THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

Produced and supported by

hamber of hipping of merica Digital ontainership ssociation nternational ssociation of Dry argo hipowners N R R nter anager nternational ssociation of ndependent anker wners N R N nternational hamber of hipping nternational Union of arine nsurance U il ompanies nternational arine orum uperyacht uilders ssociation ybass and orld hipping ouncil

BIMCO

CHAMBER OF SHIPPING OF AMERICA

dcsa

INTERCARGO
International Association of Dry Cargo Shipowners

InterManager

INTERTANKO

International Chamber of Shipping
Shaping the Future of Shipping

IUMI
International Union of Marine Insurance

OCIMF

SYBAss
SUPERYACHT BUILDERS ASSOCIATION

WORLD SHIPPING COUNCIL
PARTNERS IN TRADE

v4

Contents

Introduction

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

hipping is relying increasingly on digital solutions for the completion of everyday tasks. he rapid developments within information technology data availability the speed of processing and data transfer present shipowners and other players in the maritime industry with increased possibilities for operational optimisation cost savings safety improvements and a more sustainable business. owever these developments to a large extent rely on increased connectivity o en via internet between servers systems and systems[1] which increases the potential cyber vulnerabilities and risks.

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

pproaches to cyber risk management will be company and ship specific but should be guided by the re uirements of relevant national international and ag state regulations and guidelines. n the nternational aritime rgani ation adopted resolution . on aritime yber Risk anagement in afety anagement ystem . he resolution stated that an approved should consider cyber risk management in accordance with the ob ectives and functional re uirements of the nternational afety anagement ode. t further encourages administrations to ensure that cyber risks are appropriately addressed in no later than the first annual verification of the company s Document of ompliance Do a er anuary . he same year developed guidelines[2] that provide high level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. s also highlighted in the guidelines effective cyber risk management should start at the senior management level. enior management should embed a culture of cyber risk management into all levels and departments of an organisation and ensure a holistic and exible cyber risk governance regime which is in continuous operation and constantly evaluated through effective feedback mechanisms.

n addition to the resolution the U. . National nstitute of tandards and echnology N ybersecurity ramework Version . pril has also been taken into account in the development of these guidelines. he N ybersecurity ramework assists companies with their approach to risk assessments by helping them understand an effective approach to manage potential cyber risks both internally and externally. s a result of applying the ramework a profile is developed which can help to identify and prioritise actions for reducing cyber risks. he profile can also be used as a tool for aligning policy business and technological decisions to manage the risks. ample framework profiles are publicly available for maritime bulk li uid transfer offshore and

perational echnology systems include hardware and so ware which monitor and or control physical devices processes and events. nformation echnology systems include hardware and so ware which manages data ie systems do not control physical devices processes or events).

. irc. on uidelines on maritime cyber risk management.

passenger ship operations[3]. hese profiles were created by the United tates oast uard and N s National ybersecurity enter of xcellence with input from industry stakeholders. he N s profiles can be used together with these guidelines to assist industry in assessing prioriti ing and mitigating their cyber risks.

uidelines are also available from other associations such as the Digital ontainer hipping ssociation s D D mplementation uide for yber ecurity on Vessels v . . he D s guidelines are based on an analysis of version of these guidelines and the N framework. hile the target audience for D s guidelines is the container industry other segments of shipping may also find them worthwhile to read.

he nternational ssociation for lassification ocieties has issued a Recommendation on yber Resilience No. . his recommendation consolidates previous recommendations related to cyber resilience Nos. to and applies to the use of computer based systems which provide control alarm monitoring safety or internal communication functions that are sub ect to the re uirements of a classification society. he recommendation applies to newbuild ships only but can also serve as guidance for existing ships. n due course is expected to develop Unified Re uirements which will also apply to newbuilds only. his publication is not intended to provide a basis for and should not be interpreted as calling for external auditing or ve ng the individual company s and ship s approach to cyber risk management.

[3] he N ramework Profiles for maritime bulk li uid transfer offshore and passenger operations can be accessed here **h ps www nist ov cyberframework**.

1 Cyber security and risk management

yber security characteristics of the maritime industry

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

yber incidents can arise as the result of eg

- a cyber security incident which affects the availability and integrity of for example corruption of chart data held in an lectronic hart Display and nformation ystem D
- an unintended system failure occurring during so ware maintenance and patching for example through the use of an infected U drive to complete the maintenance
- loss of or manipulation of external sensor data critical for the operation of a ship. his includes but is not limited to lobal Navigation atellite ystems N of which the lobal Positioning ystem P is the most fre uently used.
- failure of a system due to so ware crashes and or bugs
- crew interaction with phishing a empts which is the most common a ack vector by threat actors which could lead to the loss of sensitive data and the introduction of malware to shipboard systems.

he maritime industry has a range of characteristics that affect its vulnerability to cyber incidents. hese include

- involvement of multiple stakeholders in the operation and chartering of a ship potentially resulting in lack of accountability for the and system infrastructure and ship s networks
- use of legacy and systems that are no longer supported and or that rely on obsolete operating systems
- use of systems that cannot be patched or run anti virus due to type approval issues
- ships that interface online with shoreside parties and other parts of the global supply chain
- ship e uipment that is remotely monitored and accessed eg by the manufacturers or support providers
- the sharing of business critical data sensitive and commercially sensitive information with shore based service providers including marine terminals and stevedores and also where applicable public authorities
- the availability and use of computer controlled critical systems which may not have the latest patches installed or be properly secured for the ship s safety and for environmental protection
- a cyber risk management culture that still has potential for improvement eg through more formalised training exercises and clarified roles and responsibilities
- fre uently the automation system comprises of multiple sub systems from numerous vendors that are integrated by shipyards with minimal regard to cyber issues.

hese elements should be considered and relevant parts incorporated into the company cyber security policies and .

he growing use of comprehensive data analysis smart ships and the ndustrial nternet of hings o will increase the amount of information available to threat actors and the potential a ack

surface to cyber criminals. his necessitates robust approaches to cyber risk management[4].

yber risk management should be an inherent part of a company s safety and security culture conducive to the safe and e cient operation of the ship and be implemented at various levels of the company including senior management ashore and onboard personnel. yber 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 that if disrupted could pose risks to the ship s operations and safety
- implement technical and procedural measures to protect against a cyber incident timely detection of incidents and ensure continuity of operations
- a contingency plan which is regularly exercised.

ome aspects of cyber risk management may include commercially sensitive or confidential information for example the cyber risk assessment and its associated hardware and so ware inventories and network maps. ompanies should therefore consider protecting this information appropriately and as far as possible not include sensitive information in their .

loyd s Register ineti and University of outhampton lobal arine echnology rends .

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

Development implementation and maintenance of a cyber risk management programme in accordance with the approach in figure is no small undertaking. t is therefore important that senior management stays engaged throughout the process to ensure that the protection and contingency planning are balanced to manage risks within an acceptable limit. actors such as impact likelihood vulnerabilities threats capability opportunity and intent of malicious actors are interrelated see figure and are all relevant when assessing risk. t follows that if either of the factors is low or even ero the same will eventually apply to the risk. t is important to emphasi e that risk assessment is not a one time activity. t must be repeated at regular intervals to assess whether threats vulnerabilities likelihoods impacts and risks have changed and if the control measures are still appropriate.

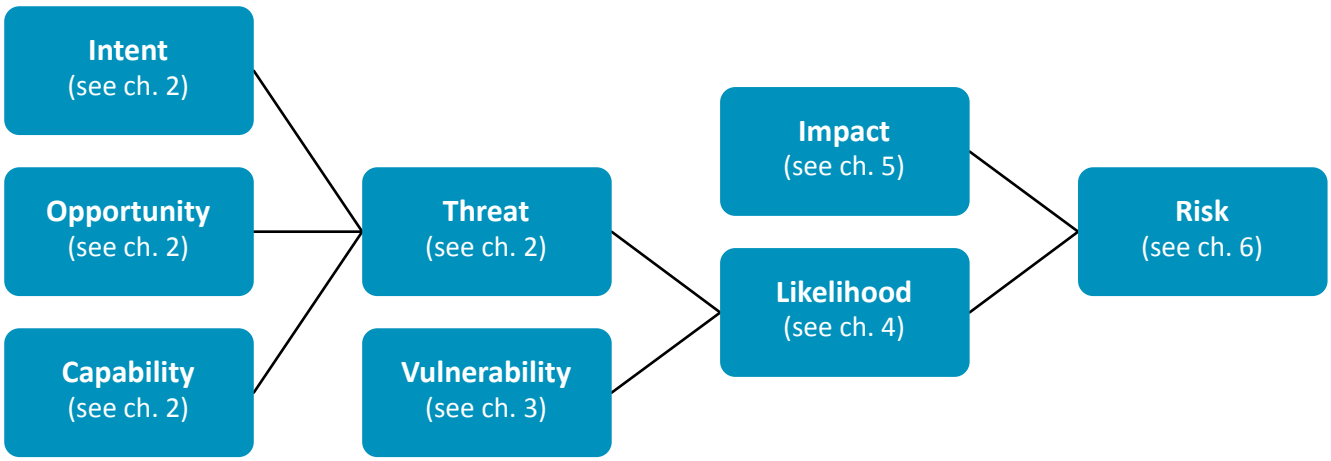

Figure 2: The relationship between different factors influencing the risk. The lines represent multiplication, ie "Likelihood" is multiplied with "Impact" to produce "Risk".

1.2 Senior management involvement

yber risk management should involve the senior management level of a company on an ongoing basis instead of for example only the ship security o cer or the manager. here are several reasons for this

- ome cyber risks have wide ranging destructive potential to the safety of personnel and the environment as well as the performance and reputation of the company. yber risks are therefore not simply security challenges but business challenges that re uire leadership s involvement.
- nitiatives to heighten cyber security and safety may affect standard business procedures and operations by rendering them more time consuming and or costly. t is therefore a senior management decision to evaluate and allocate the necessary resources to establish risk mitigation to an acceptable level of residual risk.
- nitiatives which heighten cyber awareness may change how the company interacts with unions customers suppliers and authorities and impose new re uirements on the co operation between parties. t is a senior management decision whether to drive these changes in relationships and how best to do so.

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

- hat assets are at risk
- hat is the potential impact of a cyber incident to the business customers partners and stakeholders
- ho has the final responsibility for cyber risk management
- re the systems and their working environment protected from unauthori ed access and changes
- s there remote access to the systems and if so how is it monitored and protected
- re the systems protected and is access being monitored and managed
- hat cyber risk management best practices are being used
- hat is the cyber risk training level of the personnel operating the and systems

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

oles responsibilities and tasks

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

he various responsibilities and tasks should be mapped to the ob descriptions and or role descriptions found in the . s cyber risk management planning and execution involves the whole company it may be useful during the mapping process to clarify who is the responsible person and who is re uired to support that person. or example a ship manager may well be the responsible party for cyber risk management in ships but he relies on support from other managers and staff from across the whole company eg security staff safety staff training staff procurement staff marine R staff crew etc.

en the allocation of responsibilities and tasks will work best if it is aligned with the normal chain of command. or example when allocating the responsibility for compliance with cyber risk management procedures on board a ship it will o en make sense to appoint the aster or the hief Engineer.

Task ole person	Cyber input to safety security policy	Cyber risk assessment on ship OT systems	Cyber risk assessment on ship IT systems	Ship IT infrastructure management	Crew cyber risk management training
Managing director	Responsible				
ompany manager	upporting		upporting		
Ship IT manager	upporting	Responsible	Responsible	Responsible	
afety manager	upporting	upporting	upporting	upporting	upporting
Procurement manager	upporting			upporting	
Fleet manager		upporting	upporting	upporting	upporting
Training manager			upporting		upporting
Marine HR manager			upporting		Responsible

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

4 Di erences between IT and OT systems

hereas systems manage data and support business functions is the hardware and so ware that directly monitors controls physical devices and processes and as such are an integral part of the ship and must function independently of the systems onboard. he systems can however be connected to the network for performance monitoring remote support etc. uch systems are sometimes referred to as belonging to the ndustrial nternet of hings . n such cases it must be ensured that the interface is su ciently guarded by a firewall as a minimum and potential

vulnerabilities in the systems are not exposed in the network. his is important because it is not always possible or feasible to ensure a proper patch level in systems.

covers the spectrum of technologies for information processing including so ware hardware and communication technologies. raditionally and have been separated but with the internet and are coming closer as historically stand alone systems are becoming integrated. Disruption of the operation of systems may impose significant risk to the safety of onboard personnel cargo damage to the marine environment and impede the ship s operation. ikewise failure of certain systems eg lack of immediate access to dangerous goods manifest could also result in ha ardous situations. or example in situations where a container aboard ship is on fire information about the contents of ad acent containers is critical for proper firefighting.

here may be important differences between who handles the purchase and management of the systems versus systems on a ship. managers are not usually involved in the purchase of systems and may or may not have a thorough understanding of cyber security. he purchase of such systems should involve someone who knows about the impact on the onboard systems but will most probably only have limited knowledge of so ware and cyber risk management. t is therefore important to have a dialogue with an individual knowledgeable of cyber security to ensure that cyber risks are considered during the purchasing process. Updating of so ware re uires a thorough compatibility check and class approval as opposed to so ware which is normally updated routinely. o obtain an overview of potential challenges and to help establish the necessary policy and procedures for so ware maintenance it can be an advantage for the party responsible for cyber security on board the ship to have an inventory of systems.

