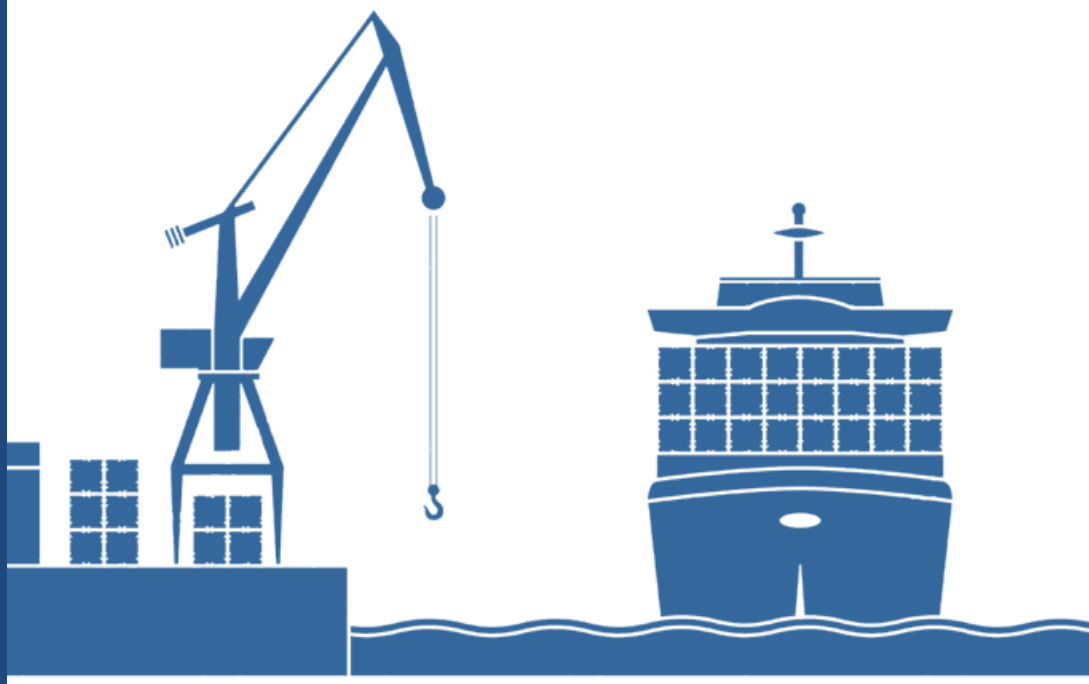
MARITIME CYBER SECURITY



INTERNATIONAL ARMOUR

www.armour.gr

Kroll CONTRACTOR

A GROUP THAT YOU CAN TRUST

CYBER SECURITY IN MARITIME

Every day, all around the world, thousands of IT systems are compromised.

Some are attacked purely for the kudos of doing so, others for political motives, but most commonly they are attacked to steal money or commercial secrets.

Our experience suggests that in practice, few companies have got this right.

And if your company doesn't have it right, your IT systems may have already been compromised, attackers could already have your new Company projects, bidding offers or research plans; they may already be running your process control systems.
Whatever business you are in, you all rely on the internet correspondence.

You communicate with your ships, local agents, Charterers, suppliers, various authorities, Classes, P&I clubs, Ports etc, in other words this is your most medium used for carrying out your business, rely upon it for your logistical support.

In simple words the internet brings immeasurable benefits. But, you cannot escape the fact that it also brings new risks.

About 80% of known attacks would be defeated by embedding basic information security practices for your people, processes and technology where companies adopt these steps it has made a tangible difference to their vulnerability to cyber attack.

WHAT WE DO

Cyber Crime Investigations

We have the global expertise and resources necessary to investigate a range of cybercrime activity, employing a full range of investigative strategies to identify system vulnerabilities, intrusions and data ex-filtrations and to recommend appropriate and cost-effective solutions that can be applied across your shipping company.

Computer Forensics

Our computer forensics experts ensure that no digital evidence is overlooked and assist at any stage of an investigation or litigation, regardless of the number or locations of data sources.

Data Breach Prevention

Draw upon our expertise and experience in data breach prevention for all of your cyber review, assessment and analysis requirements

Cyber Risk Assessments

Our cyber risk assessments deliver effective recommendations to improve security, using industry best practices & the best technology available.

Cyber Policy Review and Design

Ensure that your cyber security policy has the appropriate controls needed to keep your organization's information secure with a reliable plan in place in the event of an incident.

Vulnerability Scanning

We utilize vulnerability scanning software with the most up-to-date data security information that help our experts deliver effective and prioritized recommendations to improve your IT security.

WHAT WE DO

Third Party Cyber Audits and Reviews

Ensure that your third parties are handling sensitive data according to regulatory guidelines and industry standards with our cyber audits and reviews

Incident Response Management

For peace of mind after a data breach, rely on our rapid response team of cyber experts for compliant notifications; reputation-saving remediation; and litigation support.

Data Collection and Preservation

Improve investigations and reduce your potential for damages and fines with the strict chain-of-custody protocol our experts follow at every stage of the data collection process.

Data Recovery and Forensic Analysis

Our expertise establishes whether data was compromised and to what extent. We uncover actionable information, leaving you better prepared to manage a future incident

Malware & Advanced Persistent Threat Detection

Our expertise allows us to identify and analyze the scope and intent of advanced persistent threats to launch a targeted and effective response.

Data Breach Response

Our data breach services, is ranging from notification to call center, in order to identity monitoring, help you protect your business and reestablish trust with the persons/companies impacted by a breach, by matching the response to the harm caused by your breach.

WHAT WE DO

Data Breach Notification

Group's data breach notification solutions — from drafting compliant letters, to full-service mailing help, to alternate notifications for large breaches — we take the burden off your organization.

Credit Monitoring

Credit monitoring can be a powerful tool to offer in the wake of a data breach. We provide a monitoring alert system that's backed by the expertise of our licensed investigator team

Identity Monitoring

Our unique combination of identity monitoring services can detect more types of identity theft than credit monitoring alone, providing practical help to combat identity theft and fraud.

Identity Theft Restoration

We provide your breach employees with direct access to investigative experts for live support and best practice advice, as well as identity restoration should they become victims of identity theft

Cyber Litigation Support

Whether responding to an investigatory matter, forensic discovery demand, or information security incident, our forensic engineers have extensive experience providing litigation support to help clients win cases and mitigate losses.

WHAT WE DO

Cyber Due Diligence

The value of a deal can drop precipitously if, after the deal is finalized, disclosure of past or ongoing data breaches appear.

Cyber risks are real and costly, and wise investors assess the stability and safety of their enterprise before committing to a significant investment.

Cyber due diligence conducted prior to investments and during M&A deal-making, may help investors identify a target's cyber security vulnerabilities.

Likewise, a seller can strengthen its attractiveness and potentially close the deal faster by conducting "self" due diligence to demonstrate the cyber security health of its enterprise.

ID-Shield

ID-Shield is the only identity theft protection company armed with a team of licensed private investigators on call to restore your identity

CYBER SECURITY IN MARITIME

We are in Cyber Security Section

Specialists from law enforcement and other government and intelligence agencies, law firms, international auditing companies and management consulting companies.

Our industry-leading experts have written books and articles, taught difficult and highly technical courses, and testified in courts of law and other proceedings as expert witnesses.

Combine proven investigative methods and advanced technical expertise with deep insight into the integral role that humans play in every cyber event.

How we help

- Identifying and addressing weaknesses in technology systems and policies
- Responding to technical threats, including the human aspects of such
- Preparing for and succeeding in litigation
- Complying with relevant data protection and other regulatory requirements
- Safeguarding privacy and intellectual property
- Remediating intrusions and breaches
- Notifying, as necessary, affected entities and individuals

The diversity of our professionals enables us to bring to our cases complementary and sophisticated fact-finding skill sets and analytical methodologies.

Working seamlessly as part of a multidisciplinary team, we draw upon this knowledge to offer clients uncommon insight and superior outcomes.

CYBER SECURITY IN MARITIME

Shipping companies are becoming increasingly aware of the growing threat to shipping caused by the surge of cyber threats and are keen to comply with IMO and other maritime regulators guidance in meeting best practice in cyber protection for their fleet and the expected updating of the US “Strengthening Cyber Security Information Sharing and Coordination in Our Ports Act” (2015) which could see mandatory reporting for all vessels entering US waters.

Combine proven investigative methods and advanced technical expertise with deep insight into the integral role that humans play in every cyber event.

The interim IMO guidance issued in June 2016 draws heavily on the Identify, Protect, Detect, Respond & Recover model introduced by the US National Institute of Standard and Technology Preliminary Cyber security Framework - Improving Critical Infrastructure Cyber security Executive Order 13636

Kroll® CONTRACTORS

Following the production of the prioritised action plan, there will be a (as yet unknown) series of activities to be undertaken in order to achieve compliance with the IMO guidance.

We will be able to assist with many of these tasks from drafting policies and/or procedures to be implemented, advising on changes to systems architecture or infrastructure, testing and reviewing systems (penetration testing) and producing an audit timetable to allow the Company to demonstrate ongoing compliance.

These activities – the Delivery Phase, will be discussed with the Company once the Action Plan has been delivered

CYBER SECURITY IN MARITIME

Worried about a sophisticated internal fraud?

Considering entering a new market?

How safe is your company data?

Are you protecting your company's reputation in the market?

Are you making a sound investment decision?

The facts don't add up: what to do?

We can help provide answers to your questions!

Kroll® CONTRACTORS

Industry Depth Chart

SERVICES	WE	CYBER SECURITY FIRMS	PROFESSIONAL SERVICES FIRMS	HARDWARE MANUF/RERS	NETWORK PROVIDERS	DIY-IN-HOUSE
Cost Effective APT						
Detection of Unknown Binaries						
Rapid Deployment						
International Presence						
Information Risk Assessments						
Intrusion Experience						
Investigative and Forensic Experience						
Breach Notifications						
Insider Investigations and Due Diligence						
E-discovery Collection						
E-discovery Processing						
Data Recovery and Clean Rooms						

+35 Languages

+20 Countries

+1k Employees

Kroll® CONTRACTORS

SERVICES

All agencies that have established credit cards for transactions require compliance with the Payment Card Industry Data Security Standard (PCI DSS)

DATA PROTECTION & PRIVACY

Protect critical data and help enterprises understand the use of critical content, all while meeting constantly increasing privacy requirements.

