GUIDANCE NOTES
GD26-2019

CHINA CLASSIFICATION SOCIETY

Guidelines on Maritime Cyber Risk Assessment and Cyber Safety Management System

(2019)

Effective date: February 1, 2020

Beijing

Contents

Foreword

In response to cyber risks to ship safety and pollution prevention, the IMO Maritime Safety Committee approved the “Interim Guidelines on Maritime Cyber Risk Management” (MSC.1/Circ.1526) at its 96th Session, and the “Guidelines on Maritime Cyber Risk Management” (MSC-FAL.1/Circ.3) at its 98th Session to replace the “Interim Guidelines” (MSC.1/Circ.1526).

According to the resolution “Maritime Cyber Risk Management in Safety Management Systems” (MSC.428(98)) adopted at the 98th Session, cyber risk management needs to be taken into account in the safety management system. At the same time, the IMO encourages governments to examine whether the safety management system includes relevant contents of cyber risk management during the first annual DOC audit that is performed no later than January 1, 2021.

This guide describes the methods of maritime cyber risk assessment and proposes suggestions on the formulation, implementation and improvement of management systems, so that maritime cyber risks are fully recognized and emphasized in the industry and cyber risk management can be incorporated into the safety management system as soon as possible.

I. General

1.1 Background

With the rapid development of computer technology, the Internet has become an important guarantee and necessary tool for social and economic development. In the shipping industry, achievements in digitalization, integration, automation and networking have greatly promoted the interconnection of shipping systems via the Internet. The increasing popularity of satellite communication also has made networks onboard connected to the networks of companies and other interested parties more frequently.

While the Internet improves convenience and efficiency in the shipping industry, it also brings about cyber threats which may expose ships to malicious or unintentional accesses or attacks. Therefore, necessary measures should be taken in the shipping industry to protect all assets and reduce or avoid adverse impacts on the safety, environment, and business.

In terms of development trends, secure and efficient networks are required to guarantee the normal operation of ships and sustainable development of the shipping industry with the development of automated terminals, intelligent ships and unmanned ships.

Cyber threats are constantly changing and developing with the development of network technologies. In addition, the mobile terminals and media widely applied by personal may bring unpredictable security risks. Accordingly, cyber risks should be managed based on the known threats, and unknown threats should be taken into consideration as much as possible.

As it is reported:

- In 2011, an oil tanker from the Arabian Gulf to the Mediterranean was targeted and hijacked by pirates, with its information (e.g. schedule, goods, crew, location and armed forces) obtained in advance by the technicians hired by the pirates.
- In 2011 and 2013, the IT system of a European port was subjected to cyber attacks, then cargo data was tampered, making a goods smuggling plan executed successfully.
- In 2014, a fuel supplier paid a fine of approximately $ 18 million due to the alleged involvement of a cyber attack, charged by an insurance company.
- In 2015, London P&I Club announced that the number of cycle frauds related to ships was increasing, including the interception of mails from ship agents and intrusion to e-mail accounts, for replacement of original payment accounts with new ones, etc.

- In 2016, statistics from relevant agencies showed that the top three risks of unmanned ships were navigation risks, cyber security and loss of communication.
- In 2017, Petya's network virus spread around the world, resulting in the failure of IT systems of well-known shipping companies in global offices and business units, with the reported losses up to hundreds of millions of dollars.
- In 2018, MARAD issued a navigation warning, stating that the GPS of about 20 ships in the Black Sea encountered a strange and mischievous "interference", resulting in inaccurate position display, loss and the like.
- In the same year, the US regional website of COSCO Shipping Lines Co., Ltd., a global container shipping giant, was subject to a cyber attack. It was reported that its US regional website was attacked by ransomware.

Cycle security issues have undermined the normal operation of the shipping industry and gradually become a focus of the industry. In order to avoid and reduce risks and fulfill the recommendations of the IMO Maritime Safety Committee, all parties concerned shall carry out maritime cyber risk assessment and management as soon as possible, so that the maritime cyber security management system works properly.