1.5 Plans and procedures

Resolution . identifies an urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping which is operationally resilient to cyber risks. hus all maritime stakeholders should work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities. he resolution furthermore a rms that the should consider cyber risk management in accordance with the ob ectives and functional re uirements of the ode.

he st session of s aritime afety ommi ee the report from this meeting is found in document agreed that aspects of cyber risk management including physical security aspects of cyber security should be addressed in hip ecurity Plans P under the P ode however this should not be considered as re uiring a company to establish a separate cyber security management system operating in parallel with the company afety anagement ystem .

n the same meeting also confirmed that resolution . on aritime cyber risk management in set out s re uirements for dministrations to ensure that cyber risks were appropriately addressed in existing as defined in the ode verified by an endorsed Document of ompliance and afety anagement ertificate and that in the hip ecurity Plan reference should be made to cyber risk management procedures found in .

or a company a simple way of arranging procedures as re uired by could be to re ect the following in the hip ecurity Plan P

- procedures related to physical access to areas with and systems
- a reference to the cyber security procedures.
  onsideration should be given to wording the reference in a way that will not re uire it to be updated every time a cyber security related procedure in the is amended added or removed as changes to the P would normally re uire approval from lag tate or the Recognised rganisation authorised to do so by the lag tate.

ccordingly the remaining procedures on cyber risk management should be re ected in the whilst excluding sensitive information such as the system s documentation described in section . of the present guidelines that could be exploited by malicious actors outside the company.

he already includes procedures for reporting accidents or ha ardous situations and defines levels of communication and authority for decision making. f needed such procedures should be amended to re ect communication and authority in the event of a cyber incident. he aster must have a defined resource to refer to in the event of a cyber incident and the should include a well designed response plan for cyber contingencies see chapter .

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

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

he company should consider if there is need for ship specific risk assessments based on whether particular ships or groups of ships are configured uni uely in terms setup within their eet. he factors to be considered include but are not limited to the extent to which and are used on board the complexity of system integration and the nature of operations. imilarly consideration should be given to whether procedures in the can be arranged to cover the company s eet or whether specific procedures are re uired for specific ships.

he cyber risk assessment and the and systems documentation described in section . are considered sensitive information. hile there is no regulation describing how this information should be stored the recommendation is for it to be stored and controlled in a similar manner as the hip ecurity ssessment and hip ecurity Plan.

elationship between shipowner and ship mana er

he Document of ompliance Do holder is ultimately responsible for ensuring the management of cyber risks on board. f the ship is under third party management then the ship manager is advised to reach an agreement with the shipowner.

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

part from re uirements such an agreement should take into consideration additional applicable legislation like the U eneral Data Protection Regulation DPR or specific cyber regulations in other coastal states as appropriate. anagers and owners should consider using these guidelines as a base for an open discussion on how best to implement an e cient cyber risk management regime.

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

elationship between the shipowner and the a ent

he importance of this relationship has placed the agent[5] 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. he relationship goes beyond that of a vendor. t can take different forms and especially in the tramp trade shipowners re uire a local representative an independent ship agent to serve as an extension of the company.

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

I IDE T Ship agent and shipowner ransomware incident

shipowner reported that the company s business networks were infected with ransomware apparently from a phishing email a achment. he source of the ransomware was from two unwi ng ship agents in separate ports and on separate occasions. hips were also affected but the damage was limited to the business networks while navigation and ship operations were unaffected. n one case the owner paid the ransom[6].

he importance of this incident is that harmoni ed cyber security across relationships with trusted business partners and manufacturers is critical to all in the supply chain. ndividual efforts to fortify one s own business can be valiant and well intended but could also be insu cient. Parties in the supply chain should work together and share information as appropriate to mitigate cyber risk.

elationship with vendors and other e ternal parties

ompanies should evaluate the physical security and cyber risk management processes of their interaction with service providers vendors and other external parties including public authorities.

ack of physical and or cyber security at a supplier vendor or service provider may result in a breach of corporate systems and or corruption of ship systems. he company should therefore consider entering into supplier vendor service provider agreements and contracts that define cyber related re uirements and expectations as appropriate. ompanies should also evaluate the cyber risk management processes for both new and existing contracts. roadly recognised standards exist eg ervice rgani ation ontrol ype but the company can also define its own standards.

he processes evaluated during supplier ve ng and included in contract re uirements may involve

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

---

he party representing the ship s owner and or charterer the Principal in port. f 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 re uirements of the aster 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 onvention on acilitation of nternational aritime ra c onvention .

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

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

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

he following should be considered regarding manufacturers and third parties including vendors contractors and service providers

- anufacturers and service providers will and ability to implement effective and cost e cient cyber security best practice in their products and services which can be demonstrated in different ways eg by following the R yber Risk ode of Practice for Vendors of arine lectronic uipment and ervices and the associated implementation guidelines.[7]
- anufacturers and service providers cyber risk management awareness and procedures ome 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. hird party vendors and suppliers are increasingly being targeted by threat actors and have played a role in well publici ed cyber incidents over the years. hese companies should have an updated cyber risk management company policy which includes training and governance procedures for accessible and systems.
- he maturity of a third party s cyber risk management procedures he shipowner should uery the internal governance of cyber network security and seek to obtain a cyber risk management assurance when considering future contracts and services. his is particularly important when covering network security if the ship is to be interfaced with the third party such as a marine terminal stevedoring company or supplier for ongoing support and maintenance.

I IDE T Unrecognised virus in an ECDIS delays sailing

newbuild dry bulk ship was delayed from sailing for several days because its D was infected by a virus. he ship was designed for paperless navigation and was not carrying paper charts. he failure of the D appeared to be a technical disruption and was not recogni ed as a cyber issue by the ship s aster and o cers. manufacturer technician was re uired to visit the ship and a er spending a significant time in troubleshooting discovered that both D networks were infected with a virus. he virus was uarantined and the D computers were restored. he source and means of infection in this case are unknown. he delay in sailing and costs in repairs totalled in the hundreds of thousands of dollars U .

[7] he ode and the guidelines can be found at the website of omit nternational Radio aritime R h p cirm or publications.

2 Identify threats

2.1 Threat actors

hen identifying threats companies should consider any specific aspects of potential threat actors capability opportunity and intent to a ack. his can include using eg an external person or an insider as an unintentional middleman unknowingly carrying the threat eg on an infected U stick. nce identified threats should be considered alongside identified vulnerabilities to evaluate the likelihood of an a ack or incident taking place. ogether with the impact of a given incident the likelihood of the incident occurring produces the risk factor.

rganisations and individuals can constitute an intentional or even unintentional threat to the safety and security of a crew the environment and the ship. he following figure lists examples of threat actors and their possible motivations and ob ectives. he list is non exhaustive. uch threat actors will have varying degrees of skills and resources to potentially threaten the safety and security of ships and a company s ability to conduct its business

Group	otivation
Accidental actors	■ No malicious motive but still end up causing unintended harm through bad luck lack of knowledge or lack of care eg by inserting infected U in onboard or systems.
ctivists includin disgruntled employees)	■ revenge ■ disruption of operations ■ media a ention ■ reputational damage
Criminals	■ financial gain ■ commercial espionage ■ industrial espionage
Opportunists	■ the challenge ■ reputational gain ■ financial gain
States **State sponsored or anisations** **Terrorists**	■ political idealogical gain eg un controlled disruption to economies and critical national infrastructure ■ espionage ■ financial gain ■ commercial espionage ■ industrial espionage ■ commercial gain

Figure 4: Threat actors' motivation and objectives.

Types of cyber threats

n general there are two categories of cyber threats that may affect companies and ships

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

Untargeted attacks are likely to use tools and techni ues 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. xamples of some tools and techni ues that may be used in these circumstances include

- **Malware.** alicious so ware which is designed to access or damage a computer without the knowledge of the owner. here are various types of malware including tro ans ransomware spyware viruses and worms. Ransomware encrypts data on systems until a ransom has been paid. alware may also exploit known deficiencies and problems in outdated unpatched business so ware. he term exploit usually refers to the use of a so ware or code which is designed to take advantage of and manipulate a problem in another computer so ware or hardware. his problem can for example be a code bug system vulnerability improper design hardware malfunction and or error in protocol implementation. hese vulnerabilities may be exploited remotely or triggered locally eg a piece of malicious code may o en be executed by the user sometimes via links distributed in email a achments or through malicious websites.
- **Water holing.** stablishing a fake website or compromising a genuine website to exploit unsuspecting visitors.
- **Scanning.** earching large portions of the internet at random for vulnerabilities that could be exploited.
- **Typos ua n** lso called UR hi acking or fake UR . Relies on mistakes such as typos made by internet users when inpu ng a website address into a web browser. hould a user accidentally enter an incorrect website address they may be led to an alternative and o en malicious website.
- **Tar eted a acks** may be more sophisticated and use tools and techni ues specifically created for targeting a certain company or ship. xamples of tools and techni ues which may be used in these circumstances include
  - **Social engineering.** non technical techni ue used by potential cyber a ackers to manipulate insider individuals into breaking security procedures normally but not exclusively through interaction via social media.
  - **Brute force** n a ack trying many passwords with the hope of eventually guessing correctly. he a acker systematically checks all possible passwords until the correct one is found.
  - **redential stu n** Using previously compromised credentials or specific commonly used passwords to a empt unauthori ed access to a system or application.
  - **Denial of service Do** prevents legitimate and authorised users from accessing information usually by ooding a network with data. distributed denial of service DDo a ack takes control of multiple computers and or servers to implement a Do a ack.
  - **Phishing.** ending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information. he email may also contain a malicious a achment or re uest that a person visits a fake website using a hyperlink included in the email.
  - **Spear-phishing.** ike phishing but the individuals are targeted with personal emails o en containing malicious so ware or links that automatically download malicious so ware. n some instances messages have been used to establish a sense of familiarity with a

malicious sender s email address.

- **ubvertin the supply chain** acking a company or ship by compromising e uipment so ware or supporting services being delivered to the company or ship.

he above examples are not exhaustive. ther cyber a ack 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 a ack. he potential number and sophistication of tools and techni ues used in cyber a acks continue to evolve and are limited only by the ingenuity of those organisations and individuals developing them.

ta es of a cyber incident

n it took on average days between the time a victim s network was breached and the containment of the breach. owever intrusion can go undetected for years. his figure went up from days in [8]. he length of time to prepare a cyber a ack can be determined by the motivations and ob ectives of the a acker and the resilience of technical and procedural cyber risk controls implemented by the company including those onboard its ships. hen considering targeted cyber a acks the generally observed stages of an incident are

- **urvey reconnaissance** pen public sources such as social media are used to gain information about a potential target eg a company ship or seafarer in preparation for a cyber a ack. ocial media technical forums and hidden properties in websites documents and publications may be used to identify technical procedural and physical vulnerabilities. he use of open public sources may be complemented by monitoring analysing sni ng the actual data owing into and from a company or a ship.
- **Delivery.** ackers may a empt to access the company s and ship s systems and data. his may be done from either within the company or ship or remotely through connectivity with the internet. xamples 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 so ware update to an onboard system
  - creating false or misleading websites which encourage the disclosure of user account information by personnel.
- **Breach.** he extent to which an a acker can breach a company s or ship s system will depend on the significance of the vulnerability found by an a acker and the method chosen to deliver an a ack. t should be noted that a breach might not result in any obvious changes to the status of the e uipment. Depending on the significance of the breach an a acker may be able to
  - make changes that affect the system s operation for example interrupt or manipulate information used by navigation e uipment
  - gain access to take copies of or alter operationally important information such as loading lists or commercially sensitive data such as cargo manifests and or crew and passenger visitor lists
  - achieve full control of a system for example a machinery management system.
- **Pivot.** Pivoting is the techni ue of using an already compromised system to a ack other systems in the same network. During this phase of an a ack an a acker uses the first compromised system to a ack otherwise inaccessible systems. n a acker will usually target the most vulnerable part of the victim s system with the lowest level of security. nce access is gained then

8 IBM Cost of a Data breach Report 2019.

the a acker will try to exploit the rest of the system. Usually in the pivot phase the a acker may try to

- upload tools exploits and scripts in the system to support the a acker in the new a ack 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 a acks on the system.

he motivation and ob ectives of the a acker will determine what effect they have on the company or ship system and data. n a acker may explore systems expand access and or ensure that they are able to return to the system in order to

- access commercially sensitive or confidential data about cargo crew visitors and passengers
- manipulate crew or passenger visitor lists cargo manifests stow plans or loading lists. his may subse uently be used to allow the fraudulent transport of illegal cargo or facilitate the s
- cause complete denial of service on business and operational systems
- enable other forms of crime for example piracy the and fraud
- disrupt normal operation of the company and ship systems for example by deleting critical pre arrival or discharge information or overloading company systems
- demand a ransom for operational or personal data.

