DROMON BUREAU OF SHIPPING

clever solutions | beyond class

TECHNICAL PUBLICATION

Guidelines on Maritime Cyber Risk Management

Practices for implementation

JANUARY 2022

REVISION HISTORY

Rev. No	Date	Amendments
1	January 2022	The document has been revised to include information based on IACS Rec.166 as well as from MSC-FAL.1/Circ.3/Rev.1. Section on ISO 27001 has been included.
Initial	October 2018	Initial issue

CONTENT

INTRODUCTION

Effective cyber risk management should also consider safety and security impacts resulting from the exposure or exploitation of vulnerabilities in information technology systems.

This could result from inappropriate connection to operational technology systems or from procedural lapses by operational personnel or third parties, which may compromise these systems (e.g. inappropriate use of removable media such as a memory stick).

These rapidly changing technologies and threats make it difficult to address these risks only through technical standards. As such, this Publication recommends a risk management approach to cyber risks that is resilient and evolves as a natural extension of existing safety and security management practices.

For details and guidance related to the development and implementation of specific risk management processes, Ship-Owners should refer to specific Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

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

Predicated on the goal of supporting safe and secure shipping, which is operationally resilient to cyber risks, this Publication provides recommendations that can be incorporated into existing risk management processes.

DEFINITIONS

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.

Attack surface is the computer based systems which can be accessed externally either through network or locally.

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

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

Category of maintenance means A category assigned to a software maintenance activity based upon the reason for undertaking the maintenance, which may be:

- Bug Fix (resolving software bugs);
- Feature Release (adding additional functionality);
- Compliance Update (maintaining conformity with regulations);
- Security Update (protecting against cyber threats);
- Obsolescence Update (addressing software and/or hardware that is no longer supported);
- Or some combination of the above.

Computer based system is Combination of interacting programmable devices and/or cyber systems organized to achieve one or more specified purposes. Computer based System may be a combination of subsystems connected via network. Onboard computer based System may be connected directly or via public means of communications (e.g. Internet) to ashore based computer based Systems, other vessels' computer based System and/or other facilities.

Contingency Plan is the plan which provides essential information and established procedures to ensure effective response and recovery in case of a cyber incident affecting computer-based system providing essential contribution.

Critical System is the technical systems that the sudden operational failure of may result in hazardous situation.

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

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 resilience means capability to reduce the occurrence and mitigating the effects of incidents arising from the disruption or impairment of operational technology (OT) used for the safe operation of a ship, which potentially lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

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

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.

Cyber Safety is the condition of being protected against vulnerabilities resulting from inadequate operation, integration, maintenance and design of cyber related systems, and from intentional and unintentional cyber threats.

Data Quality is intended as the activity, or set of activities, aimed at enforcing the security of data generated, processed, transferred and stored in the operation of computer based systems on board. The three terms below can be broadly defined as following:

- CONFIDENTIALITY – a loss of confidentiality because of an unexpected or unauthorized disclosure of information.
- INTEGRITY – a loss of integrity because of an unexpected or unauthorized modification of information
- AVAILABILITY – a loss of availability because of an unexpected or unauthorized destruction of the information or disruption of access to, or use of an information system.

Data Provider is stakeholder that supplies data necessary for the functioning of the computer based system on board.

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

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

Demilitarized zone (DMZ) is A physical or logical sub network that contains and exposes an organization's external-facing services to an untrusted network.

DLP means Data Loss prevention.

Essential Systems are Systems contributing to the provision of essential services for the safe operation of the ship.

Failure Mode and Effects Analysis (FMEA) is A technique to identify foreseeable causes of independent failures together with their effects on the hardware, software or process, based on a systematic decomposition into elements. The technique can be used to demonstrating that foreseeable risks have been identified and accounted for.

Firewall is a logical or physical break designed to prevent unauthorized 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.

HMI means Human Machine Interface.

Information Technology (IT) is the automated systems used for storing, retrieving, processing and sending data [IT networks, e-mail, administration, accounts, crew lists, planned maintenance, spares management and requisitioning, electronic manuals, electronic certificates, permits to work, charter party, notice of readiness, bill of lading, etc.].

Integrated system is Interconnected system combining a number of interacting shipboard equipment Organized to achieve one or more specified purposes.

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.

Local control control from a location in the immediate vicinity of the concerned machinery.

Malware generic term for a variety of malicious software, which may adversely impact the performance of computer systems.

Managed Network network which uses managed switches, that allows connected network devices to communicate with each other, and also gives the network administrator greater control over managing and prioritizing network traffic. Network traffic can be controlled and prioritized through configuration changes.

Media Access control (MAC) is A hardware address that differentiates one device on a network from another.

M2M is Machine to machine interface.

Network is A group of two or more computer systems linked together.

Network Hub is Network hub, is a common connection point for devices in a network.