1.2 Purpose

This guideline were compiled according to the "Guidelines on Maritime Cyber Risk Management" (MSC-FAL.1/Circ.3) approved by the IMO Maritime Safety Committee at its 98th Session, and can be used as a guide for the industry to execute the resolution "Maritime Cyber Risk Management in Safety Management Systems" (MSC.428(98)) of the 98th Session.

Through introducing the fundamentals of maritime networks, this document provides an approach of maritime network risk assessment, suggestions on the development, execution and improvement of the maritime cyber management system, and comprehensive, effective and executable guidelines for the industry, as a reference for decision maked based on actual situations, thus preventing or reducing cyber threats to ships at present and in the future.

Maritime cyber risk management is a process for ship owners, management companies and ships to control cyber risks to a reasonable level by formulating and implementing measures and plans for avoidance, transfer, reduction or tolerance. A simple approach may be adopted within a limited network. For a broad network and complex system, a comprehensive solution shall be adopted, and efforts shall be made to seek the support of the industry, competent authorities and partners.

Maritime cyber risk management is to maximize the normal operation for safe shipping. Thus, the measures and plans for maritime cyber risk management shall involve as much buffer spaces and margins as possible to avoid cyber security incidents. At the same time, efforts shall be made to protect the safety of assets and personnel, also to prevent marine pollution even in the case of cyber security incidents.

1.3 Scope of application

The scope of application of this guideline is consistent with that of the "International Safety Management (ISM) Code". In terms of maritime networks, this guideline is applicable to ship safety management in onboard networks and corporate network.

If a ship (especially a highly networked ship) may be remotely hijacked in a cyber attack, the requirements of the "International Ship and Port Facility Security (ISPS) Code" shall be conformed during cyber risk management.

In accordance with the resolution "Maritime Cyber Risk Management in Safety Management Systems" (MSC.428(98)) of its 98th Session, the IMO encourages implement maritime cyber risk management no later than the first annual DOC audit carried out after January 1, 2021.

From the perspective of operational practice, it is recommended to implement maritime cyber risk management no later than the first temporary DOC audit, initial audit, annual audit or renewal audit carried out after January 1, 2021.

Relevant provisions of this document may be referenced where the "International Safety Management (ISM) Rules" are not applicable. All organizations in the shipping industry are also expected to carry out cyber risk management in accordance with this document.

The guideline herein are recommended only.

1.4 Basic principles

For efficient implementation of measures and plans, maritime cyber risk management shall involve all personnel from senior management to crew members or employees. Senior management should embed a culture of cyber risk awareness into all levels of the company by taking various actions, and through an efficient feedback system, ensure that cyber risk management is performed continuously and assessed regularly, thus developing a comprehensive, efficient, flexible and operable management system. In addition, senior management shall allocate sufficient manpower and necessary funds for the development and implementation of the maritime cyber risk management system.

In order to be implemented efficiently, the maritime cyber risk management system should be developed based on the actual cyber conditions of the company and ship. In this sense, cyber conditions should be surveyed before the documents for the maritime cyber risk management system are prepared; cyber risks shall be assessed based on survey results; appropriate measures shall be developed against the risks identified in assessment, and resources shall be utilized efficiently and reasonably to solve problems; and measures of cyber risk management shall be ultimately incorporated into the security management system.

To guarantee the effectiveness, all parties concerned shall fully consider the requirements of flag states as well as relevant international standards, industry standards and best practices during specific operations.

Maritime cyber risk management as an integral part shall be coordinated with the safety management system. Sensitive or confidential business data involved in cyber risk management shall be protected and particularly prevented from being mentioned in safety management system documents. Meanwhile, attention shall be paid to the mandatory requirements of "ship security assessment" in Chapter 8 of Part A of the ISPS Code, and non-mandatory requirements of "radio and wireless communication systems including computer systems and networks" in Paragraph 8.4.11 of Part B of the ISPS Code.