4 uantifyin the threat

General considerations

hreat is the product of the threat actor s capability opportunity and intent to cause harm. he purpose of uantifying the threat is to help the uantification of the likelihood which forms part of the assessment of risk that is the product of likelihood and impact. n other words if either the capability opportunity or intent of a threat actor is ero or close to ero the threat and thereby the risk will be small.

Threats against OT systems

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

ndications are that a acks targeted specifically against systems are less common and in many cases not publicised. Reasons for this are likely to be eg

- ost systems in the marine industry are still not connected to networks with external access ie threat exposure is low and cybercriminals have no opportunity to a ack. here are exceptions however for example many monitoring devices eg devices monitoring engine performance are connected to the internet and usually have minimal cyber security controls in place especially in comparison to or even systems. hese systems are referred to as ndustrial nternet of hings o and are becoming more integrated onboard ships to provide remote monitoring and connection of systems to allow for greater automation and e ciency in operations. hreat actors can scan for these systems and use them as initial point of infiltration to a ship network from which they can pivot as outlined previously. herefore risks to these systems are important to assess and should not be overlooked.
- systems normally have no direct potential for economically rewarding the cybercriminal.
- acking systems entail safety risks to the victims something which may constitute a disincentive and even a deterrent to some cybercriminals.

Despite the above the risks to systems should not be underestimated. hreats posed eg by malware introduced through so ware updates either online or through manual processes such as eg U sticks or through unregulated or unauthorised access by crew can still materialise and have been known to cause disruptions and operational downtime.

Threats against IT systems

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

3 Identify vulnerabilities

ommon vulnerabilities

he following are common cyber vulnerabilities which may be found onboard existing ships and on some newbuild[9] ships

- obsolete and unsupported operating systems
- unpatched system so ware
- outdated or missing antivirus so ware and protection from malware
- inade uate 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 e uipment or systems always connected with the shore side
- inade uate access controls to cyber assets networks etc for third parties including contractors and service providers
- staff inade uately trained and or skilled to manage cyber risks
- missing inade uate or untested contingency plans and procedures.

IT and OT systems documentation

o assist every step of the risk assessment the and systems need to be clearly identified with documented governance and ownership responsibilities within an asset register which shall be kept updated as appropriate. he asset register should include an asset valuation with the cost of the asset and the cost of maintaining that asset. Recommendation no. on yber Resilience is applicable to newbuilds only however it may nevertheless serve as guidance for the development of documentation that may include

- nventory of communicating devices
- inventory network communication devices
- logical map of networks
  - P addresses
  - non P addresses
  - non Ethernet access points
  - desktops and servers
  - connectors and communicating field devices
- so ware inventory in some cases this inventory is part of a hip o ware ogging ystem
- inventory of network services for each e uipment.

ools are available to handle the inventory of an system but not recommended for an system as the integrity of the system could be disrupted unless handled by a well ualified expert in close consultation with the aster hief ngineer etc .

[9] ith the publication of Recommendation on yber Resilience No. future newbuild ships may be less vulnerable.

3.3 Typical vulnerable systems

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

I IDE T rash of inte rated navi ation brid e system at sea

ship with an integrated navigation bridge system suffered a failure of nearly all navigation systems at sea in a high tra c area and reduced visibility. he ship had to navigate by one radar and backup paper charts for two days before arriving in port for repairs. he cause of the failure of all D computers was determined to be a ributed to the outdated operating systems. During the previous port call a manufacturer technical representative performed a navigation so ware update on the ship s navigation computers. owever the outdated operating systems were incapable of running the so ware and crashed. he ship was re uired to remain in port until new D computers could be installed classification surveyors could a end and a near miss notification had been issued as re uired by the company. he costs of the delays were extensive and incurred by the shipowner.

his incident emphasi es that not all computer failures are a result of a deliberate a ack and that outdated so ware is prone to failure. ore robust testing and proactive so ware maintenance on the ship may have prevented this incident from occurring.

he goal of an assessment of a ship s network and its systems and devices is to identify any vulnerabilities that could compromise or result in the loss of confidentiality integrity or availability of data and systems re uired to operate the e uipment system network or even the ship. hese vulnerabilities and weaknesses could fall into one of the following categories

- temporary exposures such as so ware defects outdated or unpatched systems
- design such as access management or unmanaged network interconnections
- implementation errors for example misconfigured firewalls
- procedural or other user errors.

tand alone systems will be less vulnerable to external cyber incidents compared to those a ached to uncontrolled networks or connected directly to the internet. Network design and network segregation will be explained in more detail in nnex . are should be taken to understand how critical shipboard systems might be connected to uncontrolled networks. he human element should be taken into consideration as many incidents are initiated by personnel s actions. nboard systems could include

- **Cargo and loading management systems.** Digital systems used for the loading management and control of cargo including ha ardous cargo may interface with a variety of systems ashore including ports marine terminals and stevedores. uch systems may include shipment tracking tools available to shippers via the internet. nterfaces of this kind make cargo management systems and data in cargo manifests and loading lists vulnerable to cyber incidents.
- **Bridge systems.** he increasing use of digital network navigation systems with interface to shoreside networks for update and provision of services make such systems vulnerable to cyber incidents. ridge systems that are not connected to other networks may be e ually vulnerable as removable media are o en used to update such systems from other controlled or uncontrolled networks. cyber incident can extend to service denial or manipulation and therefore may affect all systems associated with navigation including D N VDR and Radar RP .
- **Propulsion and machinery management and power control systems.** he use of digital systems to monitor and control onboard machinery propulsion and steering makes such systems vulnerable to cyber incidents. he vulnerability of these systems can increase when used in con unction with remote condition based monitoring and or are integrated with navigation and

communications e uipment on ships using integrated bridge systems.

- **Access control systems.** Digital systems used to support access control to ensure physical security and safety of a ship and its cargo including surveillance shipboard security alarm and electronic personnel on board systems are vulnerable to cyber incidents.
- **Passenger servicing and management systems.** Digital systems used for property management boarding and access control may hold valuable passenger related data. ntelligent devices tablets handheld scanners etc are themselves an a ack vector as ultimately the collected data is passed on to other systems.
- **assen er facin public networks** ixed 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.
- **dministrative and crew welfare systems** nboard computer networks used for administration of the ship or the welfare of the crew are particularly vulnerable when providing internet access and email. his can be exploited by cyber a ackers to gain access to onboard systems and data. hese systems should be considered uncontrolled and should not be connected to any safety critical system on board. o ware provided by ship management companies or owners is also included in this category.
- **ommunication systems** vailability of internet connectivity via satellite and or other wireless communication increases the vulnerability of ships and recent developments indicate that for example V signals are vulnerable to exploitation using low cost off the shelf products. ommunication systems with encryption should be considered. he 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. ncluded in these systems are communication links to public authorities for transmission of re uired ship and cargo reporting information. pplicable authentication and access control management re uirements by these authorities should be strictly complied with. lso included are shipboard capabilities to collect data from and interrogate devices and data loggers a xed to containers for onward transmission to designated recipients ashore see also section below on ship to shore interface .

he abovementioned onboard systems consist of potentially vulnerable e uipment which should be reviewed during the assessment. he vulnerability assessment can be assisted by answering the below uestions for each system

- s the system stand alone or is it connected to other systems
- s the system connected externally either directly or via other systems
- Does the system have effective built in risk mitigation measures such as eg encryption
- Does the system re uire regular so ware updates
- Does operating the system involve connecting removable devices for example to obtain diagnostic information
- s the system easy to physically access

4 hip to shore interface

hips 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 o ces. urthermore critical ship systems essential to the safety of navigation power and cargo management have become increasingly digitalised and connected to the internet to perform a wide variety of legitimate functions such as

- engine performance monitoring

- remote diagnostics
- maintenance and spare parts management
- cargo and container tracking and management loading and unloading and stowage planning
- crane and pump management
- monitoring of systems for adherence to environmental regulations and reporting
- voyage performance monitoring.

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

 odern technologies can add vulnerabilities to the ships especially if there are insecure designs of networks and uncontrolled access to the internet. dditionally shoreside and onboard personnel may be unaware how some e uipment manufacturers and so ware providers maintain remote access to shipboard e uipment 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.

 t is recommended that companies fully understand and document as appropriate the ship s and systems and how these systems connect and integrate with the shore side including public authorities marine terminals and stevedores. his re uires an understanding of all computer based onboard systems and how safety operations and business including cargo and load management can be compromised by a cyber incident.

3.5 Ship visits

Visits to ships by third parties re uiring a connection to one or more computers on board can also result in connecting the ship to shore. t is common for technicians vendors port and other o cials marine terminal representatives agents pilots and other technicians to board the ship and plug in devices such as laptops and tablets. ome technicians may re uire the use of removable media to update computers download data and or perform other tasks. t has also been known for customs o cials and port state control o cers to board a ship and re uest the use of a computer to print o cial documents a er having inserted an unknown removable media.

 ometimes 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. n such cases it is di cult to know if malicious so ware has been le in the onboard systems. t is recommended that sensitive data is removed from the ship and reinstalled on returning to the ship and at the very least there should be a back up of data. here possible systems should be scanned for malware prior to use. systems should be tested to check that they are functioning correctly.

3.6 Remote access

 ome and systems are remotely accessible and may operate with a continuous internet connection for remote monitoring data collection maintenance functions safety and security. hese systems can be third party systems whereby the contractor remotely monitors and maintains the systems. hese systems could include a two way data ow and or upload only. ystems and workstations with remote control access or configuration functions could for example be

- bridge and engine room computers and workstations on the ship s administrative network
- cargo such as containers with reefer temperature control systems or specialised cargo that are tracked remotely

- stability decision support systems
- hull stress monitoring systems
- navigational systems including lectronic Navigation hart N Voyage Data Recorder VDR dynamic positioning DP
- load planning stowage and cargo management
- engine monitoring and control
- safety and security networks such as V closed circuit television
- specialised systems such as drilling operations blow out preventers subsea installation systems mergency hut Down D for gas tankers submarine cable installation and repair.

he extent and nature of connectivity of e uipment should be known by the shipowner or operator and considered as an important part of the risk assessment.

ystem and so ware maintenance

and systems so ware and maintenance can be outsourced to third party service providers and the company itself may not be in a position to verify the level of security supplied by these providers. ome companies use different providers responsible for so ware and cyber security checks. n such cases the suppliers should be re uested to provide details of the updates.

I IDE T avi ation computer crash durin pilota e

ship was under pilotage when the D and voyage performance computers crashed. pilot was on the bridge. he computer failures brie y created a distraction to the watch o cers however the pilot and the aster worked together to focus the bridge team on safe navigation by visual means and radar. hen the computers were rebooted it was apparent that the operating systems were outdated and unsupported. he aster reported that these computer problems were fre uent referred to the issues as gremlins and that repeated re uests for servicing from the shipowner had been ignored.

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

4 Assessing the likelihood

4 ikelihood as the product of threat and vulnerability

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

4 uantifyin the likelihood

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

Level	ikelihood description
1	Never heard of in industry. lose to being something unimaginable.
2	eard of in industry but only extremely rarely and as the result of a chain of many unfortunate events.
3	ncident has probably occurred in own company but in the context of faulty e uipment or by surprising mistakes made by people involved.
4	appens occasionally in own company typically in the context of faulty e uipment or by mistakes by people involved the kind of mistakes that tend to happen on board from time to time .
5	appens fre uently when undertaking the work in uestion.

Figure 5: Example of likelihood scale from an SMS.

n an ideal world uantifying the likelihood would be substantiated by access to shipping specific industry wide threat intelligence based on incident reports. owever such threat intelligence is not immediately available and it is therefore worthwhile to look to other sectors than shipping as threat actors fre uently repurpose techni ues previously used to a ack one sector to target another sector. urthermore it will o en be worthwhile to look closer at the threat factors capability opportunity and intent. ooking especially at intent can be useful as ero intent will uantify a given potential threat as theoretical and therefore produce only a small likelihood when uxtaposed against or multiplied with the vulnerability.

5 Impact assessment

5.1 The CIA model

he confidentiality integrity and availability model[10] provides a framework for assessing the impact of

- loss of confidentiality of information eg unauthorised access to and disclosure of information or data about the ship crew cargo and passengers
- loss of integrity which would modify information and data relating to the safe and e cient operation and management of the ship
- loss of availability due to the destruction of the information and data and or the disruption to services operation of ship systems.

he relative importance of confidentiality integrity and availability depends on the use of the information or data. onversely assessing the vulnerability of systems onboard ships particularly safety critical systems may focus on availability and or integrity instead of confidentiality.

uantifyin the impact

company s will normally contain a risk assessment matrix where the impact of a given event is measured on a five step scale of increasingly serious impacts to different categories eg safety of personnel safety of environment cargo safety asset safety business continuity financial impact and company s reputation. Using the s existing impact scale can be an advantage because using existing language and concepts to describe cyber related risks will ease the understanding throughout the company. f this scale has not been used to describe impacts arising out of cyber risks it may be necessary to modify the verbal description of each of the impact levels. Using such a scale also allows the company to distinguish between different ships in the eet according to their criticality to the company s overall activities. ne example of such a scale can be found below

Level	Impact description
1	No health effect in uries. No damage to environment assets finances or company s reputation.
2	Very slight health effect in uries. Very slight damage to environment assets finances or to company s reputation.
3	ome health effect minor in uries. inor damage to environment assets finances or to company s reputation.
4	a or health effect relatively serious in uries. ocal but ma or damage to environment assets finances or to company s reputation.
5	atality or permanent disabilities. idespread significant damage to environment assets finances or company s reputation.