Network Router is A network device which is responsible for routing traffic from one network to another network.

Network switch (Switch) is A device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device.

Operational technology (OT) includes devices, sensors, software and associated networking that monitor and control onboard systems [PLCs, SCADA, On-board measurement and control, ECDIS, GPS, Remote support for engines, Data loggers, Engine & Cargo control, Dynamic positioning, etc.].

OT system means Computer based systems, which provide control, alarm, monitoring, safety or internal communication functions.

Patches means Software designed to update installed software or supporting data to address security vulnerabilities and other bugs or improve operating systems or applications.

Programmable device Physical component where software is installed.

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

Protocols are a common set of rules and signals that computers on the network use to communicate.

Quality of Service (QoS) is The measurable end-to-end performance properties of a network service.

RAID means Redundant Array of Independent Disks.

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

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, analyzing, assessing and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

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

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

Simulation test is System testing where the equipment under control is partly or fully replaced with simulation tools, or where parts of the communication network and lines are replaced with simulation tools.

System Categories (I, II, III) System categories based on their effects on system functionality, which are defined in IACS UR E22.

- Those systems, failure of which will not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.
- Those systems, failure of which could eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.
- Those systems, failure of which could immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

System Integrator The stakeholder that combines shipboard equipment into an integrated system.

Test Case is Set of conditions, methods and expected results under which a tester will determine whether a software application is working according to the design specifications or not.

Unmanaged Network is Network which uses unmanaged switches, that allows devices connected to a network to communicate with each other. It is a plug-and-play switch that does not require or allow any user intervention, setup, or configuration.

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.

BACKGROUND

Cybertechnologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment. In some cases, these systems have to comply with international standards and Flag Administration requirements. However, the vulnerabilities created by accessing, interconnecting or networking these systems can lead to cyber risks which **should be addressed**.

Vulnerable systems may include, but are not limited to:

- Bridge systems;
- Cargo handling and management systems;
- Propulsion and machinery management and power control systems;
- Access control systems;
- Passenger servicing and management systems;
- Passenger facing public networks;
- Administrative and crew welfare systems; and
- Communication systems.

As a preliminary remark, the distinction between information technology and operational technology systems should be considered. Information technology systems are used to create, store and transfer data as information, whereas operational technology systems are used to control or monitor physical processes. Consequently, the protection of information and data exchange within these systems should also be considered.

While these technologies and systems provide significant efficiency gains for the maritime industry, they also entail risks to critical systems and processes linked to the operation of systems integral to shipping. These risks may result from vulnerabilities arising from inadequate operation, integration, maintenance and design of cyber-related systems, and from intentional and unintentional cyberthreats.

Cyberthreats may arise from malicious actions (e.g. hacking or introduction of malware) or the unintended consequences of benign actions (e.g. software maintenance or user permissions). In general, these actions either expose vulnerabilities (e.g. outdated software or ineffective firewalls) or exploit a vulnerability in operational or information technology. Thus, cyber risk management should consider both kinds of threat.

Vulnerabilities can result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyberdiscipline. In general, where vulnerabilities in operational and/or information technology are exposed or exploited, either directly (e.g. weak passwords leading to unauthorized access) or indirectly (e.g. the absence of network segregation), there can be implications for security and the confidentiality, integrity and availability of information.

Additionally, when operational and/or information technology vulnerabilities are exposed or exploited, there can be implications for safety, particularly where critical systems (e.g. bridge navigation or main propulsion systems) are compromised.

Effective cyber risk management should also consider safety and security impacts resulting from the exposure or exploitation of vulnerabilities in information technology systems. This could result from inappropriate connection to operational technology systems or from procedural lapses by operational personnel or third parties, which may compromise these systems.

A REAL EXAMPLE

Maersk was among a number of multinational companies that were hit by the "NotPetya" cyberattack on June 17, 2017. Its IT systems were disabled, preventing the shipping line from taking new orders for several days. Maersk announced that it kept its outlook despite the costs of the cyberattack, as the container shipping market improves.

The ransomware attack initially targeted Ukraine and was rapidly propagated across Europe and India.

According to Maersk, the breakdown affected all of its business units, including container shipping, port and tug boat operations, oil and gas production, drilling services, and oil tankers.

The IT breakdown could extend across the company's global operations, as reported by a spokeswoman, but it was left unclear how Maersk's operations were impacted.

With a fleet of more than 600 container vessels, Maersk is the world's biggest shipping company with a market share of around 16%. The company handles around 25% of all containers shipped on the key Asia-Europe route.

Maersk's port operator APM Terminals was also hit, with Dutch broadcaster RTV Rijnmond reporting that 17 shipping container terminals run by APM Terminals had been hacked, including 2 in Rotterdam and 15 in other parts of the world.

The RTV report stated that computers were infected by ransomware that encrypted hard drives at APM Terminals.