1.5 Three stages of system establishment

It is recommended to establish a system at three stages in this document, the details as followings.

Stage 1 **Risk assessment**	**Stage 2** **System** establishment	**Stage 3** **System performance**
(1) Maritime cyber survey	**(1) Measurement institution**	**(1) System institution**
Identify and familiarize with the scope and characteristics of maritime cyber connections.	Avoid and reduce the occurrence and harm of risks.	Incorporate measures, plans, responses and recovery into the system.
(2) Risk identification	**(2) Emergency plan**	**(2) System implementation**
Identify the risks arising from maritime cyber use.	Reduce hazards caused by cyber incidents.	Implement the system and keep relevant records after release.
(3) Risk assessment	**(3) Response and recovery**	**(3) System improvement**
Quantitatively evaluate the identified risks.	Have efficient capabilities on response and recovery after a cyber incident.	Improve the system according to the industry information, feedback, risks, etc.

II. Maritime Network and Its Risks

2.1 Maritime network

With the extensive application of computer technologies in the shipping industry, modern ships are increasingly information-based and automated. For better sharing, storage and use of ship data, more and more ship electronic/IT systems are connected through networks, in which a number of modules or systems are connected to the Internet through satellite, WIFI or 4G techniques.

Generally, maritime networks can be divided into two categories: (1) network for information collection and information management service, such as reporting, dispatching, inventory management, operation and maintenance management, emails, phone calls, printing services and ship-shore communication systems, usually known as the information technology network (IT network), consisting of computers, gateways, routers, file servers, database servers, application servers and others used by crew members; (2) network for collecting, monitoring and controlling the operating statuses of ship equipment and serving the ship control system, known as the control network (OT network), such as the main propulsion monitoring system, auxiliary machine monitoring system, electric power station monitoring system and fire alarm system in the engine room, the navigation system and integrated bridge system on the bridge. The schematic diagram of the network system onboard is as followings.

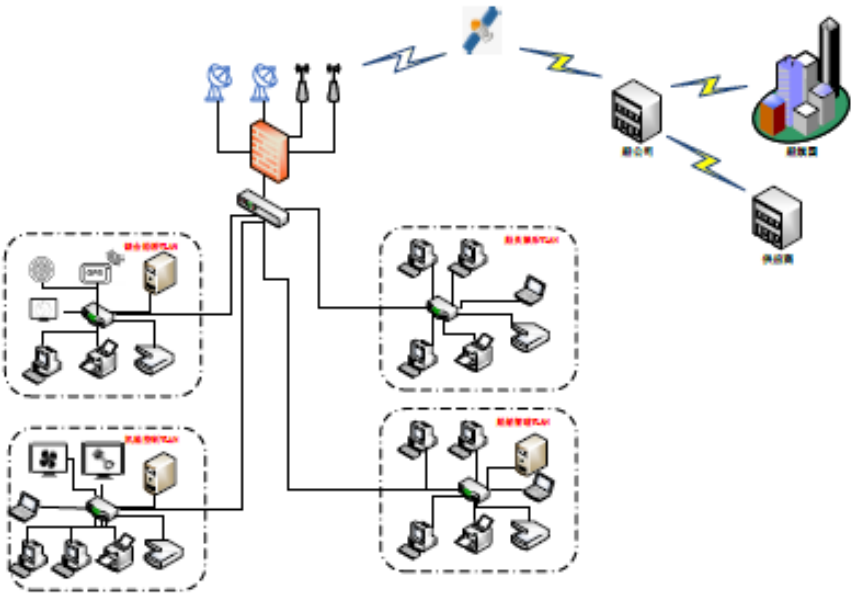

Figure 2.1 Schematic Diagram of Onboard network System

2.2 Cyber risk

As network technologies are widely applied in the shipping industry, the network onboard plays an increasingly important role in key systems for ship safety and pollution prevention. However, this brings about cyber risks due to incorrect operations, software defects, intrusion of unauthorized systems, management companies taking ineffective risk control procedures, and the like. Survey results show that the systems of smart ships vulnerable to cyber risks include the bridge systems, cargo operation and management systems, propulsion and machinery management and power control systems, access control systems, passenger servicing and management systems, passenger public network management and crew protection systems, communication systems, etc.