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

here are also several other assessment methodologies that can help define the magnitude of the

10 ederal nformation Processing tandards Publication omputer ecurity Division nformation echnology aboratory National nstitute of tandards and echnology aithersburg D .

impact from a cyber incident eg the example in figure [11]

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

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

ritical e uipment and technical systems

he impact assessment should be carried out for every system on board. or systems such an impact assessment also forms part of the list of e uipment and technical systems the sudden operational failure of which may more or less promptly result in ha ardous situations which is re uired by paragraph . of the ode o en referred to as critical e uipment and technical systems .

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

11 ethodologies include and are not limited to nformation technology ecurity techni ues nformation security risk management nterprise Risk anagement ramework and Risk management uidelines.

E ample

ship is e uipped with a complex power management system. t consists of switchboards and generators controlling systems for auto load sharing power control and auto synchroni ing. n top of the power management system a supervisory control and data ac uisition D 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. t also has a clear environmental and financial impact as power is generated by use of fuel either by the ship s main engine sha generator and or auxiliary engines. herefore a cyber incident that disables or causes the power management system to malfunction can place the operation and safety of the ship at risk. o lower the risk the company should add protection measures that minimi e the possibility of such a cyber incident taking place.

he D system contains real time sensor data which is used on board for power management. t also generates data about the power consumption which is used by the shipping company for administrative purposes. o determine if the potential impact of data and information is being breached the model should be used. hen doing so the shipping company should determine the potential impact of the most sensitive information stored processed or transmi ed by the D system.

Using the model the shipping company can conclude that

- losing confidentiality of the sensor data ac uired by the D system will have a low impact as the sensors are publicly displayed on board. owever from a safety point of view it is important that the information transmi ed by the sensors can be relied upon. herefore there is a potential high impact from a loss of integrity. t will also be a safety issue if the information cannot be read. o 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. here will also be a potential low impact from a loss of integrity and availability as the data is only used for in house considerations.

he following figure shows the result of the assessment

SCADA system	onfidentiality	Integrity	Availability	Overall impact
Sensor data	Low	High	High	High
tatistical data	Low	Low	Low	Low

Figure 8: Result of CIA assessment of SCADA system.

6 Risk assessment

elationship between factors in uencin risk

nly a er having established an overview of threats intent capability and opportunity vulnerabilities impacts and likelihood is it then possible to conduct the risk assessment. risk assessment is not a one off activity but should be repeated at appropriate intervals to ensure that the risk assessment s findings are kept up to date.

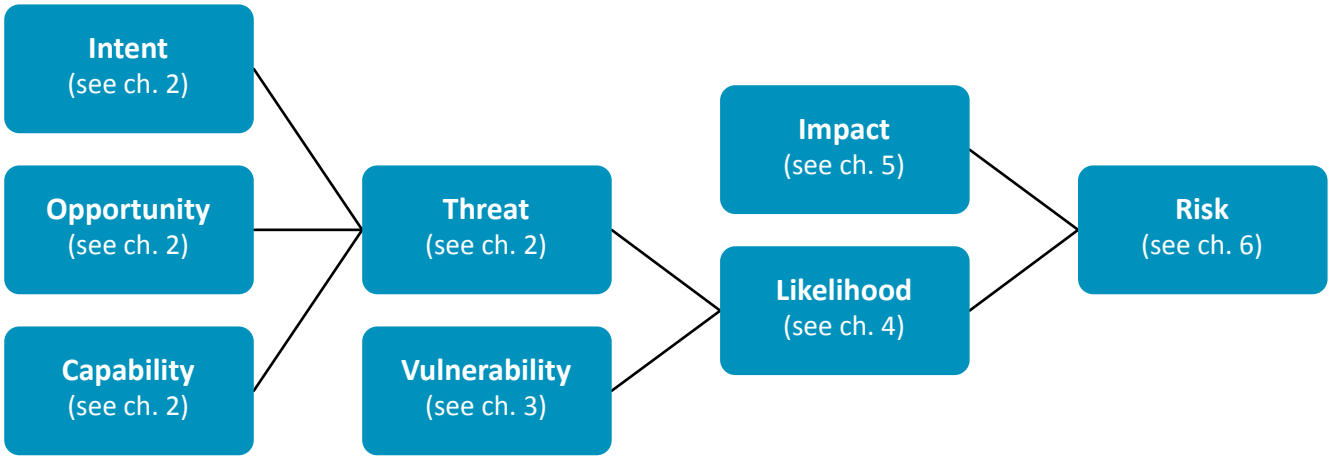

Figure 9: The relationship between different factors influencing the risk. The lines represent multiplication, ie "Likelihood" is multiplied with "Impact" to produce "Risk".

The four phases of a risk assessment

hase re-assessment activities

Risk assessments apply to existing ships as well as newbuilds and second hand ships entering the eet. ssessment of cyber risks is a complex undertaking which re uires detailed knowledge about cyber risk management and third party support to the risk assessment process is likely to be re uired in some cases.

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

- Review the documentation of and systems as described in . and assess potential impact levels for example using the model see . . .
- dentify main manufacturers of critical shipboard and e uipment a risk based approach should be used in this identification process .
- dentify cyber security points of contact with the most important manufacturers and establish a working relationship with them.
- Review detailed documentation on the ship s maintenance and support of the and systems.
- stablish contractual re uirements and obligations that the shipowner ship operator may have for maintenance and support of shipboard networks and e uipment.

hase hip assessment

hen all risk factors threats vulnerabilities likelihood and impact are assessed the risk assessment and associate risk mitigation can be carried out. he risk assessment is a systematic consideration of relevant risk factors.

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

he identification and implementation of mitigation measures based on risk assessments is well established on all ships via the code and the company . owever cyber risk assessments should not be confused with the operational risk assessments normally carried out by the crew as per the . yber risk assessments are a more complex undertaking that will uite likely re uire the involvement of o ce staff and possibly even third party consultants depending on the level of complexity.

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

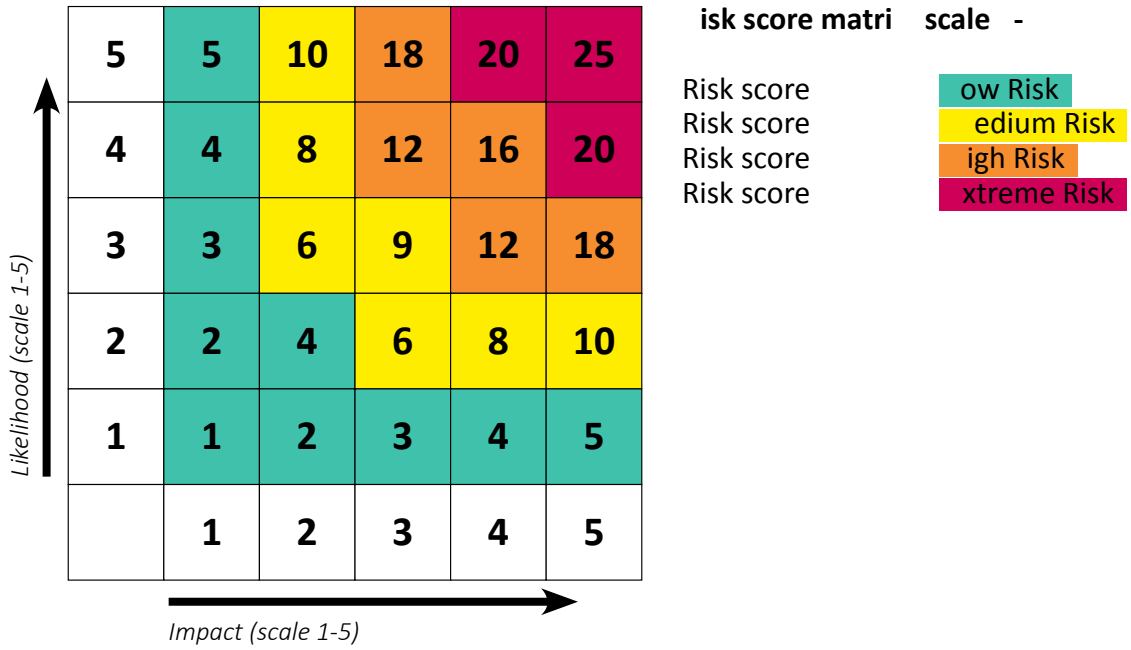

Figure 10: Example of a company's risk score matrix.

f the calculated initial risk for a given system is above what is acceptable in accordance with the company s risk acceptance criteria the risk must be mitigated for the residual risk to reach an acceptable level as demonstrated in the following example

System	Impact	Likelihood	Initial risk	iti ation	Residual risk
ECDIS	**Score 5** due to risk of catastrophic events like grounding and collision	**Score 4** due to active U ports computer used for other purposes connection to admin network for access to shared printer connection to automatic chart updates via satellite via trusted vendor	Risk x	Password protect and restrict P use to D only	Risk x
				Disconnect from admin network	Risk x
				lind off U ports	Risk x

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

lthough carried out system by system the risk assessment for the ship as a whole will re uire a holistic approach cognisant of the fact that some potential risk mitigation measures suggested for one system may impact on the risk assessment of other systems. holistic approach will ensure that risk mitigation measures are selected according to their impact to the different systems that are o en connected and of course their cost effectiveness. Different risk mitigation measures are described in more detail in the subse uent chapters of the present guidelines.

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

n aspect of onboard ship assessment is the involvement of crew of all levels particularly the aster hief ngineer and first mate. his process assists to understand the implementation of the and systems onboard and how they may vary from stated design documentation and to understand the level of cyber training to be delivered to the ship s crew.

or obvious reasons selection of mitigation measures depends on the resources available and the nature of the risk. ome mitigation measures eg procedural changes may be e ually as effective as expensive technical solutions. specially for existing ships with legacy systems technical solutions can be di cult and expensive to implement.

ssessing the effectiveness of different risk mitigation measures should be an integral part of the risk assessment process.

t can also be considered to categorise different risk mitigation measures so it becomes easier to understand and provide guidelines on which controls to use and where.

hase Debrief and reportin

o satisfy the re uirements of the ode the risk assessment should be a coherent and up to date document which re ect how risks are assessed and mitigated. Producing such a risk assessment will o en be an iterative process where different mitigation measures are considered in different combinations until a decision can be made to the optimal composition of the risk mitigation measured in terms of legal re uirements risk appetite feasibility effectiveness and cost.

f the risk assessment is carried out by an external party eg if su cient expertise is unavailable held in house the initial report of the external party is likely to be an interim account in which recommendations are made. nce recommendations have been considered and a final decision has been taken this should be re ected in the final risk assessment.

n initial third party cyber risk assessment could for example include the following

- **e ecutive summary** a high level summary of results recommendations and the overall security profile of the assessed ship
- **technical findin s** breakdown of discovered vulnerabilities their probability of exploitation the monetary cost of exploitation the resulting impact on the crew ship and environment and appropriate technical fix and mitigation advice
- **prioritised list of actions** the priorities allocated should re ect the effectiveness of the measure the cost the applicability etc. t is important that this list should be a complete list of options available and not represent a list of services and products which the third party risk assessor if applicable would like to sell.
- **supplementary data** a supplement containing the technical details of all key findings and comprehensive analysis of critical aws. his section should also include sample data recovered during the penetration testing if any of critical or high risk vulnerabilities

- **appendices** record of activities conducted and tools used by the cyber risk assessment team.

hase 4 anufacturer s debrief

nce the shipowner has had an opportunity to review discuss and assess the findings a subset of the findings may need to be sent to the manufacturers of the effected systems in order to reduce or mitigate the risk. ny findings eg any identified cyber vulnerability in the factory standard configuration of a critical system or component could be further analysed with support from external experts who should work with the manufacturer s cyber security point of contact to ensure that a full risk and technical understanding of the problem is achieved. his supporting activity is intended to ensure that any remediation plan developed by the manufacturer is comprehensive in nature and identifies the correct solution to eliminate the vulnerabilities.

6.3 Third party risk assessments

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

hird party risk assessment can also include penetration tests of critical and infrastructure to identify whether the actual defence level matches the desired level set forth in the cyber security strategy for the company. uch tests can simulate incidents using both systems social engineering and if desired even physical penetration of a facility s security perimeter. hese tests are referred to as active tests because they involve accessing and potentially inserting so ware into a system. his may only be appropriate for systems. here risk to systems during penetration testing is unacceptable passive testing approaches should be considered. Passive methods rely on scanning data transmi ed by a system to identify vulnerabilities. n general no a empt should be made to actively access or insert so ware into the system.

hird party risk assessments are a valuable way of integrating speciali ed skills and field expertise to perform varying tasks in the overall effort of managing and remediating cyber risk. hese assessments are also beneficial to companies with limited personnel resources to perform ob ective and transparent cyber risk assessments. hoosing third parties to assist in these activities also allows stakeholders to learn from multiple perspectives and perform due diligence empowering them to make informed and confident choices.

hile penetration testing has been viewed as a way of determining if networks and systems can be compromised there are numerous other ways of building the foundation of understanding of one s own organisation s and eet s environments that can also be performed. hese services could include asset discovery and inventory on networks to assist shipowners and operators with understanding what is connected where and with whom. hird parties may also perform network architecture reviews and design to understand and audit current design as well as spot where improvements can be made in cost effective and sensible ways. Vulnerability assessments can be performed as a deeper dive and a broader look to even include passive network scanning. Penetration testing is intrusive carries more risk is largely more expensive and re uires an understanding of networks and inventoried assets. Penetration testing should be reserved for more specific circumstances and technical action. s in any other service it is important for the supervising o cers and shoreside staff to coordinate these activities for safety purposes and to choose third party services with eet awareness and experience.