IMO GUIDELINES

The International Maritime Organization (IMO) recognizing the need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, approved through its Maritime Safety Committee (MSC) and the Facilitation Committee, the MSC.428(98) and the MSC-FAL.1/Circ.3/Rev.1. The resolution provides high-level recommendatory recommendations for maritime cyber risk management that can be incorporated into existing risk management processes.

In particular, the ISM code stresses the need to encompass cyber risk management in organizations' safety management systems, in accordance to its objectives and functional requirements. Ship Owners need to ensure that the adjustments of appropriately addressing cyber risks, will be in effect **no later than the first annual verification of the company's Document of Compliance after 1 January 2021**. The ISM acknowledges the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management.

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

These IMO Guidelines are primarily intended for all organizations in the shipping industry and envisage to encourage safety and security management practices in the cyber-domain.

Recognizing that no two organizations in the shipping industry are exactly alike, the Guidelines are expressed in broad terms in order to have a wide scope of application. Ships with limited cyber-related systems may find an elementary application of the Guidelines to be sufficient; however, ships with complex cyber-related systems may require a greater standard of care and should seek additional resources through reputable industry and Government partners.

For the purposes of the Guidelines, *cyber risk management* is defined as the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders.

The goal of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyber risks.

Effective cyber risk management should start at the senior management level. Senior management should cultivate a culture of cyber risk awareness into all levels of an organization. Additionally, it should establish a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.

An accepted methodology that organization could follow to achieve the above, is through comprehensive comparison. Initially the organization could carefully examine and identify its current cyber risk management position. The latter should then be contrasted with the desired standard of cyber risk management that the organization has set out to accomplish. This comparison process may cause ongoing gaps or deficiencies to become apparent, which can subsequently be addressed through a prioritized cyber risk management plan.

A risk-based prioritization approach will aid organizations to allocate their resources effectively, as it will instruct them which issue is more efficient to be dealt with first.

The Guidelines present the functional elements that support effective cyber risk management. These functional elements are not sequential – all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework:

1. Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.
2. Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
3. Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.
4. Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.
5. Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

These functional elements encompass the activities and desired outcomes of effective cyber risk management across critical systems affecting maritime operations and information exchange and constitute an ongoing process with effective feedback mechanisms.

Effective cyber risk management should ensure an appropriate level of awareness of cyber risks at all levels of an organization. The level of awareness and preparedness should be appropriate to roles and responsibilities in the cyber risk management system.

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

1. The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.
2. ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
3. United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).
4. Consolidated IACS Recommendation on cyber resilience (IACS Rec. 166). April 2020.

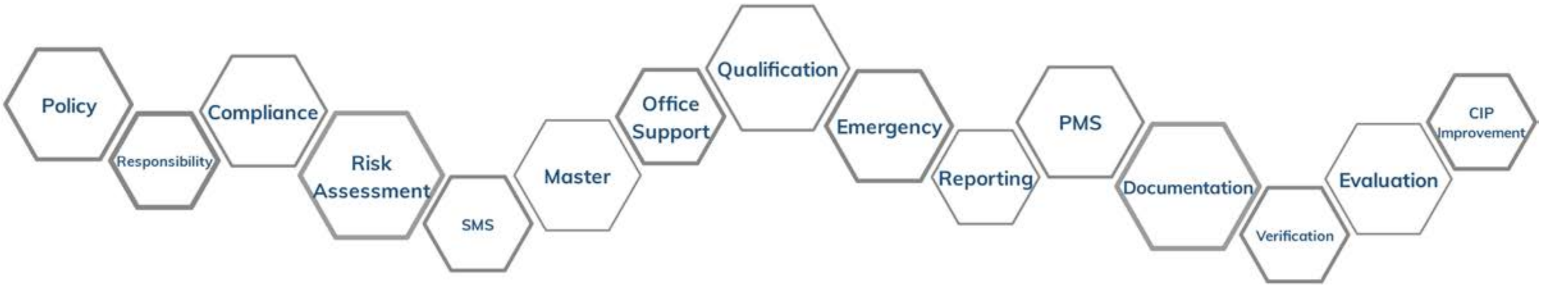
Reference should be made to the most current version of any guidance or standards utilized.

PRACTICES FOR IMPLEMENTATION

The approach to cyber risk management described below provides a foundation for better understanding and managing of cyber risks, enabling a risk management approach to address cyberthreats and vulnerabilities.

The ISM Code is a mandatory international instrument to establish measures for the safe management and operation of ships. The modular concept of the Code allows the integration of necessary cyber security measures in the Safety Management System (SMS) of the company.

The incorporation allows the company to amend their own safety management system with the required and specific Cyber Risk requirements.



A. Company's Policy

The top management of a shipping company recognizes the fundamental risks to safe ship operation through cyber crime and the need for regulation and those for the expansion of the own ISM management objectives. The existing policy needs to be amended with cyber security aspects and required measures. Cyber security becomes a direct concern of the management board. All measures are should ideally be tailored to protect the safe operation of ships while sustaining prevention of pollution in all circumstances.