In the past, it was difficult to update systems onboard in a timely manner, but these systems were usually isolated, and the network onboard was often offline since the ship had been offshore for a long time, thus reducing the exposure to and suffering from remote attacks. In addition, modern ships are equipped with embedded systems, even outdated and unsupported components, high network speeds bring about risks due to their own particularities, in spite of convenience in system updating.

The security awareness of the crew has a decisive influence on the security of the network onboard. Crew members may use a virus-infected USB device, which will infect the PC and onboard network, once be inserted into an onboard PC. The biggest challenge to network system onboard is the access to the Internet, while the most important problem is to update the OT system and applications. If users do not connect the Internet with their own accounts, no computer can maintain uninterrupted access to the Internet.

As satellite broadband data rates are increased, the competitiveness of onboard networks are enhanced and thus naturally become more similar to onshore “branches”. Also, the inexpensive access to networks has changed almost shipping operations and every aspect of daily life. The relative security of this critical system is therefore negatively affected. Although the threat of USB-borne malware is currently a major concern, expansion of the access to networks will bring new threats, so mature business processes are required to manage them. Vulnerability management, especially the system used for determining the status of network by scanning, could be an effective way against cyber security risks. This should be completed before network systems onboard are connected to the public Internet and other ashore networks.

In some cases, legacy systems onboard cannot work properly without old or fragile Web browsers and Java clients, which occur rarely with ashore infrastructure, this can be changed with the extensive application of the Internet for ships. When it is necessary to use outdated or unsupported software components, compensation controls should be designed and deployed against risks. For example, if it is absolutely necessary to use an older version of browser, a host-based firewall can be applied to restrict communication to the terminals of applications. Then the latest browser can then be used to access the generic Internet. Such a compensation for control is not ideal, but what is important is to understand that security measures often have a negative impact on the availability. Considerations should be given to an appropriate balance of risk management while maintaining the availability, so tests and errors may be involved under some circumstances.

III. Maritime Cyber Risk Assessment

3.1 Basic principles

The process and results of maritime cyber risk assessment are important bases for establishing a maritime cyber risk management system. The assessment process should at least include: maritime network survey, risk identification and risk assessment.

Maritime cyber risk assessment will not only enhance the cyber risk awareness of participants, but also help to identify risks in a deeper and more extensive manner.

The result of maritime cyber risk assessment is a basis for formulating security management measures. In this sense, risk assessment should be supported at all levels and by all departments of the company.

Concerning the expertise and rapid development of network technologies, it is recommended in this document that at least one participant in the assessment has sufficient computer and network knowledge.

An effective supplement to corporate self-assessment of maritime cyber risks is to engage a third party. The third party can help to determine more potential risks through in-depth identification.

3.2 Maritime network survey

Surveying the scope and characteristics of maritime networks is the starting point for risk identification and also the process of recognizing and familiarizing maritime networks. All factors related to network connection should be noted during the survey, including systems, assets, data, functions, ports, permissions, and personnel, etc. Necessary records should be made during the survey to facilitate the follow-up work and the improvement after implementation.

Maritime networks can be surveyed by means of reviewing drawings, crew self-examination, field inspection, service provider inspection, etc. Depending on the complexity and similarity of networks, the company may survey maritime networks in one way or a combination of multiple ways.

3.2.1 Example of maritime network survey

Maritime networks should be fully surveyed, and survey results should be as complete and accurate as possible. In order to facilitate understanding and reference by all parties, for ships with simple maritime networks, it is recommended in this document to survey in the following aspects:

1. No need for access to networks and no office computers;
2. No need for access to networks but with office computers;
3. Need of ship equipment for network access;
4. Need of office computers for network access;
5. Network access need of crew members for entertainment;
6. Network access need of passengers for entertainment.