EU GDPR COMPLIANT

We have developed a methodology for assessing organizations of all sizes.

SECURITY ADVISORY SERVICES

Assess your business risks, define and implement strategies to optimize security readiness.

INTERNAL VULNERABILITY ASSESSMENT

Outsource your vulnerability scan and trust the experts to secure your business

SECURITY RISK MANAGEMENT

Adopting our risk based approach allows companies to prioritize activities based on the likelihood and consequence of a vulnerability being exposed

CLOUD SECURITY

We secure your virtual environments for cloud and IaaS while offering you full visibility across platforms

CYDOME

Protecting Global Shipping at Sea

Cyber Risk Today

At any given time, vessels are exposed to more and more cyber threats that may have severe repercussions: In 2019 alone, cybercrime was estimated to cost around $600 billion globally.

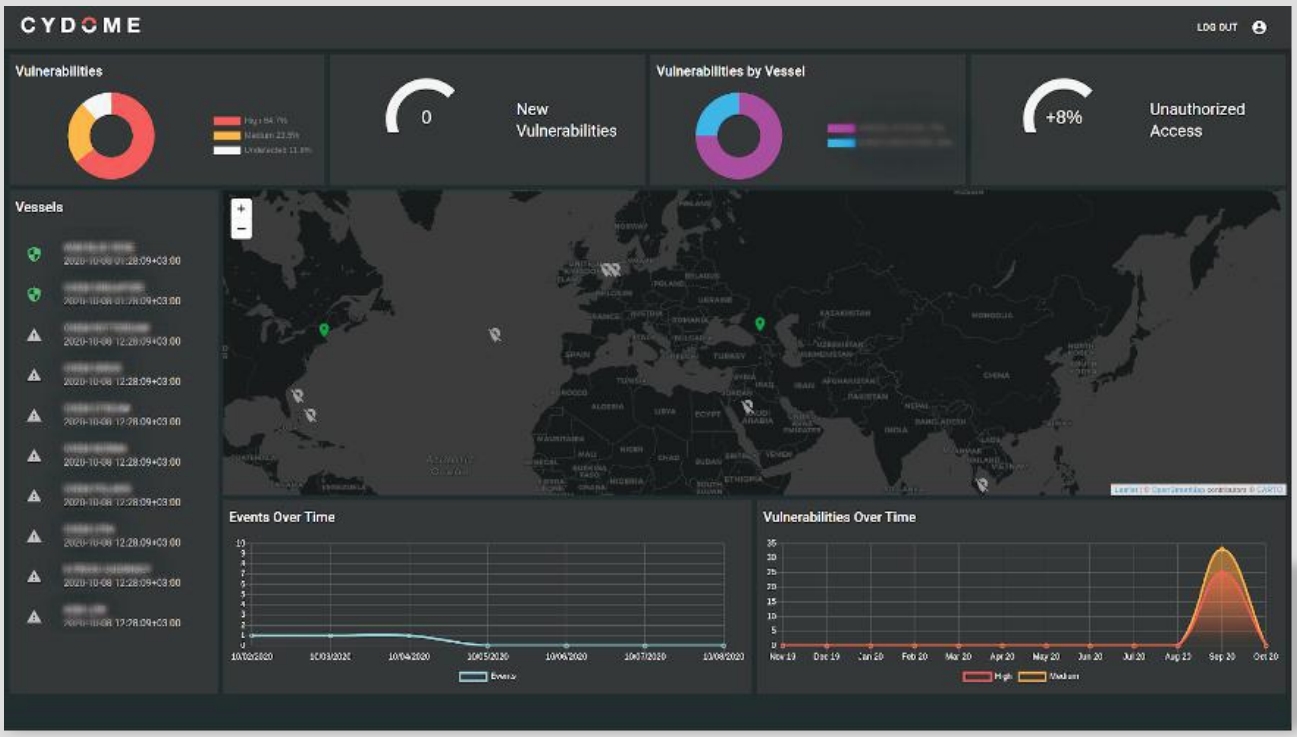
The Rapid and constant increase in band- width and modern computing systems together with the increasing amount and complexity of IT and OT systems on board - resulting in a steady increase in cyber attacks.

Cydome Onboard Suite

“Cydome Onboard Suite” provides a multilayer cybersecurity solution uniquely designed to protect the maritime industry against cyber-attacks.

Cydome offers innovative and advanced security methods and services to match the specific challenges onboard vessels, based on years of experi- ence in both cyber security and the maritime industry.

It secures a vessel’s business and crew networks by providing oversight, security threat alerting, and control of the vessel’s entire IT and OT infrastructures.



Features

End to End Protection

- IT and OT Asset protecting and monitoring.
- Real time IT network Intrusion detection and prevention.
- Vulnerability Scanning
- Critical system isolation

Visibility

- Full visibility and control over all connected devices, real-time connection detection, cyber security status, etc.
- Comprehensive monitoring dashboard

Regulation Compliance

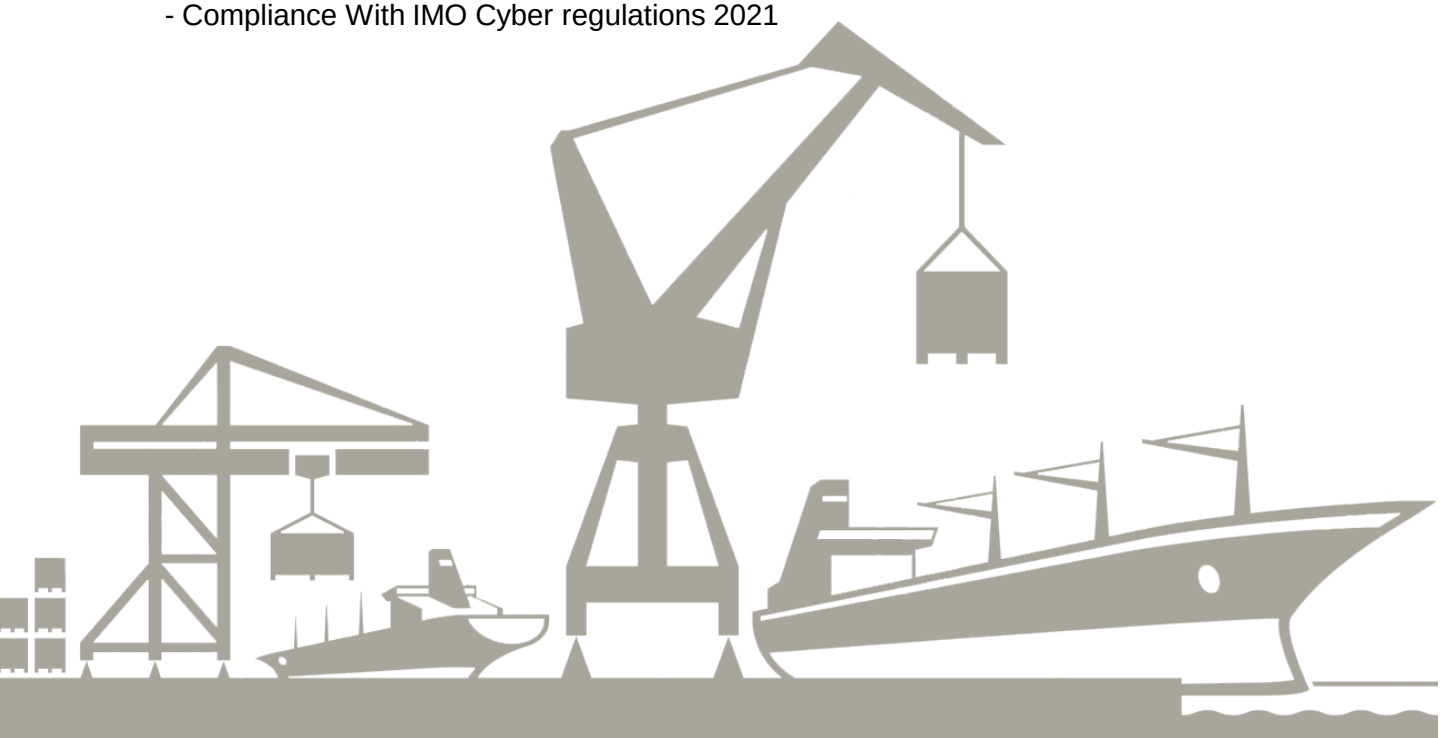
- Preparation and Assistance to **IMO 2021** compliancy
- Real time Cyber risk analysis reports

Unique Advantage

- Integrates with existing systems and software.
- No further installation needed on your systems.
- Requires no human intervention.
- Does not require constant communication connection

Your Benefits

- Seamlessly protects every critical device (IT & OT) on board your ship!
- Reduces the risks of cyber attacks and security breaches
- Compliance With IMO Cyber regulations 2021



THINKS YOU NEEED TO KNOW!

EXECUTIVE SUMMARY

Advancement in broadband technologies and the move towards ‘Big Data’ and 'Ship Intelligence could leave the maritime industry vulnerable to cyber-crime unless it develops a better awareness of ICT (information, communication technology) security and adopts best security practice.

Certainly there is the possibility for AIS, GNSS, ENC and ECDIS charts to disappear from bridge screens or be modified which can create a safety havoc, but the big issue today is that most adversaries want to obtain data for financial gain.

Payment systems can be easily penetrated using targeted phishing scams to raise fake invoices or even to change shipping manifests in order to transport illicit goods, drugs and weapons.

The loss of sensitive data through breaches in the system security is the single most important challenge that faces the maritime industry today.