B. Responsibility

The ultimate responsibility in cyber security remains with the top management. To the extent possible and depending on company´s organization and size, an appropriate person - usually the head of the company's IT department - will be designated as the responsible person for managing and protecting against cyber risks and to assist the Master in conducting assigned shipboard tasks and responsibilities. Queries to the P&I and H&M insurers can influence the consideration of the significance and priority, and thus the scope of the measures especially when considering financial risks.

C. Compliance

Rules, guidelines and recommendations of the IMO, Flag State, Class and related industry are identified, and the essential requirements are derived. They form a basis for creating and updating the Risk Assessment (RA) and Company´s SMS. Legal registers will be amended or recreated accordingly and list these guidelines and recommendations. Each organization should elect measures for implementation that correspond to its size. Attempts to establish and maintain a continuous improvement process should take primacy over concerns to regulate and cover all issues at once.

D. Risk assessment

With the ISM Risk Assessment the risks and necessary safeguards are being identified. Unless an equivalent system exists, the following steps can be used for a systematic assessment.

1. Hazard Identification

   A non-exhaustive list of all potential hazards and potentially endangered systems on board need to be prepared. The list is subject to futher updates, and provides the benchmark for risk assessment. If the list is devised by a diversified team of experts (e.g. Masters, Engineers, DPA, quality manager, CSO, super-intendents, IT managers/ experts, top management, etc.) and subdivided in advance into the four areas IT, IF, OT and ACP, this can enhance the list's effectiveness to portray an accurate overview of the hazards.

   To gain an overview, first create a list with all potential hazards and potentially endangered assets, without prioritizing or making a risk-determination.

   Makers and contractors may have to be involved if the own resources are not sufficient – this may be necessary in particular for OT and IF protection.

   Depending on its size, a company may not have the necessary resources to identify hazards, especially in respect to the areas of IT and IF. In this case external makers and contracts may have to be consulted.

2. Resource Identification

   The list should identify which resource becomes necessary.

3. Potential safeguards

   A non-exhaustive list of all potential safeguards (technical, operational and personal) as a non-exhaustive list to be further updated. The list is subject to further updates and provides an additional benchmark for risk assessment.

   A possible way to develop such a list, could be in a brainstorming session comprised by different departments (IT, DPA, QM/QHSE, Nautical & Technical Department top management or others). Such safeguards could be:

   Technical

   - Backup Storage;
   - Anti-virus Software;
   - Firewall;
   - Limitation on e-mail attachments (e.g. allow only .pdf, .txt files and block all other types of attachments);
   - Remote access control: authentication of accesses; and
   - Unnecessary software functions & plug-ins are removed or locked.

   Operational

   - Password policy, prescribing regular changes or passwords;
   - Continuous weak point analysis and evaluation of the reporting system;
   - Automatic screen lock after the elapse of a given number of minutes, and manual screen lock before leaving the work station;
   - Audit and
   - Remote access control: Authentication of accesses (RAS, VPN).

   Personal

- Awareness programmes;
- Initial Familiarization;
- On-demand training (administration, employees);
- Training content: behavior, monitoring, detection, response measures, password management; and
- Disciplinary measures in case of intentional/non-intentional disregard of instructions.

Cyber security should include measures for personal data protection.

4. Assessment: Based on the preparation: determining the risks, safe guards and responsibilities

Processing the Risk Assessment (RA) to identify and assess the risk. Risk is determined by multiplying the likelihood of an event materializing, with the severity of harm of the event. When the presence of a risk is successfully identified, appropriate measures should be implemented in a hierarchical manner, akin to the measures principle of occupational health & safety standards. This covers technical, processual and human aspects. The technical control measures take precedence over the two other kinds of safeguards.

Personal behavioural measures may be faster faster in terms of implementation and a cheaper means to achieve protection. Notwithstanding it cannot be assured and cannot be perceived as safe. This is only possible by technical measures. The RA must be constantly reviewed and updated.

Risk = Likelihood of occurrence x Severity caused by the event

	Severity of harm		
Likelihood of occurrence	Medium risk	High risk	Very high risk
	Low risk	Medium risk	High risk
	Low risk	Low risk	Medium risk

Table 1

Potential impact	Action and timescale
Low risk	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on company and ship, organizational assets, or individuals
Medium risk	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
High Risk	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.

Table 2

The results of the risk assessment - and thus the necessary safe guards – are a subject to be included into the SMS of the company. They are recorded as a process or operating instruction or in another suitable way. Basically, the required measures should be made known to the crew. If the RA determines that certain measures should not be made public or should not address all persons within the Company, they can be a subject to the Ship Security Plan (SSP).