As recommended in this document, ships involving complex networks should be surveyed from the perspectives of network construction and needs, and attention should be paid to the following aspects:

1. Company requirements for networks access;
2. Devices (e.g. navigation equipment, CCTV, mailbox services, and crew entertainment) using the network according to the supply contract signed between the company and network service provider (usually radio survey service provider);
3. Services purchased by the network service provider from the network service vendor, and supporting equipments (antenna, modem, and router) provided by the network service provider;
4. Purchase of switches and firewalls by the network service provider, network configuration and security configuration according to the supply contract, and restriction of network access within the contract range based on the compliance with network needs;
5. Access of terminals to networks, which should be connected to switches behind the firewall. But routers for read-only data (e.g. CCTV) can be directly connected;
6. On the ship, installation of anti-virus software may be carried out through networks.

3.3 Risk identification

Maritime cyber risks generally refer to the acts or data that do potential harm to personnel, pollution prevention and assets. They may be caused by improper operation, unreasonable integration, untimely maintenance, nonconforming operation and unreasonable network design, or intentional or unintentional cyber attacks.

The emergency of risks will expose loopholes and deficiencies, so it is necessary to identify risks to find and improve weak links and reduce risks at least to an acceptable level.

In addition to generic items, risks of special equipment or systems of ships should be identified during cyber risk identification.

It is recommended to classify maritime cyber risks in order to facilitate identification.

The systems used can be divided as follows: IT system, OT system, data, and transmission. The IT system is for information in data use. The OT system is to control or monitor physical activities in data use. The data in computer science refers to all kinds of media that can be inputted into computers and processed by programs. Data transmission involved in this document includes network transmission, mobile media transmission and special interface transmission.

The measures to be taken can be divided as follows: external protection and internal protection. External protection focuses on preventing unauthorized access, being controlled or destroyed, while internal protection focuses on remedy related to the availability and integrity of critical data and OT systems. More vividly, external protection is to actively restrict hazard sources to the outside, while internal protection is to passively take measures to restore the original capabilities of the protected object. Internal protection incidents may be caused by external protection incidents, errors in software maintenance and upgrading, and loss, control or counterfeiting of external data required in operation.

3.3.1 Threat

Through network interconnection, some organizations or individuals unauthorized for access to a network may intentionally or unintentionally affect the normal operation of the network from the outside, thereby causing foreseen or unforeseen hazards.

Potential hazards are as follows:

- Dangerous organizations or individuals (including dissatisfied employees) may destroy data, disclose sensitive data, attract media attention and hinder the normal use of services and systems, aiming to tarnish the reputation of related parties or interrupting daily operations;
- Criminals may, in terms of economic benefits or commercial or industry competitions, sell the stolen data, extort the availability of the redeemed data or systems, counterfeit cargo transportation information, and collect information for criminal purposes;
- Speculators may break network protection and economic benefits to prove their personal abilities or for extortion purposes;
- Ambitious governments, government-funded agencies and terrorists may obtain information, wreck the economy and destroy important facilities for political interests or espionage purposes.

These are always performed in networks, and the personnel involved have adequate skills and resources to significantly threaten the safety of assets and daily operations of companies.

Both ashore and onboard personnel may do harm to network systems and data. Companies should be prepared against operation errors or noncompliance with security measures during operation and management of IT and OT systems. Surely, this may be caused deliberately by those dissatisfied.

The acts endangering the normal use of networks in this document refer to the cyber attacks, which can be divided as follows:

- Random attacks: systems and data of a company or ship are part of potential targets;
- Specific attacks: systems and data of a company or ship are the selected targets.

Random attacks are performed by tools and technical means available on the Interne, in which attackers locate, discover and use widespread weaknesses. The weak link of a company or ship, which happens to be consistent with the target, will be attacked. Examples of such attacks are as follows:

- Malware;
- Social engineering;
- Phishing;
- Fake websites;
- Random scan.

