DBS
DROMON BUREAU OF SHIPPING

clever solutions | beyond class

TECHNICAL PUBLICATION

Guidelines on Maritime Cyber Risk Management

Practices for implementation

OCTOBER 2018

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.

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.

BASIC TERMS

Access control is selective limiting of the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions.

Back door is a secret method of bypassing normal authentication and verification when accessing a system. A back door is sometimes created 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.

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 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.

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.

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.

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.]

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.

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.]

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.

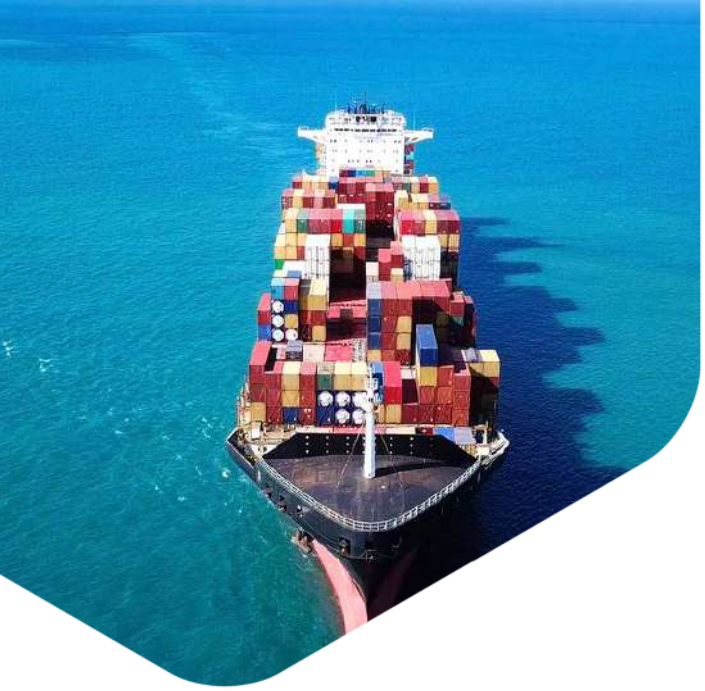
Sandbox is an isolated environment, in which a program may be executed without affecting the underlying system (computer or operating system) and any other applications. A sandbox is often used when executing untrusted software.

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

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.



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. 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).

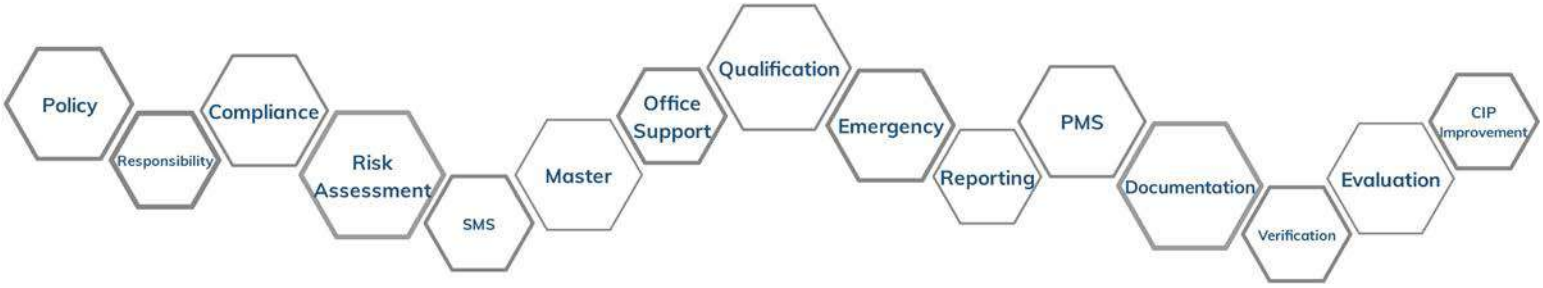
Reference should be made to the most current version of any guidance or standards utilized.

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 safe guards 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 safe guards

   A non-exhaustive list of all potential safe guards (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 safe guards 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

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.

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 safe guards is inadequate. Henceforth, RA and SMS should be updated to sustain a continuous improvement process.

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]