E. Master

The ISM lists qualification procedures for the master so that he can meet those SMS requirements directed to his position. The company's organization considers that the new cyber security tasks are not solely the responsibility of the captain.

F. Office support

By a suitable organization, the captain will receive qualified land-based support to fulfil his SMS tasks. This includes responding to a cyber-attack; responding to the consequences of an attack; and restore (backup measures).

G. Qualification

Newly employed crew members and office staff should receive a familiarization in the company's SMS cyber security activities, while incumbent crew members and staff receive additional familiarization in case they change their job position within the firm due to promotion, or any other reason.

Instructions are deemed necessary for all persons with cyber security tasks and for all persons being in contact with a ship. Familiarization, instruction and further training measures are regularly recurring and should be repeated as necessary. The SMS prescribes a training and qualification plan and describes measures to determine training needs. This includes seafarers and office personnel. The scope of each person's training requirements depends on their position on board / in the company.

H. Emergency

The SMS contains a cyber security contingency plan for the sea and shore office sector. This contingency plan is regularly practiced through exercises, simulations and training with the aim of reflective action. The shore organization has emergency plans in place to assist the captain. The plans include measures to:

- respond to an attack and its consequences; and
- restore (backup measures).

An IT manager (if available) may support the shore-based emergency response team.

I. Reporting

Incidents, accidents, near-misses and other relevant occurrences should be reported to the responsible departments by using the ISM reporting system. Reports should be subject to an assessment and analysis. As a result, corrective and preventative actions will be determined and communicated.

1. Navigation

Masters and nautical officers should be trained to know, recognize and respond to hazardous situations. In addition to general navigational instructions and qualification measures, the existing ISM emergency plans should be amended as necessary.

For example, hazards can result from:

- Failure or manipulation of GPS and DGPS data (jammer);
- Failure or manipulation of AIS data;
- Incorrect speed input leads to faulty ARPA evaluation;
- Incorrect ECDIS information;
- Failure (shut down) and reboot error of the radar equipment; and
- Impact on the control and monitoring of the machinery and power management.

2. Human Element

Lack of awareness, missing or failing to conduct recurring familiarization and training measures for seafarers and shore staff increase the likelihood of misconduct.

3. IT (limiting)
   The RA and SMS should not be reduced to IT only. OT, interfaces and access to IT/OT should be included in any case.

4. Sustainability
   RA and SMS should be continually reviewed and adjusted to respond to the changing cyber threats. One-time integration into the SMS is inadequate.

5. Risk Ship-Shore Connections
   Available connections to the "outside" of a system may become an unprotected gateway.

6. Risk container stowage planning
   Correctness of container information (weight, dangerous goods, stowage positions) is primarily the task of the terminal and the character and is an important component for the safe carriage of cargoes. Despite that fact, the RA and SMS should also reflect the electronic data exchange regarding stowage planning between shore and ship.

J. PMS

PMS (Planned Maintenance System): the safety measures that have been identified at the RA as recurrently been put in practice, e.g. software updates, are added to the PMS. The PMS monitors and documents those measures. The Critical Equipment area will be amended to the needs and required details determined via the RA.

K. Documentation

Generally, the SMS describes the applicable requirements for any documentation. These are taken over for the field of cyber security. If documented measures and requirements are within a sensitivity range that does not permit public documentation in the SMS, specific measures should be implemented which are accessible only to a limited group of persons on board and ashore.

L. Verification

Internal audits on board and onshore at the office will be amended with cyber security aspects and will be conducted at intervals not exceeding 12 months. The implementation of the cyber security management to the company ISM system as well as the continuous updating shall be monitored and verified by audits and reviews.

M. Evaluation

The Company should regularly verify and evaluates the safety management system.

N. CIP Improvement

Companies should comprehend the fast-changing nature of Cyber security and try to keep pace with its continuous changes. In this regard, a one-off introduction and implementation of safeguards is inadequate. Henceforth, RA and SMS should be updated to sustain a continuous improvement process.

MORE ACTIONS THAT CAN PREVENT CYBER ATTACHED AND INCIDENTS

1. Encryption techniques and safeguarding encryption keys

The knowledge to implement the right encryption protocol for your system from basic RSA or AES algorithms to advance technologies like BB84 quantum key distribution is essential to protect sensitive information while in transit or rest. The storing of private or public keys in another environment that does not link to any of your systems is highly recommended.

2. Brute-Force attacks and Mask attacks

Are the very common type of attacks and lethal when combined with HPC (High-Performance Computing). The intruder designs or uses publicly available software (Hashcat, John the Ripper) that will try different combinations of passwords and eventually access your system in a matter of time.

3. DDOS and DOS attacks

This is a denial of service attack on both connectionless (UDP) and connection-oriented (TCP) protocols that can flood a network with packet request and eventually shut it down. A very common point of entry is Smart TVs, Printers, or any other device with a low level of networking card. This can be prevented with third-party providers (Cloudflare) that will reroute your entire network on their servers, and are capable of handling billions of requests per minute.