Cyber attacks in oil and gas industry has an extreme increment year by year

Awareness on cyber security in maritime sector is growing!

In maritime industry attacks often remain in secret

Critical infrastructure & Cyber Security (HORIZON 2020)

Maritime Security & Awareness

Cyber security in the maritime industry is a major concern, due to a lack of security awareness or accountability while increasing use of new, sophisticated communications technologies raises the threat level to high.

With the potential for sensitive customer data leaks via ECDIS, AIS, RFID and GPS, it is important that security procedures and processes are in place so that operators know how to identify a potential security threat or have been trained to respond when a cyber attack is in process.

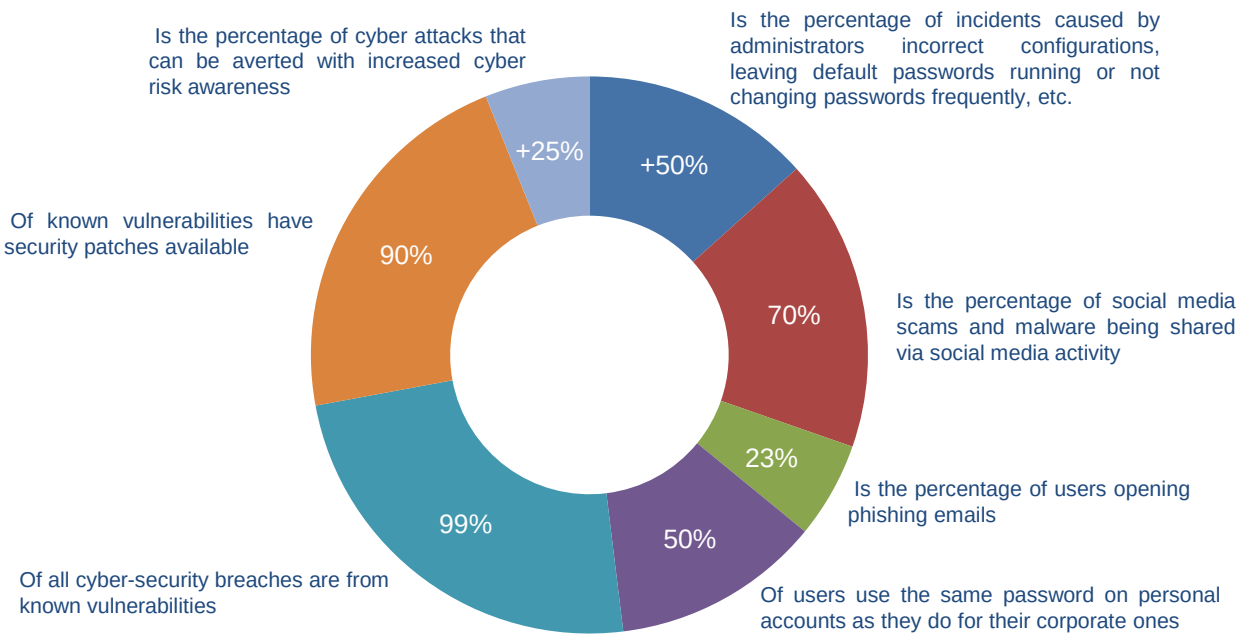
The perpetrators active in the maritime industry are mostly interested in financial gain, looking to gain access, stay hidden and extract financial profit from their targets.

However, accessing and extracting sensitive information or intellectual property can also help criminal or terrorist organizations whose motive is to use the industry to transport hazardous materials or weapons or use the ship itself as a weapon at a sensitive area or close to a port.

In an advanced threat, the attacker will spend a large amount of time researching a list of potential targets, gathering information about the organization's structure, clients etc. Social media activity of the people in the target company will be monitored to extract information about the systems and forums favored by the user and any technology vulnerabilities assessed.

Once a weakness is found the next step the hacker will take is to breach the cyber security perimeter - the basic security most companies adopt - and gain access, which, for most attackers, is easily done.

Perimeters Breached



Introduction

As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are increasingly being networked together – and more frequently connected to the worldwide web.

This brings the greater risk of unauthorized access or malicious attacks to ships' systems and networks. Risks may also occur from personnel having access to the systems onboard, for example by introducing malware via removable/USB media.

Relevant personnel should have training in identifying the typical modus operandi of cyber-attacks.

The safety, environmental and commercial consequences of not being prepared for a cyber-incident may be significant. Responding to the increased cyber threat, a group of international shipping organizations, with support from a wide range of stakeholders, have developed these guidelines, which are designed to assist companies develop resilient approaches to cyber security onboard ships.

Approaches to cyber security will be company- and ship-specific, but should be guided by appropriate standards and the requirements of relevant national regulations.

The Guidelines provide a risk-based approach to identifying and responding to cyber threats.

Aim and scope

Our aim and scope is to offer information to ship-owners and operators on how we can assess their operations and put in place the necessary procedures and actions to maintain the security of cyber systems onboard their ships.

Company plans and procedures for cyber risk management should be seen as complementary to existing security and safety risk management requirements contained in the International Safety Management Code (ISM) Code and the International Ship and Port Facility Security (ISPS) Code.

Cyber security should be considered at all levels of the company, from senior management ashore to crew on board, as an inherent part of the safety and security culture necessary for safe and efficient ship operations.

The Guidelines are designed to develop understanding and awareness of key aspects of cyber security.

The Guidelines are not intended to provide a basis for auditing or vetting the individual approach to cyber security taken by companies and ships.

Existing international standards and guidelines cover cyber security issues for shore side operations – whereas these Guidelines focus on the unique issues facing the shipping industry onboard ships.

The measures to lower cyber security risks include:

- How to raise awareness of the safety, security and commercial risks for shipping companies if no cyber security measures are in place;

- How to protect shipboard OT and IT infrastructure and connected equipment;

- How to manage users, ensuring appropriate access to necessary information;

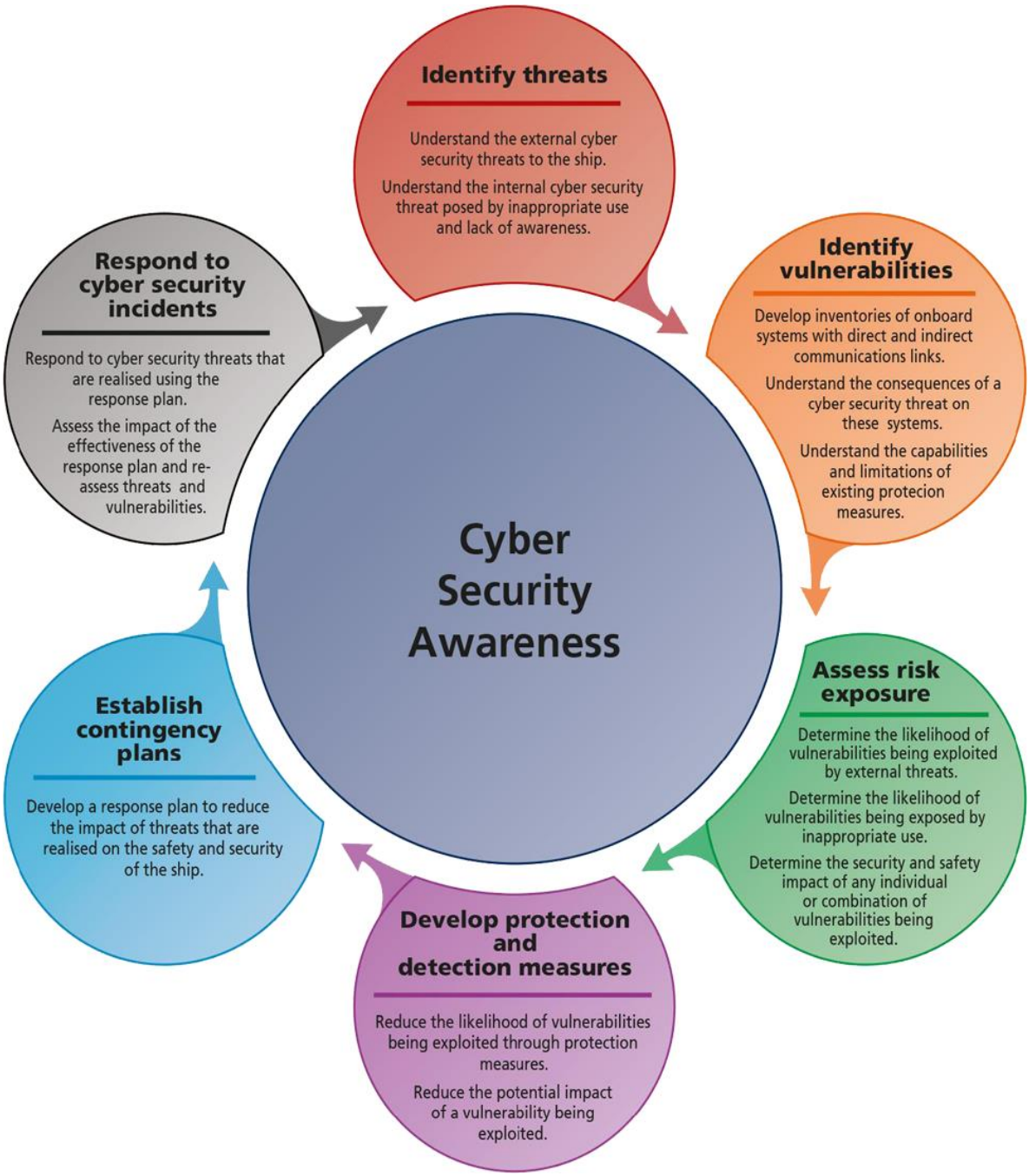
- How to protect data used onboard ships, according to its level of sensitivity;

- How to authorize administrator privileges for users, including during maintenance and support on board or via remote link; and

- How to protect data being communicated between the ship and the shore side.

MOST VURNERABLE SHIPBORNE SYSTEMS

ESDIS
VDR
IBS
POSITIONING SYSTEM
BNWAS
GMDSS
CARGO CONTROL SYSTEM
ENGINE CONTROL AND MONITORING SYSTEM
OTHER!