7 Develop protection measures

Defence in depth and in breadth

Defence in depth

t is important to protect critical systems and data with multiple layers of protection measures which consider the role of personnel procedures and technology to

- increase the probability that a cyber incident is detected
- make the best use of resources re uired to protect confidentiality integrity and availability of data in and systems.

onnected systems on board should re uire 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 su cient to cope with insider threats.

his defence in depth approach encourages a combination of

- physical security of the ship in accordance with the ship security plan P
- protection of networks including effective segmentation
- intrusion detection
- use of firewall
- periodic vulnerability scanning and testing
- so ware whitelisting
- access and user controls
- configuration and change management controls
- appropriate procedures regarding the use of removable media and password policies
- personnel s cyber security awareness and understanding of the risk to themselves and the industry
- understanding and familiarity with appropriate procedures including incident response.

ompany policies and procedures should help ensure that cyber security is considered within the overall approach to safety and security risk management. he complexity and potential persistence of cyber threats means that a defence in depth approach should be considered. uipment and data protected by layers of protection measures are more resilient to cyber incidents.

Defence in breadth

hen 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 . or 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.

owever onboard ships where levels of integration between and 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. his is defence in breadth and it is used to prevent any vulnerabilities in one system being used to circumvent protection measures of another system.

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

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

Technical protection measures

yber risk protection measures may be technical and focused on ensuring that onboard systems are designed and configured to be resilient to cyber incidents. onsideration needs to be given to implementing technical controls that are practical and cost effective particularly on existing ships. t should be noted that implementation of technical control measures is not a one off activity. nce implemented they should be kept up to date to avoid risk of failure.

he entre for nternet ecurity provides guidance on measures[12] that can be used to address cyber security vulnerabilities. he protection measures are a list of ritical ecurity ontrols that are prioritised and ve ed to help ensure that they provide an effective approach for companies to assess and improve their defences. he s include both technical and procedural aspects.

he below mentioned examples of s have been selected as particularly relevant to e uipment and data onboard ships[13].

imitation to and control of network ports protocols and services

ccess lists to network systems can be used to implement the company s security policy. his helps ensure that only appropriate tra c will be allowed via a controlled network or subnet based on the control policy of that network or subnet.

t is recommended that routers are secured against incidents and unused ports should be closed to prevent unauthorised access to systems or data.

onfi uration of network devices such as firewalls routers and switches

t should be determined which systems should be a ached to controlled or uncontrolled[14] networks. ontrolled networks are designed to prevent any security risks from connected devices by use of firewalls security gateways routers and switches. Uncontrolled networks may pose risks due to lack of data tra c control and should be isolated from controlled networks as direct internet connection makes them highly prone to infiltration by malware. or example

- networks that are critical to the operation of a ship itself should be controlled. t is important that these systems have a high level of security
- networks that provide suppliers with remote access to navigation and other systems so ware on board should also be controlled. t may be necessary to allow suppliers to upload system upgrades or perform remote servicing on these networks. horeside external access points of such connections should be secured to prevent unauthorised access
- cargo stowage load planning and cargo and container management systems should be controlled.
  - o 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.

12 ritical ecurity ontrols for ffective yber ecurity available at **www cisecurity or critical-controls cfm**.

13 tephenson arwood yber Risk.

14 n accordance with aritime navigation and radiocommunication e uipment and systems Digital interfaces Part ultiple talkers and multiple listeners thernet interconnection afety and security.

ffective segregation of systems based on necessary access and trust levels is one of the most successful strategies for the prevention of cyber incidents. ffectively segregated networks can significantly impede an a acker s access to a ship s systems and is one of the most effective techni ues for preventing the spread of malware. nboard networks should be partitioned by firewalls to create safe ones. irewall configurations should be reviewed regularly to detect unauthorised changes. he fewer communications links and devices in a one the more secure the systems and data are in that one. onfidential and safety critical systems should be in the most protected one. ee annex of these guidelines for more information on shipboard networks and also refer to as well as Recommendation no. on yber Resilience.

I IDE T Worm incident on maritime IT and OT

ship was e uipped with a power management system that could be connected to the internet for so ware updates and patching remote diagnostics data collection and remote operation. he ship was built recently but this system was not connected to the internet by design.

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

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

he worm spread via U devices into a running process which executes a programme into the memory. his programme was designed to communicate with its command and control server to receive its next set of instructions. t could even create files and folders.

he company asked cyber security professionals to conduct forensic analysis and remediation. t was determined that all servers associated with the e uipment were infected and that the virus had been in the system undiscovered for days. canning tools removed the virus. n 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 U ash drive during a so ware installation.

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

Physical security

Physical security[15] is sometimes the simplest cheapest and most obvious form of cyber defence. t is a central aspect of cyber risk management and an effective defence in depth strategy should aim to ensure that physical control measures cannot be circumvented. reas containing sensitive or control components should be securely locked security and safety critical e uipment and cable runs should be protected from unauthorised access and physical access to sensitive user e uipment such as exposed U ports on bridge systems should be secured. n the hip ecurity Plan such areas will be defined as Restricted reas as re uired by the P ode Part section . . taking into account the guidance in the ode s part . his is particularly relevant to places that are normally unmanned in port such as the bridge.

atellite and radio communication

yber security of the radio and satellite connection should be considered in collaboration with the service provider. n this connection the specification of the satellite link should be considered when establishing the re uirements for onboard network protection.

15 ee also the P ode.

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

Protection against eavesdropping is typically done by means of Virtual Private Network VPN connection or encrypted protocols. hile protection against hacking piercing and other types of a ack can be achieved by other means such as a security arrangement with the service provider connection through a secure server ashore for example owned by the company or an onboard firewall.

ne important aspect of cyber security is to make the satellite terminal invisible. his can be achieved by deactivating functions such as remote administration page and port forward . Deactivation can typically be done in the terminal s se ngs menu.

hen establishing a connection for a ship s navigation and control systems to shore based service providers consideration should be given on how to prevent illegitimate connections gaining access to the onboard systems. t is advised that a public P address should not be published and routable directly to a ship from the internet. onnections from the internet should route through a shoreside network and firewall for routing and access control. second consideration is the close monitoring of outbound connections originating from ship networks control networks or networks that have a connection to control networks ie reverse tunnel connections .

he access interconnect is the distribution partner s responsibility. he final routing of user tra c from the internet access point to its ultimate destination onboard last mile is the responsibility of the shipowner. User tra c is routed through the communication e uipment for onward transmission onboard. t the access point for this tra c it is necessary to provide data security firewalling and a dedicated last mile connection.

hen using a Virtual Private Network VPN the data tra c should be encrypted to an acceptable international standard. urthermore a firewall in front of the servers and computers connected to the networks ashore or on board should be deployed. he distribution partner should advise on the routing and type of connection most suited for specific tra c. nshore filtering inspection blocking of tra c is also a ma er between a shipowner and the distribution partner. oth onshore filtering of tra c and firewalls security inspection blocking gateways on the ship are needed and supplement each other to achieve a su cient level of protection.

anufacturers of satellite communication terminals and other communication e uipment may provide management interfaces with security control so ware that are accessible over the network. his 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. xamples of protection of administrative interfaces include limiting networks that can access such interfaces whether they are web based or command line or entirely disabling unnecessary interfaces that are only used during initial configuration. s for other systems the passwords should be managed appropriately eg default passwords which are o en well known to criminals should be changed.

Wireless access control

ireless access to networks on the ship should be limited to appropriate authorised devices and secured using a strong encryption key which is changed regularly. he 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 eg guest networks isolated from administrative networks
- the adoption of systems such as wireless P that can intercept non authori ed wireless access points or rogue devices. Using network access control N to profile devices corporate versus personal and control wireless network access is effective at managing access

- the protection of the physical interconnection between wireless access devices and the network such as network plugs network racks etc to avoid unauthori ed access by rogue devices.

ecure confi uration of hardware and so ware

User profiles should be restricted to only allow the computers workstations or servers to be used for the purposes for which they are re uired. User profiles should not allow the user to alter the systems or install and execute new programmes.

Email and web browser protection

ny email and web browser protection should

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

ome best practices for safe email transfer are emails as ip or encrypted files when necessary disable hyperlinks on email system avoid using generic email addresses and ensure the system has configured user accounts.

pplication so ware security patch mana ement

ecurity updates should be provided to onboard systems and it is recommended to develop a so ware and hardware patching roadmap. ecurity patches should be included in the periodic maintenance cycle and it is recommended to pay special a ention to e uipment utili ed to do virtual network segregation V N and firewalling. hese updates or patches should be applied correctly and in a timely manner to ensure that any vulnerabilities in a system are addressed before they are exploited and available to hackers. t can be complicated and expensive to patch some systems because all so ware and hardware firmware needs to be aligned and thorough tests must be conducted post installation to validate the integrity. n other cases security patches may not be applicable without upgrading system hardware partly or completely. or those reasons systems are not updated so fre uently or not at all. nd it is important to assess the compatibility and potential operational impact on the systems prior to any patches are installed. f a critical patch cannot be installed alternative measures should be evaluated to ensure the vulnerabilities are not exposed in larger networks or ultimately the internet. his could be a combination of physical protection limiting network access and implementation of virtual patching techni ues.

rocedural protection measures

Protection measures may also be procedural and should be covered by company policies safety management procedures security procedures and access controls. s with all other control measures only procedural controls that are practical and cost effective should be implemented. Procedural controls are focused on how personnel use the onboard systems. Plans and procedures that contain sensitive information should be kept confidential and handled according to company policies.

xamples for procedural actions can be

Training and awareness

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

he internal cyber threat should be considered. Personnel have a key role in protecting and 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.

raining and awareness should be tailored to the appropriate levels for

- onboard personnel including the aster o cers and crew
- shoreside personnel who support the management loading stowage and operation of the ship.

he onvention[16] re uires companies to ensure that seafarers are familiari ed with all ship arrangements installations e uipment procedures and ships characteristics that are relevant to their routine or emergency duties and that the ship s compliment can effectively coordinate their activities in an emergency situation and in performing functions vital to safety or to the protection or mitigation of pollution. he managing as appropriate of cyber risks fall within the scope of the convention.

n addition to the familiari ation training of seafarers re uired by the convention an awareness programme should be in place for all onboard personnel according to their role covering for example some of the following

- risks related to emails and how to behave in a safe manner. xamples are phishing a acks where the user clicks on a link to a malicious site or opens a malicious a achment
- risks related to internet usage including social media chat forums and cloud based file storage where data movement is less controlled and monitored
- risks related to geolocation data for personnel and ship that is publicly available
- risks related to the use of own devices. hese 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 so ware on company hardware using infected hardware removable media or so ware infected package
- risks related to poor so ware 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 le to work on e uipment without supervision
- detecting suspicious activity or devices and how to report a possible cyber incident. xamples of this are strange connections that are not normally seen or someone plugging in an unknown device on the ship network
- awareness of the conse uences 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.

n addition personnel need to be made aware that the presence of anti malware so ware does not remove the re uirement for robust security procedures for example controlling the use of all removable media.

urther relevant personnel should know the signs when a computer has been compromised. his may include the following

- an unresponsive or slow to respond system

16 he nternational onvention on tandards of raining ertification and atchkeeping for eafarers as amended.

- unexpected password changes or authorised users being locked out of a system
- unexpected errors in programmes including failure to run correctly or programmes running unexpectedly
- unexpected or sudden changes in available disk space or memory
- emails being returned unexpectedly
- unexpected network connectivity di culties
- fre uent system crashes
- abnormal hard drive or processor activity
- unexpected changes to browser so ware or user se ngs including permissions.

Designated personnel should be able to understand reports from ntrusion Detection ystems if used. his list is not comprehensive and is intended to raise awareness of potential signs which should be treated as possible cyber incidents.

hese guidelines assume that other ma or 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. t 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.

omputer access for visitors

Visitors such as authorities technicians agents port and terminal o cials and owner representatives should be restricted regarding computer access whilst on board. Unauthorised access to sensitive computers should be prohibited. f access to a network by a visitor is re uired and allowed then it should be restricted in terms of user privileges and conducted under supervision. ccess to certain networks for maintenance reasons should be approved and co ordinated following appropriate procedures as outlined by the company ship operator.

f a visitor re uires computer and printer access an independent computer isolated from all controlled networks should be used. o avoid unauthorised access removable media blockers should be used on all other physically accessible computers and network ports.