4. Penetration Testing

A service that can be performed based on your requirements and prevent any security thread.

CONTROL, MONITORING AND ALARM

Network Protection Safeguards

Suitable network protection and detection systems, based on network criticality analysis should be provided for inter network communication. Following controls should be provided:

1. Management of identities and credentials of network users, including M2M networks
2. Enhanced authentication control, or restricted privileges, for remote access or from access points of the lower level of security
3. Physical access control to network access points
4. Pervasive implementation of Least Privilege Policy
5. Encryption for data at rest (stored) and data in transit (exchanged)
6. Integrity checks for data at rest and data in transit
7. Separation of networks, firewalling, De-Militarized Zones (DMZs), etc.
8. Separation of networks supporting IT systems (e.g. for administrative tasks, passenger and crew connectivity, etc.), OT systems (e.g. for engine control, cargo control, etc.) and alarm systems
9. Event logging and Quality of Service (Quos)
10. Use of routing technology for ship to shore and ship to ship communication, where considered necessary through risk assessment, separation of CAT I, CAT II, CATIII systems networks should be implemented.
11. Where considered necessary through risk assessment additional layers of controls should be provided. (A defence in depth approach)

Cyber incident detection safeguards

A document containing description of the safeguards and instructions on how to verify their effective implementation, or a rationale for those not implemented is to be developed. Controls should be based on risk assessment of a particular network and appropriate safeguards should be identified to suit a particular system

As most of the existing available detection methods are specific to IT system or specific to few communication protocols, implementation of various detection methods given below for OT systems should be implemented as per equipment manufacturer recommendations.

1. Intrusion Detection System (IDS) and Intrusion Protection System (IPS)
2. Connection quality monitoring tools
3. Event log auditing tools and procedures
4. Timely incident alert systems
5. Network Performance Monitoring System
6. Malicious code detection tools, e.g. antivirus, antimalware
7. Collection of all the events detected by the above listed systems, tools- from a) to g) - with dedicated network facility
8. Displaying of security events, e.g. Security Information Event Monitoring (SIEM)

Network and system Recovery Measures

Appropriate recovery measures for networks affected due to a cyber event should be developed by the supplier and/or system integrator as per industry standard practices. Critical systems should have the capability to support back-up and restore in a timely, complete and safe manner.

Following measures to restore network capabilities or service that has been impaired due to a cyber incident should be provided:

1. Redundancy or backup measure of data, network devices and communication media
2. Controlled shutdown, reset and restart of affected systems

Protection devices

Firewalls

1. Internal firewall should be applied between each network segment.
2. Perimeter Firewall between onboard network and external network should be applied.
3. If safety of life or safety of ship is dependent on communication between network segments through a firewalling system, then two different firewalls should be provided and both the firewalls should operate in real time. They should be arranged such that in case of failure of one of the firewall units or cyber incidents, the second unit can maintain the full security of the Ship's network.
4. Firewall should be applied for network between onboard computer systems of Category II or Category III. 5) The firewall rules should be designed to allow passage of data traffic that is essential for the intended operation of that network. To prevent any unintended communication taking place, the last rule of the firewall should be configured to deny all communication.

Routers and protocols

1. Each segment should have its own range of Internet Protocol (IP) address.
2. Protocols should be encrypted. Data transfer from systems for Category II and III through networks should be properly encrypted in the software.
3. Spanning Tree Protocol or similar should be applied to network switches.

Anti-virus Where practicable Anti-virus software should be installed on each onboard computer based system or any programmable device having a standard operating system. The Anti-virus software should not affect performance of Category II and III systems.

For PLCs or other equipment without standard operating system, security measures should be applied in accordance with manufacturer recommendations. Anti-virus should include the following prevention:

1. anti-virus signature database
2. file pattern
3. file size
4. file type
5. grayware
6. heuristics
7. Virus scan. Means to identify the status of anti-virus database should be provided on each onboard computer.
8. updates and procedure for update of anti-virus software should be documented

Advanced Security Measures

Following advanced security measures as applicable should be implemented on board (especially where IT system is integrated with OT systems) and should be based on risk analysis specific to an installation.

1. Virtual private network (VPN) should be deployed into the network. VPN protocols should encrypt traffic going from sender to receiver.
2. Intrusion prevention system (IPS) should be deployed into the network. IPS should issue an alarm in case of starting to record events that may affect security. It should also block unwanted traffic.
3. Alarm from IPS should be generated at the relevant and centralized station which is normally considered to be manned.
4. IPS should contain predefined signatures (database of attack signatures), custom signature entries, out-of-band mode, packet logging.
5. Data loss prevention (DLP) software should be implemented to prevent "leakage" of important data.
6. Content filtering technology module should be installed. This device should block traffic to and from a network by IP address, domain name/URL and type of content.
7. Anti-spam filtering should be applied.