Cyber security awareness as set out in the Guidelines In the event of a cyber-incident, a response plan is needed to quickly recover systems and data and to maintain the safety and commercial operability of the ship.

Some mitigating measures are already covered by the ship's safety management system for complete systems failure, but more sophisticated cyber incidents may only cause partial malfunction of a system, making it harder to detect

NATURE OF THE ATTACKS

Malware
Phising
Spear Phising
Application Attack
Brute Force
Denial of service
Network of protocol attack
Man in the middle
Theft of credentials
Known vulnerability
Other…

EXTENT OF THE ATTACKS

Financial Loss

Loss of Corporate Data

IT System Functionality

Shipborne Systems Functionality

1. Understanding the cyber threat

The cyber risk is specific to the company, ship, operation and/or trade.

When assessing the risk, companies should be aware of any specific aspect of their operations that might increase their vulnerability to cyber incidents.

Unlike other areas of safety and security where historic evidence is available and reporting of incidents is required, cyber security is made more challenging by the absence of any definitive information about the incidents and their impact.

There are motives for organizations and individuals to exploit cyber vulnerabilities.

The following examples give some indication of the threat posed and the potential consequences for companies and the ships they operate:

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

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

Water holing: Establishing a fake website or compromising a genuine website in order to exploit visitors.

Ransom ware: Malware which encrypts data on systems until such time as the distributor decrypts the information.

Scanning: Attacking large portions of the internet at random.

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

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

Spear-phishing: Similar to phishing but the individuals are targeted with personal emails, often containing malicious software or links that automatically download malicious software.

Deploying botnets: Botnets are used to deliver Distributed Denial of Service (DDoS) attacks.

Subverting the supply chain: Attacking a company or ship by compromising equipment or software being delivered to the company or ship.

Stages of a cyber-attack

Cyber-attacks are conducted in stages.

The length of time taken to prepare a cyber-attack will be determined by the motivations and objectives of the attacker, and the resilience of technical and procedural cyber security controls implemented by the company, including those onboard its ships.

The four stages of an attack are:

Survey/Reconnaissance: Open/public sources used to gain information about a company, ship or seafarer which can be used to prepare for a cyber-attack.

Social media, technical forums and hidden properties in websites, documents and publications may be used to identify technical, procedural and physical vulnerabilities. The use of open/public sources may be complemented by monitoring the actual data flowing into and from a company or a ship.

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

- Company online services, including cargo or consignment tracking systems;

- Sending emails containing malicious files or links to malicious websites to seafarers;

- Providing infected removable media, for example as part of a software update to an onboard system; and

- Creating false or misleading websites which encourage the disclosure of user account information by seafarers.

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

- Make changes that affect the system's operation, for example interrupting the display of chart information on ECDIS;

- Gain access to commercially sensitive data such as cargo manifests and/or crew and passenger lists; and/or

- Achieve full control of a system, for example a machinery management system

Stages of a cyber-attack

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

- *Access commercially sensitive or confidential data about cargo, crew and passengers to which they would otherwise not have access;*

- *Manipulate crew or passenger lists, or cargo manifests. This may be used to allow the fraudulent transport of illegal cargo; and*

- *Disrupt normal operation of the company and ship systems, for example by deleting critical pre-arrival information or overloading company systems.*

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

2. Assessing the risk

Cyber security should start at the senior management level of a company, instead of being immediately delegated to the Ship Security Officer or the head of the IT department.

There are several reasons for this:

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

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

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

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

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

The level of cyber risk will reflect the circumstances of the company, ship (its operation and trade), the IT and OT systems used, and the information and/or data stored.

The maritime industry possesses a range of characteristics which affect its vulnerability to cyber incidents:

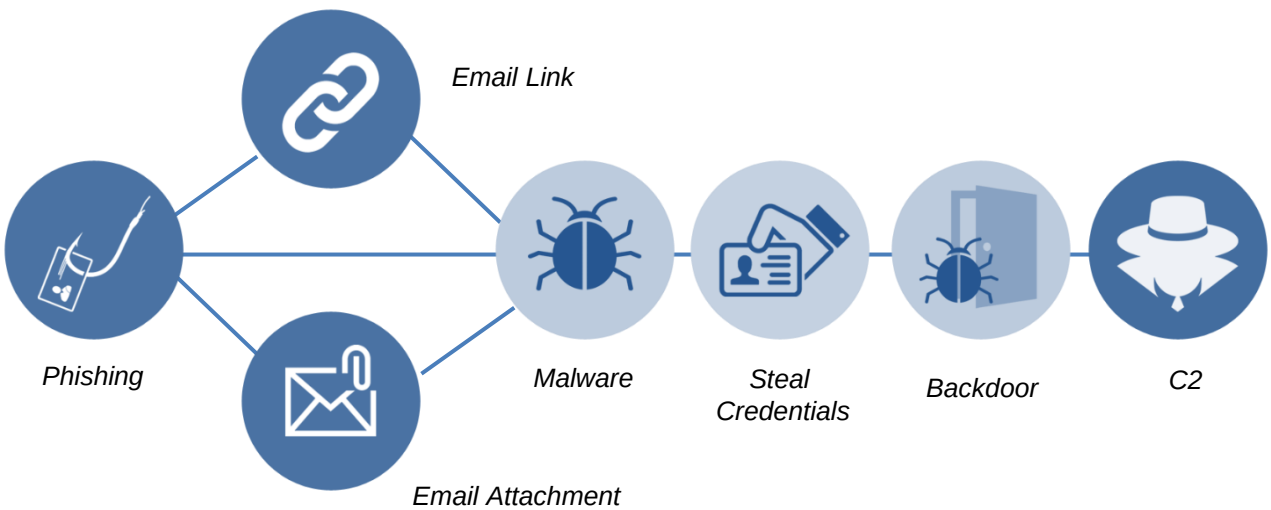
- The cyber controls already implemented by the company and onboard its ships.
- Multiple stakeholders are often involved in the operation and chartering of a ship potentially resulting in lack of accountability for the IT infrastructure.
- The ship being online and how it interfaces with other parts of the global supply chain.
- Business-critical and commercially sensitive information shared with shore-based service providers.
- The availability and use of computer-controlled critical systems for the ship's safety and for environmental protection.

These elements should be considered, and relevant parts incorporated in the company security policies, safety management systems, and ship security plans.

All relevant national legislation and flag state regulations must be complied with, and in some cases, alternative risk mitigating methods may have to be used to those suggested by these Guidelines.

The framework in adapted form, described in more detail in Annex 1, can provide an indication of the maturity of a company's approach to cyber security with respect to identifying risks, protecting systems and data, and detecting, responding to and recovering from a cyber-attack.

An increasing use of big data, smart ships and the 'internet of things' *(Lloyd's Register, Qinetiq and University of Southampton, Global Marine Technology Trends 2030)* will increase the amount of information available to cyber attackers, making the need for robust approaches to cyber security important both now and in the future.



2.1 Determination of vulnerability

It is recommended that a shipping company initially performs an assessment of the potential threats that may realistically be faced.

This should be followed by an assessment of the systems and procedures on board, in order to map their robustness to handle the current level of threat.

These vulnerability assessments should then serve as the foundation for a senior management level discussion/workshop. It may be facilitated by internal experts or supported by external experts with knowledge of the maritime industry and its key processes, resulting in a strategy centered around the key risks.

The growing complexity of ships, and their connectivity with services provided from shore side networks via the internet, makes onboard systems increasingly exposed to cyber-attacks.

In this respect, these systems may be vulnerable either as a way to deliver a cyber-attack, or as a system affected because of a successful cyber-attack.

In general, stand-alone systems will be less vulnerable to cyber-attacks compared to those attached to uncontrolled networks or directly to the internet. *Network topology will be explained in more detail in Annex 3.*

Care should be taken to understand how critical shipboard systems might be connected to uncontrolled networks.

When doing so, the human element should be taken into consideration, as many incidents are initiated by personnel actions.

Onboard systems could include:

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

Bridge systems: The increasing use of digital, networked navigation systems, with interfaces to shore side networks for update and provision of services, make such systems vulnerable to cyber-attacks. Bridge systems that are not connected to other networks may be equally vulnerable, as removable media are often used to update such systems from other controlled or uncontrolled networks.

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

Propulsion and machinery management and power control systems: The use of digital systems to monitor and control onboard machinery, propulsion and steering make such systems vulnerable to cyber-attacks.
The vulnerability of such systems can increase when they are used in conjunction with remote condition-based monitoring and/or are integrated with navigation and communications equipment on ships using integrated bridge systems.

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.

Passenger servicing and management systems: Digital systems used for property management, boarding and access control may hold valuable passenger related data.

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

Administrative and crew welfare systems: Onboard computer networks used for administration of the ship or the welfare of the crew are particularly vulnerable when they provide internet access and email.
They can be exploited by cyber attackers to gain access to onboard systems and data.
These systems should be considered uncontrolled and should not be connected to any safety critical system on board.

Communication systems: Availability of internet connectivity via satellite and/or other wireless communication can increase the vulnerability of ships.
The cyber defense mechanisms implemented by the service provider should be carefully considered but should not be solely relied upon to secure every shipboard systems and data.

The above-mentioned onboard systems consist of potentially vulnerable equipment which should be reviewed during the assessment.

More detail can be found in Annex 2 of these Guidelines.

Vulnerable information and data

The confidentiality, integrity and availability (CIA) - Federal Information Processing Standards, Publication 199, Computer Security Division Information Technology Laboratory, National Institute of Standards & Technology, Gaithersburg, MD 20899-8900) - model provides a framework for assessing the vulnerability to, and impact of:

- Unauthorized access to information or data about the ship, crew, cargo and passengers

- Loss of integrity of information and data relating to the safe and efficient operation of the ship following unauthorized modification

- Loss of availability of information or data due to the destruction of information and data or disruption to services

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

Potential Impact Levels

Sensitive information may include ship position, status of and readout from OT systems, cargo details, authorizations, certificates, etc

Example

*A power management system contains a **supervisory control and data acquisition** (SCADA) system controlling the distribution of onboard electric power.*

The system contains real-time sensor data which is used on board for power management. It also generates data about the power consumption, which is used by the shipping company for administrative purposes.
To determine if the information above is critical, the consequences likely to result from a compromise to the confidentiality, integrity or availability should be considered.