I IDE T Bunker surveyor s access to a ship s administrative network

dry bulk ship in port had ust completed bunkering operations. he bunker surveyor boarded the ship and re uested permission to access a computer in the engine control room to print documents for signature. he surveyor inserted a U drive into the computer and unwi ngly introduced malware onto the ship s administrative network. he malware went undetected until a cyber assessment was conducted on the ship later and a er the crew had reported a computer issue affecting the business networks.

his emphasises the need for procedures to prevent or restrict the use of U devices onboard including those belonging to visitors.

Crew's personal devices

Procedures must be in place to provide instructions to crew about the use of devices for personal and leisure purposes. his should include how to utilise the ship s communication networks for personal means such as skype emails gaming video streaming without endangering critical or systems.

p rades and so ware maintenance

ardware or so ware that is no longer supported by its manufacturer or so ware developer will

not receive updates to address potential vulnerabilities. or this reason the use of hardware and so ware which is no longer supported should be carefully evaluated by the company as part of the cyber risk assessment.

Relevant hardware and so ware installations on board should be updated to help maintain a su cient level of security. Procedures for timely updating of so ware may need to be put in place taking into account the ship type speed of internet connectivity sea time etc. o ware includes computer operating systems which should also be kept up to date. dditionally a number of routers switches and firewalls and various devices will be running their own firmware which may re uire regular updates that should be addressed in the procedural re uirements.

ffective maintenance of so ware depends on the identification planning and execution of measures necessary to support maintenance activities throughout the full so ware lifecycle. n industry standard[17] to help ensure safe and secure so ware maintenance has been developed. t specifies re uirements for all stakeholders involved in so ware maintenance of shipboard e uipment and associated integrated systems. he standard covers on board on shore and remote so ware maintenance.

nti-virus and anti-malware tool mana ement

canning so ware tools used to detect and deal with malware need to be kept up to date and managed. Procedural re uirements 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 and systems. lear guidelines should establish who has permission to access when they can access and what they can access. ny procedures for remote access should include close co ordination with the ship s aster and other key senior ship personnel.

ll remote access occurrences should be recorded for review in case of a disruption to an or system. ystems which re uire remote access should be clearly defined monitored and reviewed periodically.

se of administrator privile es

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

dministrator privileges allow full access to system configuration se ngs and all data. Users logging onto systems with administrator privileges may enable existing vulnerabilities to be more easily exploited. dministrator privileges should only be given to appropriately trained personnel who as part of their role in the company or onboard need to log onto systems using these privileges. n any case use of administrator privileges should always be limited to functions re uiring such access.

User privileges should be removed when the person concerned is no longer onboard. User accounts should not be passed on from one user to the next using generic usernames. imilar rules should be applied to any onshore personnel with remote access to systems on ships when they change roles and no longer need access.

n a business environment such as shipping access to onboard systems is granted to various stakeholders. uppliers and contractors are a risk because they o en have both intimate knowledge of a ship s operations and full access to systems.

17 ee ndustry standard on so ware maintenance of shipboard e uipment by and R omit nternational Radio aritime .

ulti factor authentication F and passwords

o protect access to confidential data and safety critical systems a robust password policy in con unction with should be developed[18]. should be used as widely as possible ie for all appropriate levels. o reduce the chances of a brute force a ack passwords[19] should be strong and can be either user or machine generated. he company policy should address the fact that over complicated passwords which must be changed too fre uently are at risk of being wri en on a piece of paper and kept near the computer. Passwords should be supplemented with the use of which is based on something that you have eg a token or device and something that you know eg a password and something you are eg a fingerprint passcode on a phone. here is implemented the risk of a password being compromised is reduced as the token or device will not be in the possession of the threat actor who manages to obtain the password.

I IDE T ain application server infected by ransomware

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

he root cause of the infection was poor password policy that allowed a ackers to successfully brute force remote management services. he company s 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

hen 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 a ack systems that are otherwise not connected to the internet. 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 uncontrolled and controlled systems.

here are however situations where it is unavoidable to use these media devices for example during so ware maintenance. n such cases there should be a procedure in place to check removable media for malware and or validate legitimate so ware by digital signatures and watermarks.

Policies and procedures relating to the use of removable media should include a re uirement to scan any removable media device in a computer that is not connected to the ship s controlled networks. f it is not possible to scan the removable media on board eg the laptop of a maintenance technician then the scan could be done prior to boarding. ompanies should consider notifying ports and terminals about the re uirement to scan removable media prior to permi ng the uploading of files onto a ship s system. his scanning should be carried out when transferring files for example

- cargo files and loading plans eg container ship P files
- national customs and port authority forms
- bunkering and lubrication oil forms
- ship s stores and provisions list
- so ware update files
- engineering maintenance files.

his list represents examples and should not be seen as exhaustive. herever possible the files and

18 ore information can be found in N publication P Digital dentity uidelines.

19 h ps www ncsc ov uk collection passwords updatin -your-approach

forms should be transferred electronically or be downloaded directly from a trusted source without using removable media.

E uipment disposal includin data destruction

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

8 Develop detection measures

Detection blockin and alerts

Detecting intrusions and infections is a central part of cyber risk management. baseline of network operations and expected data ows for users and systems should be established and managed so that cyber incident alert thresholds can be established. ey to this will be the definition of roles and responsibilities for detection to help ensure accountability.

dditionally a company may choose to incorporate an ntrusion Detection ystem D or an ntrusion Prevention ystem P into the network or as part of the firewall. ome of their main functions include identifying threats malicious activity and code and then logging reporting and a empting to block the activity. urther details concerning D and P can be found in nnex of these guidelines. Relevant onboard personnel should be able to understand the alerts and their implications. nowledge of incidents detected should be directed to an individual or service provider who is responsible for acting on this type of alert.

alware detection

canning so ware that can automatically detect and address the presence of malware in systems onboard should be kept up to date and managed.

s a general guideline computers on board should be protected to the same level as o ce computers ashore. nti virus and anti malware so ware should be installed maintained and updated on all personal and work related computers onboard. his will reduce the risk of these computers acting as a ack vectors towards servers and other computers on the ship s network. ow regularly the scanning so ware will be updated must be taken into consideration when deciding whether to rely on these defence methods.

9 Establish contingency plans

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

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

he loss of systems may have a significant and immediate impact on the safe operation of the ship. hould a cyber incident result in the loss or malfunctioning of 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. n 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 . deally some of the existing procedures in the ship s will already cover such cyber incidents. owever cyber incidents may result in multiple failures causing more systems to shut down at the same time. he contingency planning should take such incidents into consideration.

he following is a sample non exhaustive list of cyber incidents which should be addressed in plans for onboard contingencies. rguably most of these incidents are probably already addressed in the company s procedures for dealing with shipboard emergencies as re uired by the ode s chapter mergency preparedness .

- loss of availability of electronic navigational e uipment or loss of integrity of navigation related data
- loss of availability or integrity of external data sources including but not limited to N
- loss of essential connectivity with the shore including but not limited to the availability of lobal aritime Distress and afety ystem D communications
- loss of availability of industrial control systems including propulsion auxiliary systems and other critical systems as well as loss of integrity of data management and control
- the event of a ransomware or denial of service incident.

urthermore it is important to help ensure that a loss of e uipment or reliable information due to a cyber incident does not make existing emergency plans and procedures ineffective. ontingency plans and related information should include communications and escalation management to ensure that the correct shore based support can be accessed and should be available in a non electronic form as some types of cyber incidents can include the deletion of data and shutdown of communication links.

ontingency plans should be carefully designed and simple and designated personnel ashore should be integrated with the ship in the event of a cyber incident. he aster and designated o cers should be provided with this plan to enable training and periodic review for familiarity.

Disconnectin OT from shore network connection

onnections between shore and systems can be relevant in a wide range of applications like performance monitoring predictive maintenance and remote support ust to mention a few.

ommon for these systems are that they are not strictly necessary for operating the ship safely.

owever they represent a potential a ack vector to the systems that are needed for the ship s safe operation. herefore it is relevant to assess when these connections are allowed and under what circumstances. Plans should be established specifying when such systems should be temporarily separated from the shore network connection to protect the ship s safe operation. Disconnecting will help prevent the a acker 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.

o 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 isolated uickly by removing a single network cable eg marked in an odd colour or powering off the firewall. his design and procedure should be provided by the responsible shoreside staff to the aster. raining should also be provided to aid the aster and o cers with understanding cyber threats. he crew should also be trained to operate the ship should there be a disconnection of . hese impacts should be known in advance tested and procedures developed for each ship.

10 Respond to and recover from cyber security incidents

E ective response

he starting point for effective response is the response plan covering relevant contingencies. owever it is unlikely that response plans will eventually match a cyber incident scenario as it unfolds. his is why it is important to regularly drill the response plan and develop contingencies according to lessons learned about the threats vulnerabilities and impacts. or most ships the contingency plans are already in place in the emergency procedures re uired by the ode . . .

yber incidents will re uire an active response to return the ship to operation. f for example the D has been infected with malware starting the backup D may cause another cyber incident. t is therefore recommended to build and rehearse an incident response plan detailing roles and responsibilities communications paths and core activities.

here may be occasions when responding to a cyber incident may be beyond the competencies on board or at head o ce due to the complexity or severity of such incidents. n these cases external expert assistance should be available to assist with multiple functions such as network activity anomalous behaviour of connected devices or the detection of non inventoried devices unauthori ed or uncoordinated accesses by vendors to critical systems and aspects of response and recovery such as post event forensic analysis and clean up .

o the extent available knowledge about previously identified cyber incidents in own eet as well as in other eets should be used to improve the response plans of all ships in the company s eet and an information strategy for such incidents may be considered.

The four phases of incident response

s determined by N there are four key phases to incident response

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

hase reparation

n accordance with previous advice in this guidance

- determine the critical components on the ship their prioriti ation and location
- ensure regular back up as appropriate of all relevant data
- identify single points of failure and define work arounds as necessary
- create an incident response plan and rehearse it regularly. he plan should include the roles and responsibilities of crew and personnel ashore as well as guidance on clear communication. he plan should also detail critical network and data recovery processes as necessary.

hase Detection and analysis

o help ensure an appropriate response the response team should find out wherever possible

- how the incident occurred

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

hase ontainment and eradication

ontaining the outbreak of an incident is a time critical exercise. here possible remove the device from the network. here this is not possible then it is important to uarantine the device from its V N or N and to ensure that boundary controls are operational between networks. urthermore

- heck the firewall rules have not changed. sophisticated a acker has the ability to open up network ports. here systems are internet V facing shut down remote access management ports.
- nsure that anti virus and anti malware definitions are up to date.
- ake a full disk image of any impacted systems. tore this securely in accordance with the hain of ustody for forensic investigation ashore. chain of custody process involves the identification labelling recording handling transportation access control and secure storage of the disk image.
- onsider taking memory dumps R image as this is important for forensics purposes. Note that restarting or powering off a computer will destroy volatile data like R so expert advice should be considered when dealing with threat eradication.

hase 4 ost-Incident recovery

- **ecover systems and data** ollowing an initial assessment of the cyber incident and 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 so ware. he content of a recovery plan is covered in section . .
- **Investi ate the incident** o understand the causes and conse uences of a cyber incident an investigation should be undertaken by the company with support from an external expert if appropriate. he information from the investigation will play a significant role in preventing a potential recurrence. nvestigations into cyber incidents are covered in section . .
- **revent a re-occurrence** onsidering the outcome of the investigation mentioned above actions to address any inade uacies in technical and or procedural protection measures should be considered in accordance with the company procedures for implementation of corrective action.

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

- whether or systems should be shut down or kept running to protect data
- whether certain ship communication links with the shore should be shut down and what the implications of such steps may be
- the appropriate use of any recovery tools provided in pre installed security so ware
- the extent to which the incident has compromised or systems beyond the capabilities of existing recovery plans.

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

10.3 Recovery plan

Recovery plans in hard copy onboard and ashore should be available to personnel responsible for cyber security and who are tasked with assisting in cyber incidents. he purpose of the plan is to support the recovery of systems and data necessary to restore and to an operational state. o help ensure the safety of onboard personnel the operation and navigation of the ship should be prioritised in the plan. he detail and complexity of a recovery plan will depend on the type of ship and the and other systems installed onboard.

he 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 on the causes of an incident. here appropriate professional cyber incident response support should be obtained to assist in preservation of evidence whilst restoring operational capability.

s explained in section . a data recovery capability is a valuable technical protection measure. Data recovery capabilities are normally in the form of so ware backup for data. he availability of a so ware backup either on board or ashore should enable recovery of to an operational condition following a cyber incident. ecause ransomware and worms have historically also spread to backup appliances the use of o ine backups should also be considered.

Recovery of may be more complex especially if there are no backup systems available and may re uire 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.

f ualified personnel are available on board more extensive diagnostic and recovery actions may be performed. therwise the recovery plan will be limited to obtaining uick access to technical support.

t is important that companies o en test their recovery procedures and the whole ship to shore collaboration on responding to a cyber incident.

10.4 Data recovery capability

Data recovery capability is the ability to restore a system and or data from a secure copy or image thereby allowing the restoration of a clean system. ssential information and so ware ade uate 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 uick restore capabilities to reduce the impact. ystems that have high data availability re uirements should be made resilient. systems which are vital to the safe navigation and operation of the ship should have backup systems to enable the ship to uickly and safely regain navigational and operational capabilities a er a cyber incident.

