equipment
- Voyage Data Recorders (VDRs)
- other monitoring and data collection systems.

Propulsion and machinery management and power control systems

- engine governor
- power management
- integrated control system
- alarm system
- emergency response system.

Access control systems

- surveillance systems such as CCTV network
- Bridge Navigational Watch Alarm System (BNWAS)
- Shipboard Security Alarm Systems (SSAS)
- 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 sensing systems
- level indication system
- valve remote control system
- ballast water systems
- water ingress alarm system.

Passenger or visitor servicing and management systems

- Property Management System (PMS)
- 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.

Passenger-facing networks

- passenger Wi-Fi or Local Area Network (LAN) internet access, for example where onboard personnel can connect their own devices[19]
- 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.

[19] 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 so as to address cyber risk management in an approved SMS.

IDENTIFY[20]

Roles and responsibilities[21]	
Action	**Remarks**
ISM Code: 3.2 Industry Guidelines: 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 Industry Guidelines: 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[22] 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 Industry Guidelines: 5.2 Using existing company procedures, identify any training which may be required to support the incorporation of cyber risk management into the SMS.	Cyber awareness training is not a mandatory requirement. Notwithstanding this, training is a protection and control measure that forms the basis of CRM. It helps to ensure that personnel understand how their actions will influence the effectiveness of the company's approach to CRM. Existing company procedures for identifying training requirements should be used to assess the benefits and need for: ■ all company personnel to receive basic cyber awareness training in support of the company's CRM policies and procedures ■ company personnel, who have been assigned CRM duties, to receive a type and level of cyber training appropriate to their responsibility and authority.

Identify systems, assets, data and capabilities that, when disrupted, pose risks to ship operations	
Action	**Remarks**
ISM Code: 10.3 Industry Guidelines: 3 & 4 Using existing company procedures, identify equipment and technical systems (OT and IT) the sudden operational failure of which may result in hazardous situations.	An approved SMS will already identify the equipment and technical systems (including OT and IT), and capabilities, which may cause hazardous situations if they become unavailable or unreliable. The impacts should already have been documented in an approved SMS. However, an approved SMS, which incorporates CRM will also need to address data in the context of sudden operational failure. Loss of availability or integrity of data used by critical systems can have the same impact on safety and protection of the environment as the system becoming unavailable or unreliable for some other reason. Consequently, it is recommended that the list of equipment and technical systems, should be supplemented by a list of the data used by those systems and its source(s).

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

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

[22] 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 Industry Guidelines: 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 authorized and unauthorized devices on company controlled networks. The SMS should include procedures for maintaining this inventory throughout the operational life of the ship. ■ Software inventory – Develop and maintain a register of all authorized and unauthorized software running on company-controlled hardware onboard, including version and update status. The SMS should be updated to include procedures for: • maintaining this inventory when hardware controlled by the company is replaced • maintaining this inventory when software controlled by the company is updated or changed • authorizing the installation of new or upgraded software on hardware controlled by the company • prevention of installation of unauthorized software, and deletion of such software if identified • software maintenance. ■ Map data flows – Map data flows between critical systems and other equipment/technical systems on board and ashore, including those provided by third parties. Vulnerabilities identified during this process should be recorded and securely retained by the company. The SMS should be updated to include procedures for: • maintaining the map of data flows to reflect changes in hardware, software and/or connectivity • identifying and responding to vulnerabilities introduced when new data flows are created following the installation of new hardware • reviewing the need for connectivity between critical systems and other OT and IT systems. Such a review should be based on the principle that systems should only be connected where there is a need for the safe and efficient operation of the ship, or to enable planned maintenance • controlling the use of removable media, access points and the creation of ad-hoc or uncontrolled data flows. This may be achieved by restrictions on the use of removable media and disabling USB and similar ports on critical systems. ■ Implement secure configurations for all hardware controlled by the company – This should include documenting and maintaining commonly accepted security configuration standards for all authorized hardware and software. The SMS should include policies on the allocation and use of administrative privileges by ship and shore-based personnel, and third parties. However, it is not recommended that the details of secure configurations are included in the SMS. This information should be retained separately and securely by the company. ■ Audit logs – Security logs should be maintained and periodically reviewed. Security logging should be enabled on all critical systems with this capability. The SMS should be updated to include procedures for: • policies and procedures for the maintenance of security logs and periodic review by competent personnel as part of the operational maintenance routine • procedures for the collation and retention of security logs by the company, if appropriate. ■ Awareness and training – See line 3 above. ■ Physical security – The physical security of the ship is enhanced by compliance with the security measures addressed in the ship security plan (SSP) required by the ISPS Code. Measures should be taken to restrict access and prevent unauthorized access to critical system network infrastructure onboard.