When doing so the shipping company should determine the criticality of the information stored, processed or transmitted by the SCADA system using the most sensitive information to determine the overall impact of the system.

Using the CIA model the shipping company concludes that:

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

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

The following table shows the result of the assessment.

SCADA System	Confidentiality	Integrity	Availability	Overall Impact
SENSOR DATA	LOW	HIGH	HIGH	HIGH
STATISTICS DATA	LOW	LOW	LOW	LOW

2.2 Risk assessment made by the company

As mentioned above, the risk assessment process starts by assessing the systems on board, in order to map their robustness to handle the current level of cyber threats. Elements of a Ship Security Assessment **(**regulation 8 of the ISPS Code**)** can be used when performing the risk assessment, which should physically test and assess the IT and OT systems on board.

1. Identification of existing technical and procedural controls to protect the onboard IT and OT systems. More information can be found with the Critical Security Controls;

2. Identification of IT and OT systems that are vulnerable, the specific vulnerabilities identified, including human factors, and the policies and procedures governing the use of these systems;

3. Identification and evaluation of key ship board operations that are vulnerable to cyber-attacks. These key operations should be protected in order to avoid disruption to commercial operations and ensure the safety of the crew, ship and the marine environment; and

4. Identification of possible cyber incidents and their impact on key ship board operations, and the likelihood of their occurrence in order to establish and prioritize mitigating measures.

Companies may consult with the producers and service providers of onboard equipment and systems to understand the technical and procedural controls that may already be in place to address cyber security.

Furthermore, any identified cyber vulnerability in the factory standard configuration of a critical system or component should be disclosed in order to facilitate better protection of the equipment in the future

2.3 Third party risk assessments

Self-assessments can serve as a good start, but may be complemented by third-party risk assessments to drill deeper, and identify the risks and the gaps that may not be found during the self-assessment.

Penetration tests of critical IT infrastructure can also be performed to identify whether the actual defense level matches the desired level set forth in the cyber security strategy for the company.

Such tests are normally performed by external experts simulating attacks using both IT-systems, social engineering and, if desired, even physical penetration of a facility's security perimeter.

Phase 1: Pre-assessment activities

Prior to commencement of a cyber-security assessment on board, the following activities should be performed:

- Map the ship's key functions and systems and their potential impact levels, for example using the CIA model;
- Identify main producers of critical shipboard IT and OT equipment;
- Review detailed documentation of critical OT and IT systems, and their interfaces;
- Identify cyber security points-of-contact at each of the producers and establish working relationships with them;
- Review detailed documentation on the ship's maintenance and support of its IT and OT systems;
- Establish contractual requirements and obligations that the shipowner/ship operator may have for maintenance and support of shipboard networks and equipment; and
- Support, if necessary, the risk assessment with an external expert to develop detailed plans and include producers and service providers.

Phase 2: Ship assessment

The goal of the assessment of a ship's network and its systems and devices is to identify any vulnerability that could compromise or result in a loss of service for the equipment, system, network, or even the ship.

These vulnerabilities and weaknesses could fall into one of two main categories:

1. Technical such as software defects, or outdated or unpatched systems, or
2. Design such as access management or implementation errors.

The activities performed under the assessment would include a build and configuration review of computers, servers, routers and firewalls. It should also include reviews of all available cyber security documentation and procedures for connected OT systems and devices.

Phase 3: Debrief and vulnerability review/reporting

Following the assessment, each identified vulnerability should be evaluated for its potential impact and the probability of its exploitation.

Recommended technical and/or procedural corrective actions should be identified for each vulnerability in a final report.

Ideally, the cyber security assessment report should include:

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

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

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

- Appendices – detailed records of all activities conducted by the cyber security assessment team and the tools used during the engagement.

Phase 4: Producer debrief

Once the ship-owner has had an opportunity to review, discuss and assess the findings, a subset of the findings may need to be sent to the producers of the affected systems.

Any findings, which are approved by the ship-owner for disclosure to the producers, could further be analyzed with support from external experts, who should work with the producer's cyber security point of contact to ensure that a full risk and technical understanding of the problem is achieved.

This supporting activity is intended to ensure that any remediation plan developed by the producer is comprehensive in nature and the correct solution to eliminate the vulnerabilities identified.

3. Reducing the risk

Reducing the risk should be the main deliverable of the company's cyber security strategy and outcome of the risk assessment decided by senior management.

At a technical level, this would include the necessary actions to be implemented to establish and maintain an agreed level of cyber security.

There are however occasions during the lifecycle of a ship where the normal controls are invalidated:

1. When there is no control over who has access to the onboard systems. This could, for example, happen during dry-docking or when taking over a new or existing ship. It is impossible to know if malicious software has been left in the onboard systems.

2. When third-party technicians connect via remote access to perform maintenance, read system data or troubleshoot.

3. When service providers or authorities connect using removable media directly to an onboard system.

Considerations on how to deal with such occasions may have to be done separately.

It is critical to identify how to manage cyber security on board and to delegate responsibilities to the master, IT-responsible officers and maybe the Company Security Officer.

Cyber security defenses may be technical and focused on ensuring that onboard systems are designed and configured to be resilient to cyber-attacks.

Defenses may also be procedural and should be covered by company policies, safety management procedures, security procedures and access controls. Both technical and procedural controls should be compatible with the confidentiality, integrity and availability (CIA) model for protecting data and information.

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

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

3.1 Technical cyber security controls

The Centre for Internet Security (CIS) provides guidance on measures that can be used to address cyber security vulnerabilities.

The control measures comprise of a list of twenty Critical Security Controls (CSC) that are prioritized and vetted to ensure that they provide an effective approach for companies to assess and improve their defenses.

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

Limitation to and control of network ports, protocols and services

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

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

Configuration of network devices such as firewalls, routers and switches

It should be determined which systems should be attached to controlled or uncontrolled *(In accordance with EC 61162-460:2015: Maritime navigation and radio communication equipment and systems - Digital interfaces - Part 460: Multiple talkers and multiple listeners - Ethernet interconnection - Safety and security)* networks.

Controlled networks are designed to prevent any security risks from connected devices by use of firewalls, routers and switches. Uncontrolled networks may pose risks due to lack of data traffic control and they should be isolated from controlled networks, as direct internet connection makes them highly prone to infiltration by malware.

- Networks, that are critical to the operation of a ship itself, should be controlled. It is imperative that these systems - *see Annex 2* - have a high level of security

- Networks, that provide suppliers with remote access to navigation and other OT system software on onboard equipment, should also be controlled. Such networks may be necessary for suppliers to allow upload of system upgrades or perform remote servicing. Shore side external access points of such connections should be secured to prevent unauthorized access.

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

Secure configuration for hardware and software

Only senior officers should be given administrator profiles so that they can control the set up and disabling of normal user profiles.

User profiles should be restricted to only allow the computers, workstations or servers to be used for the purposes for which they are required.

User profiles should not allow the user to alter the systems or install and execute new programs.

Email and web browser protection

Appropriate email and web browser protection serves to:

Protect seafarers and shore side personnel from potential social engineering.
Ensure that the exchange of sensitive information via email or by voice is appropriately protected to ensure confidentiality and integrity of data, for example protecting by encryption.
Prevent web browsers and email clients from executing malicious scripts.

Satellite and radio communication

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

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

The access interconnect is the distribution partner's responsibility.

The final routing of user traffic from the internet access point to its ultimate destination onboard ("last mile") is the responsibility of the ship-owner.

User traffic is routed through the communication equipment for onward transmission on board. At the access point for this traffic it is necessary to provide data security, firewalling and a dedicated "last-mile" connection.

When using a Virtual Private Network (VPN), the data traffic should be sufficiently encrypted.

Furthermore, a firewall in front of the servers and computers connected to the networks (ashore or onboard) should be deployed.

The distribution partner should advise on the routing and type of connection most suited for specific traffic.

Onshore filtering of traffic is also a matter between a ship-owner and the distribution partner.

It is not sufficient to either filter traffic or have firewalls; both types are needed to supplement each other to achieve a sufficient level of protection.

Producers of satellite communication terminals and other communication equipment may provide management interfaces with security control software that are accessible over the network.

This is primarily provided in the form of web-based user interfaces. Protection of such interfaces should be considered when assessing the security of a ship's installation.

Malware defenses

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

As a general guideline, onboard computers should be protected to the same level as office computers ashore.

Anti-virus and anti-malware software should be installed, maintained and updated on all personal work-related computers onboard.

This will reduce the risk of these computers acting as attack vectors towards servers and other computers on the ship's network.

The decision on whether to rely on these defense methods should take into consideration how regularly the scanning software will be able to be updated.

Data recovery capability

Data recovery capability is about having the ability to restore a system and/or data from a secure copy or image thereby allowing the restoration of a clean system. Essential information and software-adequate backup facilities should be available to ensure it can be recovered following a cyber-incident.

Where applicable, redundant information and OT systems should be tested to ensure they work as intended.

Retention periods and restore scenarios should be established to prioritize which critical systems need quick restore capabilities to reduce the impact.

Systems that have high data availability requirements should be made resilient.

OT systems, which are vital to the safe navigation and operation of the ship, should have backup systems to enable the ship to quickly and safely regain navigational and operational capabilities after a cyber-incident.

More detail on recovery can be found in Chapter 4 of these Guidelines.

Wireless access control

It should be ensured that wireless access to networks is limited to appropriate authorized devices.