Investi atin cyber incidents

nvestigating a cyber incident can provide valuable information about the way in which a vulnerability was exploited. ompanies should wherever possible investigate cyber incidents affecting and on board in accordance with company procedures. detailed investigation may re uire external expert support.

here external support is re uired the full disk image taken during the containment phase can

be shared with the investigating team. y ensuring that the hain of ustody has been securely maintained any forensic evidence obtained will be permissible in court as the process demonstrates that evidence has not been tampered with.

he information from an investigation can be used to improve the technical and procedural protection measures on board and ashore. t may also help the wider maritime industry with a be er understanding of maritime cyber risks. ny investigation should result in[20]

- a be er 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.

osses arisin from a cyber incident

s cyber related risks become a part of the overall risk landscape marine insurers also face an increasing demand for insurance products and services against these cyber related risks. Risk assessment and risk mitigation is first and paramount and a precondition for granting insurance cover.

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

successful cyber incident can have several implications relevant to insurance loss of life personal in ury pollution loss damage to cargo cargo handling e uipment or of property business interruption liabilities loss of production loss of data loss of reputation and probably any conse uential damages. study carried out by loyd s of ondon in shows that cyber incident related risks are rapidly evolving and can become a systemic risk and as such there is not necessarily a one si e fits all approach to the monitoring and uantification of this risk. yber incident exposures are hence regularly underwri en with appropriate controls in place and aggregate exposures and limits monitored appropriately.

ompanies 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.

over for property dama e

nsurance solutions covering damages arising from cyber risks in general and cyber incidents in particular have to be developed within each individual company. he current status may be summari ed as follows

- ome local insurance markets still issue unbinding recommendations for certain lines of business excluding cyber related damages. istorically the most widely used exclusion has been for malicious cyber incidents nstitute yber ack xclusion lause . t is used across all marine sectors and activities cargo energy excess of loss hull liability specialty and war . nother widely used exclusion is the merican nstitute yber xclusion lause .
- ther market solutions may either explicitly insure the risk or in all risk policies do not exclude the risk and grant silent cover ie cyber risks are covered in the contract without being mentioned explicitly . owever it should be noted that the silent cover approach has increasingly

20 ased on R yber ecurity ncident Response uide Version .

come under scrutiny.[21]

- inally so called buy back solutions may include the risk under defined preconditions and against a negotiated additional premium. uy back means that the risk is excluded in the contract but there s an option to include again additional cyber coverage in the contract at certain conditions and against additional premium.

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

uidelines for the market have been published in which marine insurers are recommended to ask uestions about a company s cyber risk awareness and non technical procedures. ompanies should therefore expect a re uest for non technical information regarding their approach to cyber risk management from insurers.

over for liability

t is recommended to contact the P lub 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.

n incident caused for example by malfunction of a ship s navigation or mechanical systems because of a criminal act or accidental cyber incident does not in itself give rise to any exclusion of normal P cover. n the event of a claim involving a cyber incident claimants may well seek to argue that the claim arose as a result of an inade uate level of cyber preparedness. his 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.

t 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 insurance. or example financial loss caused by ransomware or costs of rebuilding scrambled data would not be identified in the coverage.

t should however be noted that normal P cover in respect of liabilities is sub ect to a war risk exclusion and cyber incidents in the context of a war or terror risk will not normally be covered.

21 n mid the **rudential** Regulation uthority PR in the U released a supervisory statement detailing its expectations expecting firms to be able to identify uantify and manage cyber insurance underwriting risk. ikewise global ratings agencies announced they expect companies to be proactive and forthcoming with their own evaluation and measurement of the exposure and accumulation of their cyber liability exposure. n une the nternational Underwriting ssociation U published cyber exclusion clauses U and U . he wordings have been developed in order to address issues of non a rmative or silent cover where traditional insurance policies may unintentionally suggest protection for undefined cyber risks. n November the loyd s arket ssociation published several new purely illustrative model clauses for the guidance of its members which shall provide clarity about cyber coverage under first party property damage policies Property D yber ndorsement Property D yber xclusion arine yber xclusion and arine yber ndorsement. he clauses relate to property direct and facultative business and marine business. he clauses shall provide a starting point for the market to address cyber risks in the property marine and energy markets.

ANNEX 1 Target systems, equipment and technologies

his annex provides a summary of potentially vulnerable systems and data onboard ships to assist companies with assessing their cyber risk exposure. Vulnerable systems e uipment and technologies may include eg

ommunication systems

- integrated communication systems
- satellite communication e uipment
- Voice ver nternet Protocols V P e uipment
- wireless networks Ns
- public address and general alarm systems
- systems used for reporting mandatory information to public authorities.

Bridge systems

- integrated navigation system
- positioning systems P etc
- lectronic hart Display nformation ystem D
- Dynamic Positioning DP systems
- systems that interface with electronic navigation systems and propulsion manoeuvring systems
- utomatic dentification ystem
- lobal aritime Distress and afety ystem D
- radar e uipment
- Voyage Data Recorders VDRs
- ridge Navigational atch larm ystem N
- hipboard ecurity larm ystems .

Propulsion, machinery management and power control systems

- engine governor
- power management
- integrated control system
- alarm system
- bilge water control system
- water treatment system
- emissions monitoring
- heating ventilation and air conditioning monitoring
- damage control systems
- other monitoring and data collection systems eg fire alarms.

Access control systems

- surveillance systems such as V network
- electronic personnel on board systems.

Cargo management systems

- argo ontrol Room R and its e uipment
- onboard loading computers and computers used for exchange of loading information and load plan updates with the marine terminal and stevedoring company
- remote cargo and container tracking and sensing systems
- level indication system
- valve remote control system
- ballast water systems
- reefer monitoring systems
- water ingress alarm system.

Passenger or visitor servicing and management systems

- Property anagement ystem P
- shipmanagement systems o en including electronic health records
- financial related systems
- ship passenger visitor seafarer boarding access systems
- infrastructure support systems like domain naming system DN and user authentication authorisation systems.
- incident management systems.

assen er-facin networks

- passenger i i or ocal rea Network N internet access for example where onboard personnel can connect their own devices[22]
- guest entertainment systems.

ore infrastructure systems

- security gateways
- routers
- switches
- firewalls
- Virtual Private Network s VPN
- Virtual N s V N
- intrusion prevention systems
- security event logging systems.

dministrative and crew welfare systems

- administrative systems
- crew i i or N internet access for example where onboard personnel can connect their own devices.

---

his is not considered as ring our wn Device D . Devices are not used to access protected information. hey can only be used for an individual s personal non company use.

ANNEX 2 Cyber risk management and the safety management system

Resolution . makes clear that an approved should take into account cyber risk management when meeting the ob ectives and functional re uirements of the ode. he guidance provided in the uidelines on maritime cyber risk management . irc. provides high level recommendations regarding the elements of an appropriate approach to implementing cyber risk management. he 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 .

IDE TIF [23]

oles and responsibilities[24]	
ction	**Remarks**
ode . his publication . Update the safety and environment protection policy to include reference to the risk posed by unmitigated cyber risks.	n 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 R has both safety and security aspects but the emphasis is on managing the safety risks introduced by and networks ■ an understanding that without appropriate technical and procedural risk protection and control measures is vulnerable to disruption affecting the safe operation of a ship and protection of the environment. Nothing in the updated policy should suggest that R is given any more or less a ention than any other risks identified by the company.
ode . his publication . Update the responsibility and authority information provided in the to include appropriate allocation of responsibility and authority for cyber risk management (CRM).	n general 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. perational and technical personnel should generally understand the safety and environmental impacts of disruption to critical systems[25] onboard ships and are responsible for the . llocation of responsibility and authority may need to be updated to enable R . his should include ■ allocation of responsibilities and authorities which encourage cooperation between 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 aster.
ode . his publication . Using existing company procedures identify any training which may be re uired to support the incorporation of cyber risk management into the SMS.	yber awareness training is not a mandatory re uirement. Notwithstanding this training is a protection and control measure that forms the basis of R . t helps to ensure that personnel understand how their actions will in uence the effectiveness of the company s approach to R . xisting company procedures for identifying training re uirements 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 R policies and procedures ■ company personnel who have been assigned R duties to receive a type and level of cyber training appropriate to their responsibility and authority.

dentify Protect Detect Respond and Recover as described in the uidelines on aritime yber Risk anagement . irc. .

unctional element from the uidelines on aritime yber Risk anagement . irc. .

or the purpose of this annex critical systems means the so ware and data the sudden operational failure or unavailability of which is identified by the ompany as having the potential to result in ha ardous situations.

PROTECT

Implement risk control measures	
ction	**Remarks**
ode . . . his publication and nnex ssess all identified risks to ships personnel and the environment and establish appropriate safeguards.	he 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. s a baseline the following measures should be considered before a risk assessment is undertaken. he baseline consists of the technical and procedural measures which should be implemented in all companies to the extent appropriate. hese measures are ■ **Hardware inventory.** Develop and maintain a register of all critical system hardware on board including authori ed and unauthori ed devices on company controlled networks. he should include procedures for maintaining this inventory throughout the operational life of the ship. ■ **o ware inventory** Develop and maintain a register of all authori ed and unauthori ed so ware running on company controlled hardware onboard including version and update status. he should be updated to include procedures for • maintaining this inventory when hardware controlled by the company is replaced • maintaining this inventory when so ware controlled by the company is updated or changed • authori ing the installation of new or upgraded so ware on hardware controlled by the company • prevention of installation of unauthori ed so ware and deletion of such so ware if identified • so ware maintenance. ■ **ap data ows** ap data ows between critical systems and other e uipment 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. he should be updated to include procedures for • maintaining the map of data ows to re ect changes in hardware so ware and or connectivity • identifying and responding to vulnerabilities introduced when new data ows are created following the installation of new hardware • reviewing the need for connectivity between critical systems and other and systems. uch a review should be based on the principle that systems should only be connected where there is a need for the safe and e cient 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 ows. his may be achieved by restrictions on the use of removable media and disabling U and similar ports on critical systems. ■ **Implement secure confi urations for all hardware controlled by the company** This should include documenting and maintaining commonly accepted security configuration standards for all authori ed hardware and so ware. he should include policies on the allocation and use of administrative privileges by ship and shore based personnel and third parties. owever it is not recommended that the details of secure configurations are included in the . his information should be retained separately and securely by the company. ■ **Audit logs.** ecurity logs should be maintained and periodically reviewed. ecurity logging should be enabled on all critical systems with this capability. he 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.** aintain situational awareness of current cyber threats. ee line 3 above. ■ **Physical security.** he physical security of the ship is enhanced by compliance with the security measures addressed in the ship security plan P re uired by the P ode. easures should be taken to restrict access and prevent unauthori ed access to critical system network infrastructure onboard.

Develop contin ency plans	
ction	**Remarks**
ode his publication . and 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.	n approved should already address procedures plans and instructions for key shipboard operations concerning the safety of the personnel ship and protection of the environment. n general these plans should be unaffected by the incorporation of R into the . his is because the effect of the loss of availability of or loss of integrity of the data used or provided by such systems is the same as if the 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. his 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 to operators should be considered for inclusion in operational maintenance routines.
ode . his publication Update emergency plans to include responses to cyber incidents.	n approved should already address emergency plans for the disruption of critical systems re uired for the safe operation of ships and protection of the environment. n general these plans should be unaffected by the incorporation of cyber risk management into . his is because the effect of common shipboard emergencies should be independent of the root cause. or example a fire may be caused by e uipment malfunctioning because of a so ware failure or inappropriate maintenance or operation of the e uipment. 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 or the data used by them. he purpose of the module could be to provide information on the actions to be taken in the event of a simultaneous disruption to multiple systems re uired for the safe operation of the ship and protection of the environment. n 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	
ction	**Remarks**
ode . his publication . Update procedures for reporting non conformities accidents and ha ardous situations to include reports relating to cyber incidents.	n approved should already address procedures relating to non conformities. hen incorporating R into the company reporting re uirements for non conformities may need to be updated to include cyber related non conformities. onsider sharing the facts of a cyber related non conformity with information sharing organisations. xamples of such non conformities and cyber incidents ■ unauthorised access to network infrastructure ■ unauthori ed or inappropriate use of administrator privileges ■ suspicious network activity ■ unauthorised access to critical systems ■ unauthorised use of removable media ■ unauthorised connection of personal device ■ failure to comply with so ware 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 re uired by critical systems.