Develop contingency plans	
Action	**Remarks**
ISM Code: 7 Industry Guidelines: 6 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 Industry Guidelines: 6 Update emergency plans to include responses to cyber incidents.	An approved SMS should already address emergency plans for the disruption of critical systems required for the safe operation of ships and protection of the environment. In general, these plans should be unaffected by the incorporation of cyber risk management into safety management systems. This is because the effect of common shipboard emergencies should be independent of the root cause. For example, a fire may be caused by equipment malfunctioning because of a software failure or inappropriate maintenance or operation of the equipment. Notwithstanding the above, consideration should be given to the development of a cyber incident module in the integrated system of shipboard emergency plans for significant disruption to the availability of OT or the data used by them. The purpose of the module could be to provide information on the actions to be taken in the event of a simultaneous disruption to multiple OT systems required for the safe operation of the ship and protection of the environment. In this more complex situation, additional information on appropriate immediate actions to be taken in response may be necessary.

DETECT

Develop and implement activities necessary to detect a cyber-event in a timely manner	
Action	**Remarks**
ISM Code: 9.1 Industry Guidelines: 5.1 Update procedures for reporting non-conformities, accidents and hazardous situations to include reports relating to cyber incidents.	An approved SMS should already address procedures relating to non-conformities. When incorporating CRM into the SMS, company reporting requirements for non-conformities may need to be updated to include cyber related non-conformities. Examples of such non-conformities and cyber incidents: ■ unauthorised access to network infrastructure ■ unauthorized or inappropriate use of administrator privileges ■ suspicious network activity ■ unauthorised access to critical systems ■ unauthorised use of removable media ■ unauthorised connection of personal devices ■ failure to comply with software maintenance procedures ■ failure to apply malware and network protection updates ■ loss or disruption to the availability of critical systems ■ loss or disruption to the availability of data required by critical systems.

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 Industry Guidelines: 7.1 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, if and when the need arises ■ internal audits should confirm that adequate resources, including third parties when appropriate, are available to provide support in a timely manner to support the DPA.
ISM Code: 9.2 Industry Guidelines: 7.1 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 Industry Guidelines: 7.1 Update the specific measures aimed at promoting the reliability of OT.	An approved SMS should already include procedures for operational maintenance routines to promote the reliability of equipment on board. A SMS, which incorporates CRM, should outline procedures for: ■ Software maintenance as a part of operational maintenance routines – Such procedures should ensure that application of software updates, including security patches, are applied and tested in a timely manner, by a competent person. ■ Authorizing remote access, if necessary and appropriate, to critical systems for software or other maintenance tasks – This should include authorizing access in general (including verification that service providers have taken appropriate protective measures themselves) and for each specific remote access session. ■ Preventing the application of software updates by service providers using uncontrolled or infected removable media. ■ Periodic inspection of the information provided by critical systems to operators and confirmation of the accuracy of this information when critical systems are in a known state. ■ Controlled use of administrator privileges to limit software maintenance tasks to competent personnel.

RECOVERY

Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber incident	
Action	**Remarks**
ISM Code: 10.4 Industry Guidelines: 5.1 and 7.2 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

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

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

Physical layout

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

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

Onboard networks should normally accommodate the following:

1. necessary communication between OT equipment
2. configuration and monitoring of OT equipment
3. onboard administrative and business tasks including email and sharing business related files or folders (IT networks)
4. recreational internet access for crew and/or passengers/visitors.