Application software security (patch management)

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

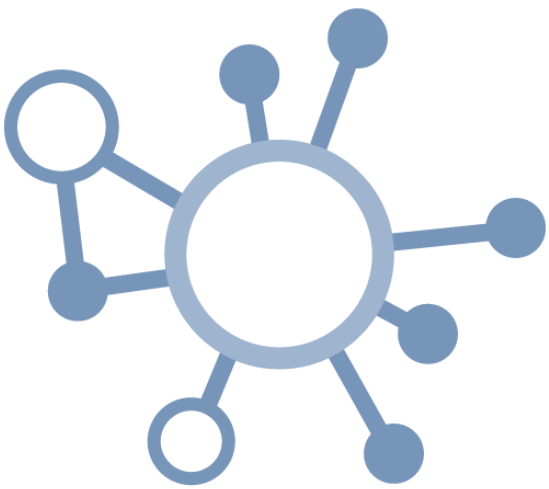
Secure network design

Onboard networks should be partitioned by firewalls to create safe zones.

The more firewalls that have to be passed through, to access a zone the more secure the systems and data in the zone.

Confidential and safety critical systems should be in the most protected zone.

See Annex 3.



Physical security

Security and safety critical equipment and cable runs should be protected from unauthorized access.

Physical security is a central aspect of cyber security (see also ISPS Code).

Boundary defense

Identifying intrusions and infections is a vital part of the controls.

A baseline of network operations and expected data flows for users and systems should be established and managed so that cyber incident alert thresholds can be established.

Key to this will be the definition of roles and responsibilities for detection to ensure accountability.

A more detailed process is defined in Annex 1.

Additionally a company may choose to incorporate an Intrusion Detection System (IDS) system or an Intrusion Prevention System (IPS).

Some of their main functions include identifying threats/malicious activity and code, and then logging, reporting and attempting to block the activity.

Further details concerning IDS and IPS can be found in Annex 3 of these Guidelines

3.2 Procedural controls

Procedural controls are focused on how seafarers use the onboard systems.

Plans and procedures that contain sensitive information should be kept confidential and handled according to company policies. Examples for procedural actions can be:

(a) Training and awareness

The internal cyber threat is considerable and should not be underestimated.

Personnel, even with the best of intentions, can be careless, for example by using removable media to transfer data from computer to computer without taking precautions; and data can be mishandled and files disposed of incorrectly. Training and awareness should be tailored to the appropriate levels for:

Onboard personnel, including the master, officers and seafarers; and
Shore side personnel who support the management and operation of the ship.

These guidelines assume that other major stakeholders in the supply chain, such as charterers, classification societies and service providers, will carry out their own best-practice cyber security protection and training.

It is advised that owners and operators ascertain the status of cyber security preparedness of their third party providers as part of their sourcing procedures for such services

An awareness program should be in place for all seafarers, covering at least the following:

- Risks related to emails and how to behave in a safe manner. Examples are phishing attacks where the user clicks on a link to a malicious site;

- Risks related to internet usage, including social media, chat forums and cloud-based file storage where data movement is less controlled and monitored;

- Risks related to the use of own devices. These devices may be missing security patches and controls, such as anti-virus, and may transfer the risk to the environment to which they are connected;

- Risks related to installing and maintaining software on company hardware, where the infection can be propagated, starting from infected hardware (removable media) or software (infected package);

- Risks related to poor software and data security practices where no anti-virus checks or authenticity verifications are performed;

- Safeguarding user information, passwords and digital certificates;

- Cyber risks in relation to the physical presence of non-company personnel, eg, where third-party technicians are left to work on equipment without supervision;

- Detecting suspicious activity and how to report if a possible cyber incident is in progress. Examples of this are strange connections that are not normally seen or someone plugging in an unknown device on the ship network;

- Awareness of the consequences or impact of cyber incidents to the safety and operations of the ship;

- Understanding how to implement preventative maintenance routines such as anti-virus and anti-malware, patching, backups, and incidence-response planning and testing; and

- Procedures for protecting against service providers' removable media before they are allowed to be connected to the ship's systems.

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

b) Upgrades and software maintenance

Hardware or software that is no longer supported by its producer or software developer will not receive updates to address potential vulnerabilities.

For this reason, the use of hardware and software which is no longer supported should be carefully evaluated by the company as part of the cyber risk assessment.

All hardware and software installations onboard should be updated to keep a sufficient security level.

Procedures for timely updating of software may need to be put in place taking into account the ship type, speed of internet connectivity, sea time, etc. Software includes computer operating systems, which should also be kept up to date (Further information can be found in the Standard on Software Maintenance of Shipboard Equipment by CIRM and BIMCO).

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

(c) Anti-virus and anti-malware tool updates

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

(d) Use of administrator privileges

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

Administrator privileges allow full access to system configuration settings and all data.

Users logging into systems with administrator privileges may thus enable existing vulnerabilities to be more easily exploited.

Administrator privileges should only be given to appropriately trained personnel who have a need, as part of their role in the company or onboard, to log into systems using such privileges.

In any case, use of administrator privileges should always be limited to execution of functions requiring such access.

User accounts should be removed when they are no longer in use. User accounts should also not be passed on from one user to the next using generic usernames.

User accounts should be removed when they are no longer in use. User accounts should also not be passed on from one user to the next using generic usernames.

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

To protect access to confidential data and safety critical systems, a robust password policy should be developed. Passwords should be strong and changed periodically.

The company policy should address the fact that over-complicated passwords which must be changed too frequently are at risk of being written on a piece of paper and kept near the computer.

(e) Physical and removable media controls

Transferring data from uncontrolled systems to controlled systems represents a major risk of introducing malware.

Removable media can be used to bypass layers of defenses and can be used to attack systems that are otherwise not connected to the internet.

A clear policy for the use of such media devices is essential; it must ensure that media devices are not normally used to transfer information between un-controlled and controlled systems.

There are however situations where it is unavoidable to use such media devices, for example during software maintenance.

In such cases, there should be a procedure in place to require checking of removable media for malware.

(f) Equipment disposal, including data destruction

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

(g) Obtaining support from ashore and contingency plans

Ships should have access to technical support in the event of a cyber-attack.

Details of this support and associated procedures should be available on board.

Please refer to Chapter 4 of these Guidelines for more information about contingency planning.

3.3 Defense in depth

The complexity and potential persistence of cyber threats means that a defense in depth approach should be considered. Equipment and data protected by layers of defenses are more resilient to cyber-attacks than equipment and data protected by only a single layer of defense.

Effective defense in depth may include multiple layers of technical measures combined with robust policies, security procedures and access controls. Existing security measures preventing access to the ship may be considered as a layer within the defiance in depth.

Preventing unauthorized access to the ship and ship systems has a role in ensuring that cyber vulnerabilities are not introduced or exploited.

Company policies should align cyber security with the requirements in the ISM and ISPS Codes and appropriately include relevant procedures.

4. Developing contingency plans

The company should develop, and ships should have access to, appropriate contingency plans in order to effectively respond to cyber incidents.

Responding to a cyber-incident may however be beyond the competencies held within the company and onboard due to the complexity or severity of such incidents. In such cases, external expert assistance should be available to ensure an effective response.

Without a contingency plan, decisions and actions may be made that inadvertently make recovery work more difficult and compromise evidence.

It is recommended that the contingency plans are tested periodically, for example using scenario exercises with all relevant personnel including management.

Contingency plans should include consideration of who has decision-making authority, when to call in external experts (and whom), as well as communication.

A non-exhaustive list of the most critical elements of contingency plans related to ships are:

- Knowing what to do in the case of disabling, or manipulation, of all types of electronic navigational equipment;

- Knowing what to do in the case of disabling, or manipulation, of industrial control systems for propulsion, auxiliary systems and other critical systems;

- Knowing how to verify that data is intact in cases where penetration is suspected but not confirmed;

- Procedures for handling ransom ware incidents; and

- Operational contingencies for ships in cases where land-based data is lost.

When a cyber-incident is discovered, it is important that all relevant personnel are aware of the exact procedure to follow.

It is crucial that contingency plans, and related information, are available in a non-electronic form as some types of cyber incidents can include the deletion of data, compromising of systems and shutdown of communication links.

4.1 Response plan

As with a successful cyber incident itself, an effective response has four stages:

1. Identify the cyber security incident;
2. Define the objectives for response and investigate the situation;
3. Take appropriate action to address a cyber-incident that effects systems and/or data; and
4. Recover systems, data and connectivity.

The response plan should, as a minimum, include the following considerations:

- Which systems does this apply to?

- Should systems be shut down immediately or kept running?

- Should certain ship communication links be shut down?

- Should certain pre-installed security software be activated?

- Who is the correct person in the IT department to contact immediately? In addition, what to do if communication links are severed?

4.2 Recovery

Recovery plans should be accessible to officers on board in accordance with their responsibilities defined in the plans.

The purpose and scope of each specific plan should be defined and understood by the officers and potential external IT personnel.

As explained in Chapter 3.1 essential information and software backup facilities should be available to ensure recovery can take place following a cyber-incident.

Recovery of essential ship or system functions related to the safe operation and navigation of the ship may have to take place with assistance from ashore.

How and where to get assistance, for example by proceeding to a port, needs to be part of the recovery planning carried out by the ship in cooperation with the ship-owner or operator.

4.3 Investigate cyber incidents

Investigating a cyber-incident can provide valuable information about the way in which a vulnerability was exploited.

This information can be used to improve the company approach to cyber security and/or provide the wider maritime industry with a better understanding of the threats it faces.

Any investigation should result in:

A better understanding of the threats facing shipping companies and the ships they operate;
Identification of lessons learned; and
Updates to technical and procedural control measures, as appropriate.

Investigating cyber incidents can be a complex and challenging task.

Companies should consider using external expert assistance to investigate such incidents as appropriate.

ANNEX 1

NIST framework

To manage risk, seafarers and owners should be aware of the probability that a cyber-incident will occur and the resulting impact, as outlined in Chapter 2 of these Guidelines.

The National Institute of Standards and Technology, U.S. Department of Commerce (NIST) framework aims to help understand, manage and express cyber-security risks both internally and externally within a ship's organization.