DATA QUALITY

Data security

The general objective of Data Security is to ensure the confidentiality, integrity and availability of Data. Depending upon the intended use of the data, these may take a different order of priority. For example, OT systems transmitting safety critical data will prioritize availability and then integrity.

The three terms can be broadly defined as below.

1. CONFIDENTIALITY – a loss of confidentiality is the unauthorized disclosure of information.
2. INTEGRITY – a loss of integrity is the unauthorized modification or destruction of information.
3. AVAILABILITY – a loss of availability is the disruption of access to, or use of an information system

The scope of application of Data Assurance covers data whose lifecycle is entirely within on board computer based system, as well as data exchanged with shore systems connected to the on board networks. While the consequences of un-authorized modification, data corruption or data loss may differ between IT systems data (typically operational data with a business impact) and OT systems data (may include set points for machinery control and safety with a safety or environmental impact), where data transfers and updates are implemented using a network, these data security objectives share common features and should be considered for the system as a whole.

Data Categorization

- Data categorization document identifying the risks for various categories of data should be developed
- Data should be categorized by the supplier or system integrator according to the possible consequences of a breach of data assurance on the three security objectives. Security Objectives are defined as follows:

The potential impact of loss of data assurance should be categorized as follows:

1. LOW: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on human safety, safety of the vessel and / or threat to the environment.
2. MODERATE: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on human safety, safety of the vessel and / or threat to the environment.
3. HIGH: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on human safety, safety of the vessel and / or threat to the environment.

The following table shows how to assign system with categories based on their effects on system confidentiality, integrity, and availability.

Category	Effects	System functionality	Confidentiality	Integrity	Availability
I	Those systems, failure of which will not lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	Monitoring function for informational / administrative tasks	Low	Moderate	Low
II	Those systems, failure of	Alarm and monitoring	Moderate	High	Moderate

	which could eventually lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	functions Control functions which are necessary to maintain the ship in its normal operational and habitable conditions			
III	Those systems, failure of which could immediately lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	Control functions for maintaining the vessel's propulsion and steering Safety functions	Moderate	High	High

Table 3

The following systems typically belong to Category III, the exact category being dependent on the risk assessment for all operational scenarios:

- Propulsion system of a ship, meaning the means to generate and control mechanical thrust in order to move the ship (devices used only during maneuvering are not in the scope of this requirement such as bow tunnel thrusters)
- Steering system control system - Electric power system (including power management system)
- Ship safety systems covering fire detection and fighting, flooding detection and fighting, internal communication systems involved in evacuation phases, ship systems involved in operation of life saving appliances equipment
- Dynamic positioning system of equipment classes 2 and 3 according to IMO MSC/Circ.645
- Drilling systems

The following systems typically belong to Category II, the exact category being dependent on the risk assessment for all operational scenarios:

- Liquid cargo transfer control system
- Bilge level detection and associated control of pumps Fuel oil treatment system
- Ballast transfer valve remote control system
- Stabilization and ride control systems
- Alarm and monitoring systems for propulsion systems

The example systems are not exhaustive.

ISO 27001

First, it is important to note that the full name of ISO 27001 is "ISO/IEC 27001 – Information technology — Security techniques — Information security management systems — Requirements."

It is the leading international standard focused on information security, published by the International Organization for Standardization (ISO), in partnership with the International Electrotechnical Commission (IEC). Both are leading international organizations that develop international standards.

ISO 27001 is part of a set of standards developed to handle information security: the ISO/IEC 27000 series.

ISO framework is a combination of policies and processes for organizations to use. ISO 27001 provides a framework to help organizations, of any size or any industry, to protect their information in a systematic and cost-effective way, through the adoption of an Information Security Management System (ISMS).

Not only does the standard provide companies with the necessary know-how for protecting their most valuable information, but a company can also get certified against ISO 27001 and, in this way, prove to its customers and partners that it safeguards their data.

Individuals can also get ISO 27001-certified by attending a course and passing the exam and, in this way, prove their skills to potential employers.

Because it is an international standard, ISO 27001 is easily recognized all around the world, increasing business opportunities for organizations and professionals.

The basic goal of ISO 27001 is to protect three aspects of information:

1. Confidentiality: only the authorized persons have the right to access information.
2. Integrity: only the authorized persons can change the information.
3. Availability: the information must be accessible to authorized persons whenever it is needed.

An Information Security Management System (ISMS) is a set of rules that a company needs to establish in order to:

- identify stakeholders and their expectations of the company in terms of information security;
- identify which risks exist for the information;
- define controls (safeguards) and other mitigation methods to meet the identified expectations and handle risks;
- set clear objectives on what needs to be achieved with information security;
- implement all the controls and other risk treatment methods;
- continuously measure if the implemented controls perform as expected; and
- make continuous improvement to make the whole ISMS work better.