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

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

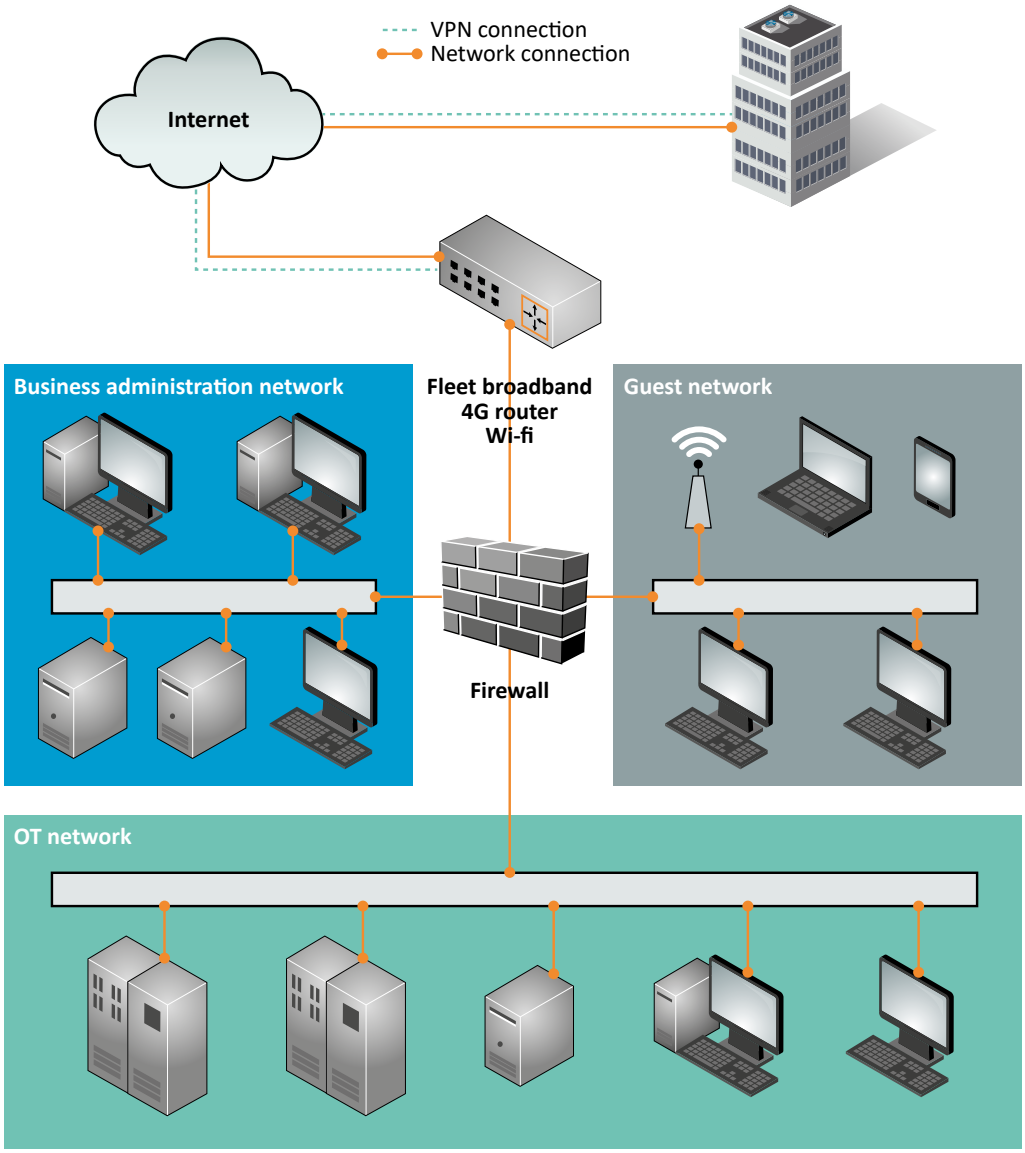

Figure 2: Example of an onboard network

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 and guest network, providing uncontrolled internet access.

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

A correctly configured and appropriate firewall is an 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 to monitor and manage systems to be aware of the networks' status and to detect any unauthorised data traffic. Logging should be implemented in the firewall and ideally in all network-attached devices so that in case of a breach, the responsible person can trace back the source and methodology of the attack. This will help to secure the network from any similar attacks in the future.

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

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

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 OT 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 an OT 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 chapter 5.1 defence-in-depth). In addition, an effective defence-in-depth strategy requires a thorough understanding of possible attack vectors on an OT system. These may include:

- backdoors and holes in network perimeter and instruments
- vulnerabilities in commonly used protocols

- vulnerable endpoints and sensors
- unprotected databases.

A secure running environment can be established by using a sandbox, 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 secret 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.

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 actually or potentially 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 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.

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.

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

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.

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

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 program may be executed without affecting the underlying system (computer or operating system) and any other applications. A sandbox is often used when executing untrusted software.

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.

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 program 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 version 3 of the guidelines

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

Anglo-Eastern Group
Aspida
BIMCO
Chamber of Shipping of America (CSA)
ClassNK
COLUMBIA Shipmanagement Ltd
Cruise Lines International Association (CLIA)
CyberKeel
International Association of Dry Cargo Shipowners (INTERCARGO)
International Association of Independent Tanker Owners (INTERTANKO)
International Chamber of Shipping (ICS)
International group of Protection & Indemnity clubs
International Union of Marine Insurance (IUMI)
InterManager
Maersk Line
Moran Shipping Agencies, Inc.
NCC Group
Oil Companies International Marine Forum (OCIMF)
SOFTimpact Ltd
Templar Executives
World Shipping Council