It can be used to help identify and prioritize actions for reducing cyber-security risks, and it is a tool for aligning policy, business and technological approaches to managing the risks.

The framework development is based on industry standards and best practices created through collaboration between various national authorities and the private sector. The framework relies on a variety of existing standards, guidelines and practices to enable critical infrastructure providers to achieve resilience.

The NIST framework is not a risk management process and does not provide guidance on prioritized and vetted actions to address cyber-security threats.

The framework table below provides guidance on the sort of activities/concerns to be considered to achieve specific cyber-security outcomes.

It is not a checklist of actions to perform but guidance on key outcomes identified as helpful in managing cyber-security risks.

It comprises three elements: functions, categories and sub-categories.

The actual functions are defined below and could be performed concurrently and continuously, to form an operational culture that addresses the dynamics of cyber security risks:

Identify – the aim should be to develop organizational understanding to manage cyber security risks to systems, assets, data and capabilities.

The activities in the identify function are foundational for effective use of the framework. Understanding the business context, the resources that support critical functions and the related cyber security risks enable an organization to focus and prioritize its efforts.

Categories within this function include asset management; business environment; governance; risk assessment; and risk management strategy, consistent with the company's risk management strategy and business needs.

ANNEX 1

Protect – the aim should be to develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
The **protect** function supports the ability to limit or contain the impact of a potential cyber incident. Examples of outcome categories within this function include access control; awareness and training; data security; information protection processes and procedures; maintenance; and protective technology.

Detect – the aim is to identify, develop and implement appropriate activities to identify the occurrence of a cyber-incident.
The **detect** function enables timely discovery of a cyber-incident.
Examples of outcome categories within this function include anomalies and incidents; security continuous monitoring; and detection processes.

Respond – the aim should be to develop and implement the processes and procedures to detect a cyber-incident. The **respond** function supports the ability to contain the impact of a potential cyber safety and security incident.
Examples of outcome categories within this include response planning, communications, analysis, mitigation, and improve

Recover – the aim is to ensure appropriate activities are developed and implemented to maintain resilience and to restore any capabilities or services that were impaired due to a cyber-incident.

The recover function supports timely recovery to normal operations to reduce the impact of a cyber-incident.

Examples of outcome categories within this function include recovery planning, improvements, and communications.

ANNEX 1

A IDENTIFY

VULNERABLE ASSETS	BUSINESS WORKING ENVIRONMENT	GOVERNANCE POLICY	RISK MANAGEMENT STRATEGIES	RISK ASSESSMENT PROCESSES
• Information and systems to be prioritised based upon classification, safety importance, criticality and business value • Physical devices inventorised • Software platforms and applications inventorised • Organisational communication and data flows are mapped • External information systems are catalogued	• Responsibilities are defined • Role in the supply chain identified • Place in critical infrastructure or sector identified • Priorities for organisation's mission, objectives and activities established • Resilience requirements to support delivery of critical services and the need for redundancy of shipboard OT systems are established	• Organisational information security policy is established • Safety and security roles and responsibilities are coordinated and aligned with onboard roles and external partners • Legal and regulatory requirements regarding cyber security are understood and managed	• Governance and risk management processes address cyber safety and security risks • Risk management processes are established, managed, and agreed by organisational stakeholders • Organisational risk tolerance is determined and clearly expressed • The organisation's determination of risk tolerance is informed by the ship, trade and cargo based on sector-specific risk analysis	• Asset vulnerabilities are identified and documented • Threat and vulnerability information is received from information-sharing forums and sources • Threats, both internal and external, are identified and documented • Potential business impacts and likelihoods are identified • Threats, vulnerabilities, likelihoods and impacts are used to determine risk • Risk responses are identified and prioritised

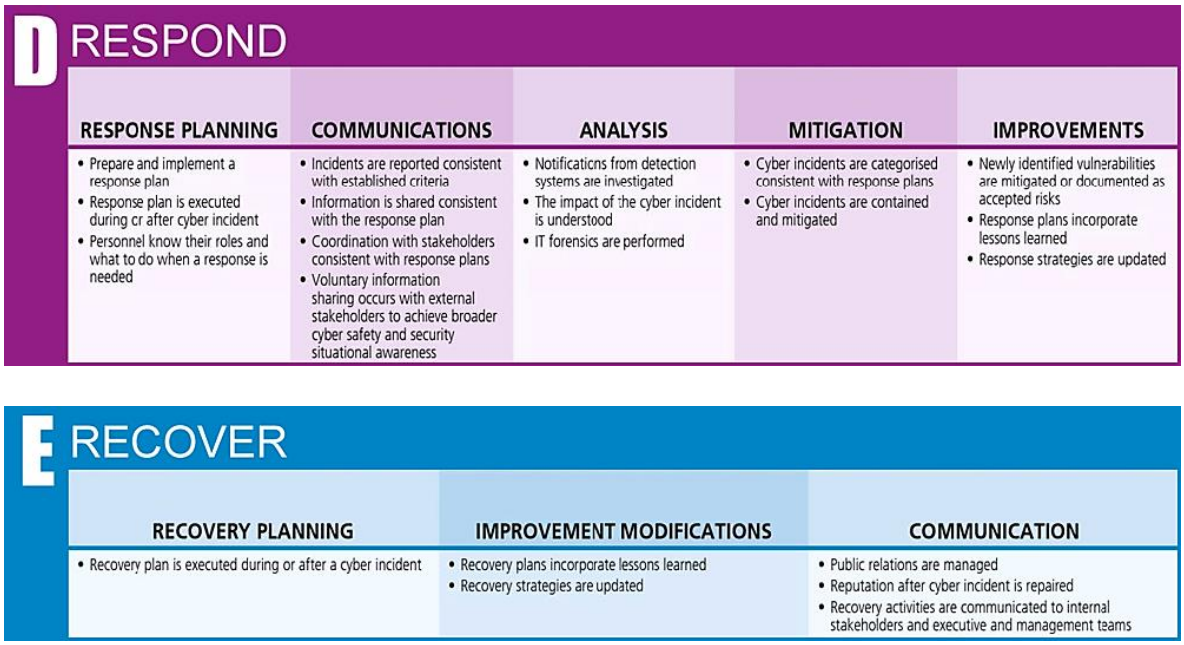
B PROTECT

ACCESS CONTROL PROCESSES	AWARENESS AND TRAINING	DATA SECURITY	INFO PROTECTION PROCESSES AND PROCEDURES	MAINTENANCE POLICY AND PROCEDURES	PROTECTIVE TECHNOLOGY APPLIED
• Identities and credentials are managed for authorised devices and users • Physical access to assets is managed and protected • Remote access is managed • Access permissions are managed, incorporating the principles of privileges and separation of duties • Network integrity is protected, incorporating network segregation where appropriate	• All users are informed and trained • Privileged users understand roles and responsibilities • Third-party stakeholders understand roles and responsibilities (eg, suppliers, authorities, port personnel, customers, partners) • Senior executives and senior officers understand roles and responsibilities • Physical and information security personnel understand roles and responsibilities	• Data-at-rest is protected • Data-in-transit is protected • Assets are formally managed throughout removal, transfers and disposition • Adequate capacity to ensure availability is maintained • Protection against data leaks is implemented • Integrity-checking mechanisms are used to verify software, firmware and information integrity • Development and testing environments are separate from the production environment • A baseline configuration of IT and OT systems on board is created and maintained	• A system development life cycle to manage systems is implemented • Configuration of management processes are in place • Backups of information are conducted, maintained and tested periodically • Policy and regulations regarding the physical operating environment for organisational assets are met • Data is destroyed according to policy • Protection processes are continuously improved • Effectiveness of protection technologies is shared with appropriate parties • Response plans (Cyber Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed • Response and recovery plans are tested • Cyber safety and security is included in human resources practices (deprovisioning, personnel screening)	• A vulnerability management plan is developed and implemented • Maintenance and repair of organisational assets are performed and logged in a timely manner, with approved and controlled tools • Remote maintenance of organisational assets is approved, logged and performed in a manner that prevents unauthorised access • Assessment/log records are determined, documented, implemented and reviewed in accordance with policy	• Removable media is protected and its use restricted according to policy • Access to systems and assets is controlled, incorporating the principle of "least functionality" • Communications and control networks are protected

C DETECT

ANOMALIES AND INCIDENTS	SECURITY MONITORING	DETECTION PROCESSES
• A baseline of network operations and expected data flows for users and systems is established and managed • Detected incidents are analysed to understand targets and methods • Incident data is aggregated and correlated from multiple sources and sensors • Impact of incidents is determined • Cyber incident alert thresholds are established	• The network is monitored to detect potential cyber security incidents • The physical environment is monitored to detect potential cyber incidents • Activity is monitored to detect potential cyber incidents • Malicious code is detected • Unauthorised code is detected • External service provider activity is monitored to detect potential cyber incidents • Monitoring for unauthorised personnel, connections, devices and software is performed	• Vulnerability scans are performed • Roles and responsibilities for detection are well defined to ensure accountability • Detection activities comply with all applicable requirements • Detection processes are tested • Incident detection information is communicated to appropriate parties • Detection processes are continuously improved

ANNEX 1



D RESPOND

RESPONSE PLANNING	COMMUNICATIONS	ANALYSIS	MITIGATION	IMPROVEMENTS
• Prepare and implement a response plan • Response plan is executed during or after cyber incident • Personnel know their roles and what to do when a response is needed	• Incidents are reported consistent with established criteria • Information is shared consistent with the response plan • Coordination with stakeholders consistent with response plans • Voluntary information sharing occurs with external stakeholders to achieve broader cyber safety and security situational awareness	• Notificaticns from detection systems are investigated • The impact of the cyber incident is understood • IT forensics are performed	• Cyber incidents are categorised consistent with response plans • Cyber incidents are contained and mitigated	• Newly identified vulnerabilities are mitigated or documented as accepted risks • Response plans incorporate lessons learned • Response strategies are updated

E RECOVER

RECOVERY PLANNING	IMPROVEMENT MODIFICATIONS	COMMUNICATION
• Recovery plan is executed during or after a cyber incident	• Recovery plans incorporate lessons learned • Recovery strategies are updated	• Public relations are managed • Reputation after cyber incident is repaired • Recovery activities are communicated to internal stakeholders and executive and management teams

Adapted and reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce.