This set of rules can be written down in the form of policies, procedures, and other types of documents, or it can be in the form of established processes and technologies that are not documented. ISO 27001 defines which documents are required, i.e., which must exist at a minimum.

There are four essential business benefits that a company can achieve with the implementation of this information security standard:

1. Comply with legal requirements – there is an ever-increasing number of laws, regulations, and contractual requirements related to information security, and the good news is that most of them can be resolved by implementing ISO 27001 – this standard gives you the perfect methodology to comply with them all.
2. Achieve competitive advantage – if your company gets certified and your competitors do not, you may have an advantage over them in the eyes of those customers who are sensitive about keeping their information safe.
3. Lower costs – the main philosophy of ISO 27001 is to prevent security incidents from happening – and every incident, large or small, costs money. Therefore, by preventing them, your company will save quite a lot of money. And the best thing of all – investment in ISO 27001 is far smaller than the cost savings you'll achieve.
4. Better organization – typically, fast-growing companies don't have the time to stop and define their processes and procedures – as a consequence, very often the employees do not know what needs to be done, when, and by whom. Implementation of ISO 27001 helps resolve such situations, because it encourages companies to write down their main processes (even those that are not security-related), enabling them to reduce lost time by their employees.

There are 14 "domains" listed in Annex A of ISO 27001, organized in sections A.5 to A.18. The sections cover the following:

1. A.5. Information security policies: The controls in this section describe how to handle information security policies.
2. A.6. Organization of information security: The controls in this section provide the basic framework for the implementation and operation of information security by defining its internal organization (e.g., roles, responsibilities, etc.), and through the organizational aspects of information security, like project management, use of mobile devices, and teleworking.
3. A.7. Human resource security: The controls in this section ensure that people who are under the organization's control are hired, trained, and managed in a secure way; also, the principles of disciplinary action and terminating the agreements are addressed.
4. A.8. Asset management: The controls in this section ensure that information security assets (e.g., information, processing devices, storage devices, etc.) are identified, that responsibilities for their security are designated, and that people know how to handle them according to predefined classification levels.
5. A.9. Access control: The controls in this section limit access to information and information assets according to real business needs. The controls are for both physical and logical access.
6. A.10. Cryptography: The controls in this section provide the basis for proper use of encryption solutions to protect the confidentiality, authenticity, and/or integrity of information.
7. A.11. Physical and environmental security: The controls in this section prevent unauthorized access to physical areas, and protect equipment and facilities from being compromised by human or natural intervention.
8. A.12. Operations security: The controls in this section ensure that the IT systems, including operating systems and software, are secure and protected against data loss. Additionally, controls in this section require the means to record events and generate evidence, periodic verification of vulnerabilities, and make precautions to prevent audit activities from affecting operations.
9. A.13. Communications security: The controls in this section protect the network infrastructure and

services, as well as the information that travels through them.

10. A.14. System acquisition, development and maintenance: The controls in this section ensure that information security is taken into account when purchasing new information systems or upgrading the existing ones.
11. A.15. Supplier relationships: The controls in this section ensure that outsourced activities performed by suppliers and partners also use appropriate information security controls, and they describe how to monitor third-party security performance.
12. A.16. Information security incident management: The controls in this section provide a framework to ensure the proper communication and handling of security events and incidents, so that they can be resolved in a timely manner; they also define how to preserve evidence, as well as how to learn from incidents to prevent their recurrence.
13. A.17. Information security aspects of business continuity management: The controls in this section ensure the continuity of information security management during disruptions, and the availability of information systems.
14. A.18. Compliance: The controls in this section provide a framework to prevent legal, statutory, regulatory, and contractual breaches, and audit whether information security is implemented and is effective according to the defined policies, procedures, and requirements of the ISO 27001 standard.

A closer look at these domains shows us that managing information security is not only about IT security (i.e., firewalls, anti-virus, etc.), but also about managing processes, legal protection, managing human resources, physical protection, etc.

Public and private organizations can define compliance with ISO 27001 as a legal requirement in their contracts and service agreements with their providers. Further, as mentioned above, countries can define laws or regulations turning the adoption of ISO 27001 into a legal requirement to be fulfilled by the organizations operating in their territory.

BIBLIOGRAPHY

1. The Guidelines on Cyber Security onboard Ships, Version 2.0 [BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI]
2. Code of Practice – Cyber Security for Ships [The Institute of Engineering and Technology]
3. MSC-FAL.1-Circ.3 - Guidelines on Maritime Cyber Risk Management [International Maritime Organization]
4. MSC-FAL.1/Circ.3/Rev.1- Guidelines on Maritime Cyber Risk Management [International Maritime Organization]
5. Consolidated IACS Recommendation on cyber resilience (Rec 166). April 2020
6. ISO Website (www.iso.org)