RESPOND

Develop and implement activities and plans to provide resilience and to restore systems necessary for shippin operations and or services impaired due to a cyber-event	
ction	**Remarks**
ode . his publication . nsure that ade uate resources and shore based support are available to support the DP in responding to the loss of critical systems.	n approved should already be supported by ade uate resources to support the DP . owever the incorporation of R into the should re uire that this resourcing includes appropriate expertise. his resource could come from within the company but may also be provided by a third party. n providing the ade uate resources the following should be considered ■ company or third party technical support should be familiar with onboard and infrastructure and systems ■ any internal response team or external cyber emergency response team R should be available to provide timely support to the DP . ■ provision of an alternative means of communication between the ship and the DP which should be able to function independently of all other shipboard systems if and when the need arises ■ internal audits should confirm that ade uate resources including third parties when appropriate are available to provide support in a timely manner to support the DP .
ode . his publication Update procedures for implementing corrective actions to include cyber incidents and measures to prevent recurrence.	n approved should already include procedures for responding to non conformities. n general these should not be affected by the incorporation of R in . owever the procedures should help ensure that consideration of non conformities and corrective actions involves the personnel with responsibility and authority for R . his should help ensure that corrective actions including measures to prevent recurrence are appropriate and effective.
ode . his publication . Update the specific measures aimed at promoting the reliability of .	n approved should already include procedures for operational maintenance routines to promote the reliability of e uipment on board. which incorporates R should outline procedures for ■ so ware maintenance as a part of operational maintenance routines. uch procedures should ensure that application of so ware updates including security patches are applied and tested in a timely manner by a competent person ■ authori ing remote access if necessary and appropriate to critical systems for so ware or other maintenance tasks. his should include authori ing 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 so ware 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 so ware maintenance tasks to competent personnel.

RECOVERY

Identify measures to back-up and restore cyber systems necessary for shippin operations impacted by a cyber incident	
ction	**Remarks**
ode . his publication . nclude creation and maintenance of back ups into the ship s operational maintenance routine.	n approved should already include procedures for maintaining and testing back up arrangements for shipboard e uipment. Notwithstanding this it may not address procedures for maintaining and storing o ine back ups for data and systems re uired for the safe operation of the ship and protection of the environment. which incorporates R 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 to enable recovery from a cyber incident ■ maintaining back ups of data re uired for critical systems to operate safely ■ o ine storage of back ups and clean images if appropriate ■ periodic testing of back ups and back up procedures.

ANNEX 3 Onboard networks

secure network depends on the set up onboard the ship and the effectiveness of the company policy based on the outcome of the risk assessment. ontrol 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. t is recommended that network layout and network control should be planned for all newbuilds[26].

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

- implement network separation and or tra c management
- manage encryption protocols to ensure correct level of privacy and commercial communication
- manage use of certificates to verify origin of digitally signed documents so ware or services.

n general only e uipment or systems that need to communicate with each other over the network should be able to do so. he overriding principle should be that the networking of e uipment or systems is determined by operational need.

Physical layout

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

Network management

ny network design will need to include an infrastructure for administering and managing the network. his may include installing network management so ware on dedicated workstations and servers providing file sharing email and other services to the network.

etwork se mentation

nboard networks should normally accommodate the following basic functions it is not uncommon that networks are even further separated

- necessary communication between e uipment and configuration and monitoring of e uipment
- onboard administrative tasks including email and sharing files or folders related to eg ship administration cargo operations technical management etc networks
- recreational internet access for crew and or passengers visitors.

ffective network segmentation is a key aspect of defence in depth . and public networks should be separated or segmented by appropriate protection measures. here relevant further segmentation between navigation systems engineering systems and cargo management systems can be considered. he 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

---

ee Recommendation on yber Resilience No. .

- network switches between each network segment
- internal firewalls between each network segment
- Virtual ocal rea Networks V N to host separate segments.

n addition each segment should have its own range of nternet Protocol P addresses. Network segmentation does not remove the need for systems within each segment to be configured with appropriate network access controls and so ware firewalls and malware detection.

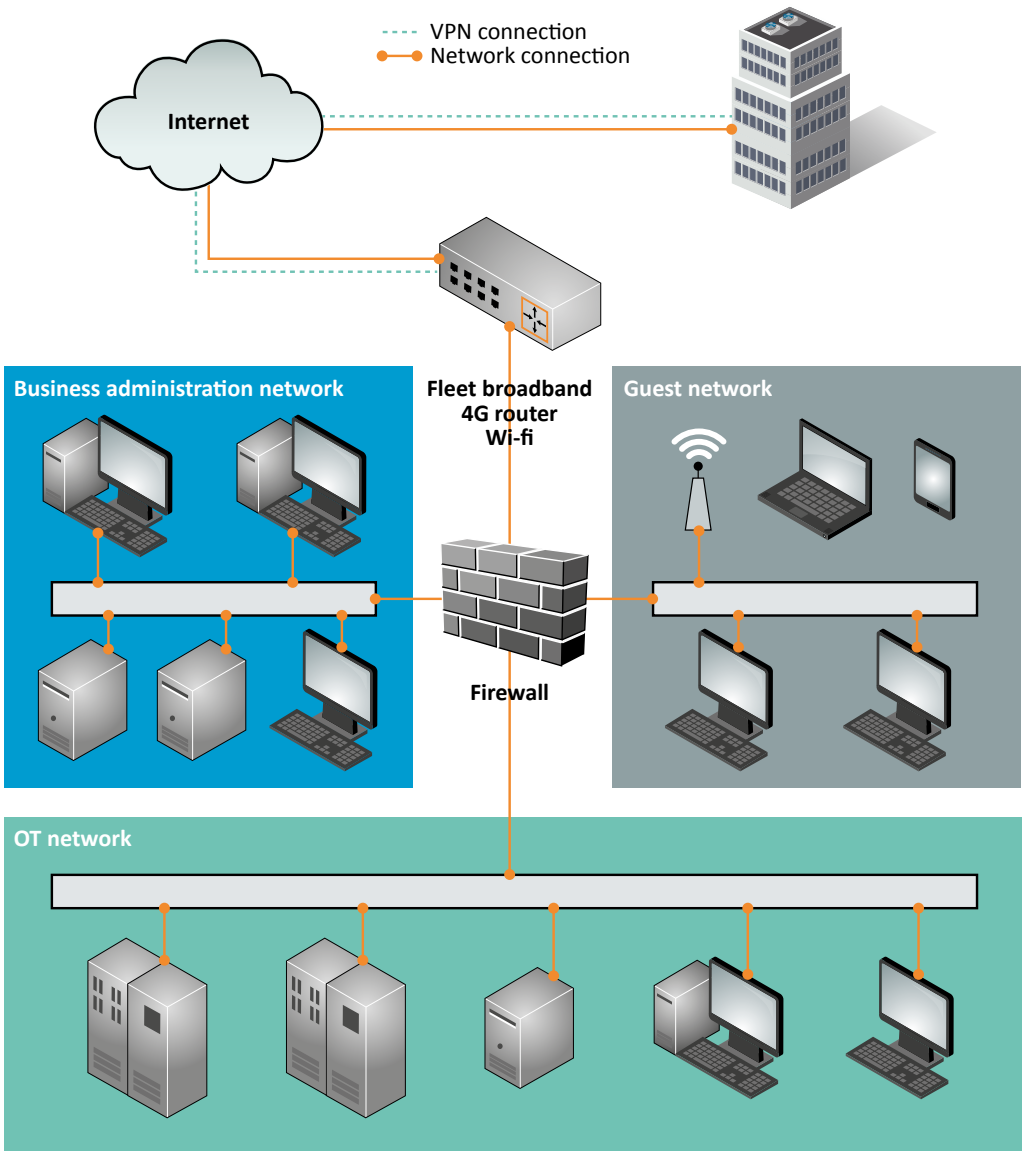

Figure 12: Example of an onboard network.

n the example shown above the network has been segmented using a perimeter firewall which supports three V Ns

1. the Network containing e uipment and systems that performs safety critical functions
2. the network containing e uipment and systems that performs administrative or business functions
3. a crew and guest network providing uncontrolled internet access.

onsiderations should be made on how to maximise the security of the switches themselves. o achieve the highest level of security each network should use a different hardware switch. his will minimise the chance of an a acker umping between networks due to misconfiguration or by ac uiring access to the configuration of a switch.

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

or 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. nabling 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. he 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.

onitorin data activity

t is important when monitoring and managing systems to be aware of the networks status and to detect any unauthorised data tra c. ogging should be implemented in the firewall and ideally in all network a ached devices so that in case of a breach the responsible person can trace back the source and methodology of the incident. his will help to secure the network from any similar incidents in the future.

network ntrusion Detection ystem D or ntrusion Protection ystem P can alert the system administrator in real time of any incidents to the network systems. he D and P inspect data tra c entry points or both to identify known threats or to re ect tra c which does not comply with the security policy. n P should comply with the latest industry best practices and guidelines.

t is recommended to place a sensor on the internet facing segment because the public servers are a visible target to a ackers. nother sensor should be placed behind the firewall to monitor tra c between the internet and the internal network. n lD P sensor could also be placed by a remote access segment for instance a Virtual Private Network VPN .

rotection 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. very network onboard has several endpoints such as workstations servers routers input and output modules transducers etc. he endpoints are very important as they control the operation and the security of the system.

single security product technology or solution cannot ade uately protect a system by itself. 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 minimi ed see section . defence in depth . n addition an effective defence in depth strategy re uires a thorough understanding of possible a ack vectors on a system. hese may include

- back doors and holes in network perimeter and instruments
- vulnerabilities in commonly used protocols
- vulnerable endpoints and sensors
- unprotected databases.

secure running environment can be established by using a testing environment isolated from networks and computers which provides additional protection against cyber threats by isolating executable so ware from the underlying operating system. his prevents unauthorised access to the operating systems on which the so ware is running. he sandbox enables so ware to be run under a specific set of rules and this adds control over processes and computer resources. herefore the sandbox helps prevent malicious malfunctioning or untrusted so ware 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. back door is sometimes created in hidden parts of the system itself or established by separate so ware.

Brin your own device B OD 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.

hain of custody is the chronological documentation or paper trail that records the se uence of custody control transfer analysis and disposition of physical or electronic evidence.

yber a ack is any type of offensive manoeuvre that targets and systems computer networks and or personal computer devices and a empts to compromise destroy or access company and ship systems and data.

Cyber incident is an occurrence which actually or potentially results in adverse conse uences to an onboard system network and computer or to the information that they process store or transmit and which may re uire a response action to mitigate the conse uences.

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 e uipment 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 and systems networks and e uipment at every stage of the system network or sub component life cycle. nboard 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 and on board.

Di itisation is the conversion of analogue information to digital information.

Di italisation is how the digital world impacts people and work.

E ecutable so ware 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 infrastructure and information.

Firmware is so ware imbedded in electronic devices that provides control monitoring and data manipulation of engineered products and systems. hese are normally self contained and not

accessible to user manipulation.

Flaw is unintended functionality in so ware.

Industrial Internet of Thin s IIoT refers to the application of instrumentation and connected sensors and other devices to machinery and vehicles in the transport energy and industrial sectors.

Information Technolo y IT covers the spectrum of technologies for data storing and processing including so ware hardware and communication technologies.

Intrusion Detection ystem ID is a device or so ware application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

Intrusion revention ystem I also known as ntrusion Detection and Prevention ystems DP s are network security appliances that monitor network and or system activities for malicious activity.

ocal rea etwork is a computer network that interconnects computers within a limited area such as a home ship or o ce building using network media.

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

anufacturer is the entity that manufactures the shipboard e uipment and associated so ware.

Operational technolo y OT includes hardware and so ware that directly monitors controls physical devices and processes typically on board.

Patches are so ware designed to update so ware or supporting data to improve the so ware 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.

rinciple of least privile e refers to the restriction of user account privileges only to those with privileges that are essential to function.

Recovery refers to the activities a er an incident re uired 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. his includes laptops U memory sticks Ds DVDs and diske es.

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.

andbo is an isolated environment in which a programme may be executed without affecting the underlying system computer or operating system and any other applications. sandbox is o en used when executing untrusted so ware.

Service provider is a company or person who provides and performs so ware maintenance.

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

o ware whitelistin means specifying the so ware which is present and active on an or system.

Typos ua n also called UR hi acking or fake UR relies on mistakes such as typos made by nternet users when inpu ng a website address into a web browser. hould a user accidentally enter an incorrect website address they may be led to an alternative and o en malicious website.

irtual ocal rea etwork is the logical grouping of network nodes. virtual N allows geographically dispersed network nodes to communicate as if they were physically on the same network.

irtual rivate etwork 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 so ware that maliciously infects and manipulates the operation of a computer programme or system.

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

ANNEX 5 Contributors to most recent revision of this publication

he following organisations and companies have participated in the development of these guidelines[27]

- **Working Group 2020**
  - BIMCO
  - olumbia hipmanagement yprus hairperson
  - Chamber of Shipping of America
  - Digital ontainership ssociation
  - nterferry
  - INTERMANAGER
  - nternational ssociation of Dry argo hipowners N R R
  - nternational ssociation of ndependent anker wners N R N
  - nternational hamber of hipping
  - nternational arine ontractors ssociation
  - nternational Union of arine nsurance U
  - oran yber
  - aersk
  - il ompanies nternational arine orum
  - uperyacht uilders ssociation ybass
  - orld hipping ouncil

- **eference Group**
  - lass N
  - yberowl
  - ygnus echnologies
  - Cobham SATCOM
  - aritime ransportation ystem nformation haring and nalysis enter
  - emplar xecutives

ollowing additional stakeholders have contributed to past revisions of the guidelines
nglo astern roup ruise ines nternational ssociation yberkeel nternational roup of P lubs impact td.