Risk management programs offer the ability to quantify and communicate adjustments to the cyber security framework of an organization.

Risks can be handled in different ways, including, by mitigating the risks, transferring the risks, avoiding the risks, or accepting the risks, depending on the potential impact to the delivery of critical services. The risk management processes will make it possible to inform and prioritize decisions regarding cyber security.

This supports recurring risk assessments and validation of business drivers to help to select target states for cyber security activities that reflect desired outcomes.

To manage risk, ships' personnel and owners should be aware of and understand the probability that a cyber-incident will occur and the resulting impact.

With this, they can determine a level of risk which is unacceptable and should trigger action.

In connection with ships, the level of risk will be closely connected to the level of cyber security knowledge of the crew personnel on board and their ability to navigate the ship and use the ship's' systems in manual mode.

ANNEX 2

Target systems, equipment and technologies

This annex provides a summary of potentially vulnerable systems and data onboard ships to assist companies with assessing their cyber risk exposure.

Vulnerable systems, equipment and technologies may include:

Communication systems

- Integrated communication systems
- Satellite communication equipment;
- Voice Over Internet Protocols (VOIP) equipment
- Wireless networks (WLANs); and
- Public address and general alarm systems.

Bridge systems

- Integrated navigation systems
- Positioning systems (GPS, etc.);
- Electronic Chart Display Information System (ECDIS);
- Dynamic Positioning (DP) systems;
- Systems that interface with electronic navigation systems and propulsion / maneuvering systems;
- Automatic Identification System (AIS);
- Global Maritime Distress and Safety System (GMDSS);
- Radar equipment;
- Voyage Data Recorders (VDRs); and
- Other monitoring and data collection systems.

Propulsion and machinery management and power control systems

- Engine governor;
- Power management;
- Integrated control system;
- Alarm system; and
- Emergency response system.

Access control systems

- Surveillance systems such as CCTV network;
- Bridge Navigational Watch Alarm System (BNWAS);
- Shipboard Security Alarm Systems (SSAS); and
- Electronic “personnel-on-board” systems.

ANNEX 2

Cargo management systems

- Cargo Control Room (CCR) and its equipment;
- Level Indication System;
- Valve Remote Control System;
- Water Ingress Alarm System;
- Ballast Water Systems; and
- Gas liquefaction.

Passenger servicing and management systems

- Property Management System (PMS);
- Medical records;
- Ship passenger/seafarer boarding access systems; and
- Infrastructure support systems like Domain Naming System (DNS) and user authentication / authorization systems.

Passenger-facing networks

- Passenger Wi-Fi or LAN internet access
- Guest entertainment systems and,
- Communication.

Core infrastructure systems

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

Administrative and crew welfare systems

- Administrative systems
- Crew Wi-Fi or LAN internet access, for example where seafarers can connect their own devises.

ANNEX 3

Shipboard networks

In order to design and build a secure network, many factors should be taken into consideration, such as the topology and placement of hosts within the network; the selection of hardware and software technologies, authentication and authorization system; and careful configuration of each component.

First, the physical and logical layout of the network should be considered.

On the physical side, the network provides the distribution of data to the workplaces on board and connectivity to the servers, which comprise the intranet, to the internet and possibly to other company locations or supply-chain partners and remote users.

It is crucial to consider the physical location onboard the ship, particularly with a view to restricting access and maintaining physical security of the network installation and control of access points.
A company policy should be considered in order to decide which parts of the network should be controlled or uncontrolled.

If the ship uses a complex network infrastructure, direct communication with an uncontrolled network should be prevented. Furthermore, a number of safety features should be built into the systems ensuring access time restrictions and password protection via an application server.

As a rule, only equipment that needs to communicate with each other over the network should be able to do so.

Considerations should be made on how to maximize the security of the switches themselves.

It should be made impossible to jump from one Virtual Local Area Network (VLAN) to another more sensitive VLAN.

To achieve the highest level of security, only one VLAN per switch should be configured.

This would minimize the chance of an attacker jumping VLANs and reduce the chance of misconfiguration. Depending on budget and risk assessment, the designer may decide that it is acceptable to combine multiple VLANs on a single switch.

It is also crucial that default security settings are reviewed and amended to ensure that data cannot be altered using generic factory default username and password, and additional devices cannot be added to the network without appropriate authorization

ANNEX 3

The basic design needs an infrastructure for managing the network.

One or more management workstations may be needed with various servers with different layers of security.

As these servers may form the foundation of network management and security, it is recommended that a ship should use a separate management VLAN, which is isolated from the rest of the network by a firewall and access lists.

Ideally, the only traffic allowed into the management network either is from the managed devices or protected by encryption.

A design goal will be to keep management traffic away from the production network to eliminate the possibility of interception. Ideally, each device should be configured with a physical port on the management VLAN.

If this is not possible owing to physical or other limitations, the management part of the system should be encrypted.

Controls for controlled networks should be measurable and monitorable.

Networks for different purposes should be kept separated by using a gateway/router between them, for example, administration net, control and monitoring systems (CAMS) or navigation equipment.

Each net should have its own range of IP addresses/subnet masks to avoid interconnection without a gateway/router.

By default, direct connections from an uncontrolled network should not be allowed.

Access to the controlled LAN from an uncontrolled LAN should be managed by registration of connections, activation registrations and automatic deactivation after a pre-defined period.

Such operations should be kept restricted to authorized personnel only, and it should be ensured that the operation could only take place after permission from an administrator.

Direct connections should only take place through a firewall or by activation from the controlled network side.

When bridging between uncontrolled and controlled LANs, a number of security measures should be in place to:

- Prevent unauthorized access by implementing network separation and/or traffic management. This can be implemented using VLANs and firewalls.

- Avoid malicious software. The main prevention measure is to maintain up-to-date anti-virus, anti-spyware and anti-adware software together with up-to-date operating system patch management on all computers accessing the LAN.

- Prevent internet access from hybrid LAN computers. Internet should only be accessible by computers that do not access onboard operational systems.

- Manage encryption protocols to ensure privacy and commercial communications.

- Manage use of certificates to verify origin of digitally signed software.

It is essential to monitor and manage systems in order to ensure that the IT personnel, in conjunction with the teams in the organization ashore and onboard the ship, are aware of the networks' status.

There are network Intrusion Detection Systems (IDSs) available which in real time can alert the system administrator when the network systems are attacked.

They work by inspecting the traffic on the wire and generating alerts if suspicious activities are identified

IDS/IPS

Generally, intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible cyber incidents, which are violations or imminent threats of violation of computer-security policies, acceptable-use policies or standard security practices.

IPSs are primarily focused on identifying possible cyber incidents, but many may also identify reconnaissance activity, which may indicate that an attack is imminent. In such situations, the IPS might be able to block reconnaissance and notify security administrators, who can take action if needed to alter other security controls to prevent related cyber incidents.

A network IDS/IPS can be a regular computer running software, an appliance-type device running proprietary software or even a specialized card built into a switch.

ANNEX 3

A firewall usually is a device or application that enforces security policy based on specific elements (for example source-destination addresses and ports) whereas an IPS is an enhanced device or application that analyses the traffic itself, looking for known threats while rejecting those that do not comply with the security policy.

Host-based intrusion detection or various kinds of proactive log-monitoring software are also recommended.

Sensors of the IDS/IPS should be placed logically within the topology of the network.

Unless resources for maintaining the network IDS/IPS analyzing and responding to alerts are plentiful, a few strategically placed sensors may be beneficial.

Other uses of the IPSs are:

- Identifying security policy problems;

- Documenting the existing threat to an organization; and

- Deterring individuals from violating security policies.

When an IPS is selected, the company should make sure it complies with the latest industry best practices and guidelines often described by authorities and organizations (for example NIST).

Some of the common detection methodologies include:

Signature-based detection: the process of comparing a known threat against observed events to identify possible cyber incidents.

Anomaly-based detection: the process of comparing definitions of what activity is considered normal against observed events to identify notable deviations. An IPS using anomaly-based detection has profiles that represent the normal behavior of such things as users, hosts, network connections or applications.

The profiles are developed by monitoring the characteristics of typical activity over a period.

Stateful protocol analysis: the process of comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations.

It is recommended to place a sensor on the internet-facing segment, because the public servers are a visible target to attackers.

Another sensor should be placed behind the firewall, to monitor traffic between the internet and the internal LAN. An IDS/IPS sensor could also be placed by a remote-access segment, for instance a dial-up server or VPN.

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.

Asset management is control of any data, computer or device.

Configuration management is a practice and process of handling hardware, software and firmware changes systematically so that a device or system maintains its integrity over time.

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

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

Cyber security onboard ships protect;

The operational technology against the unintended consequences of a cyber-incident;
Information and communications systems and the information contained therein from damage, unauthorized use or modification, or exploitation; and/or
Against interception of information when communicating and using the internet.

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

Denial of Service (DoS) is a form of cyber-attack which prevents legitimate and authorised users from accessing information, usually by flooding a network with data. A distributed denial of service (DDoS) attack involves a cyber-attacker taking control of multiple computers and/or servers to deliver a denial of service attack.

Detection processes are methods of detecting intrusions into computers and networks.

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

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

Flaw is unintended functionality in software.

ANNEX 4

Information security is the security applied to information (rather than systems) protecting it from unauthorised access, disclosure, modification or destruction.

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

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

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

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

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

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

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

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

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

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.

Router is a device which forwards data from one network to another network, eg, from a satellite communications network to an onboard computer network.

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

ANNEX 4

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

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

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

Wide Area Network (WAN) is a network that can cross regional, national or international boundaries.

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