In specific attacks, attackers are skilled in using specific tools and technical means aiming at a company or ship. Examples of such attacks are as follows:

- Storm algorithm (method of exhaustion);
- Denial of services;
- Spear phishing;
- Disruption of the supply chain.

Users and managers of maritime networks should be aware that the above attacks are active and efficient management should be performed to identify cyber attacks as early as possible, mitigate network attacks, and reduce the hazards caused by attacks.

3.3.2 Vulnerability

The network vulnerability refers to the weak link and improper operations of components, IT systems, OT systems, data, and transmission within a network. A non-networked, isolated system involves fewer risks, but may be subjected to risks due to the component reliability, software upgrade, use of removable media, and improper operation.

Examples of network systems used by ships are as follows:

- Bridge system;
- Propulsion, power and equipment management;
- Cargo management system;
- Access control system;
- Passenger service and management system;
- Passenger entertainment system;
- Ship and crew management system;
- Internet service.

The network systems for ship-shore connection are as follows:

- Diesel engine performance monitoring;
- Navigation performance monitoring;
- Reporting of navigation data;
- Maintenance and spare part management;
- Cargo, crane and cargo pump management;
- CCTV system.

Due to the diversity of network systems, the aforesaid two kinds of examples are for reference only. The parties concerned should comprehensively identify components and systems by examining the structures of onboard network systems and identifying ship-shore contact interfaces. To this end, more attention should be paid to new technologies and equipment, as new technologies and equipment may bring more unknown risks due to the lack of experience in use.

The vulnerability of network systems is usually caused by the following reasons:

- Obsolete and unsupported OT systems;
- Expiration or absence of antivirus and anti-malware software;
- Inadequate security measures and improper implementation;
- Lack of border protection measures and separation of networks;
- Constant connection of critical equipment or systems to the shore;
- Lack of access control measures for partners.

The network security of the service provider should be taken into account. It is recommended for the service provider to check the network security awareness and management, and carry out assessment based on the services it provider, especially when the service provider is directly connected to the ship or company through a network.

3.4 Risk assessment

3.4.1 Quantification of risk assessment

Risk assessment in this document refers to the quantitative assessment of identified risks with regard to the possibilities and hazards of potential negative impacts and losses.

The probability and hazard of a risk, which determines its severity, should be graded or scored first, and the risk level and score should be given based on the grades or scores of these two items. The risk at a high level has high probability and great hazards, while that at a medium or low level has low probability and insignificant hazards. Refer to Figure 3.4.1-1 for the occurrence of a small number of risks and Figure 3.4.1-2 for the occurrence of a large number of risks.

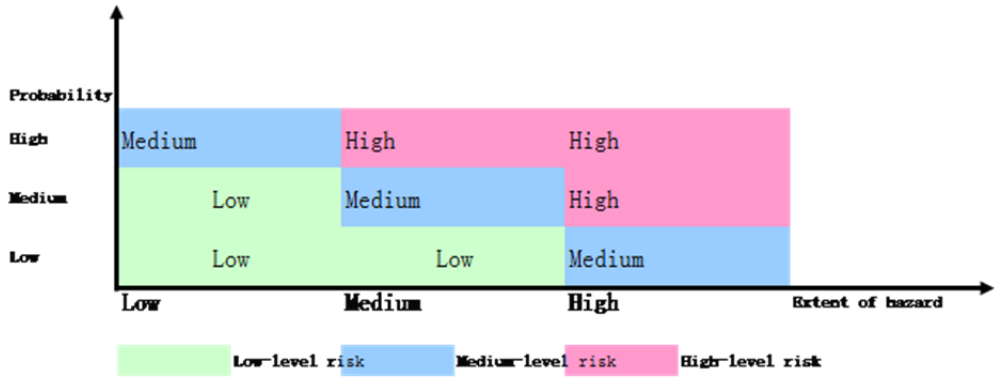

Figure 3.4.1-1 Risk Levels in the Case of a Small Number of Risks

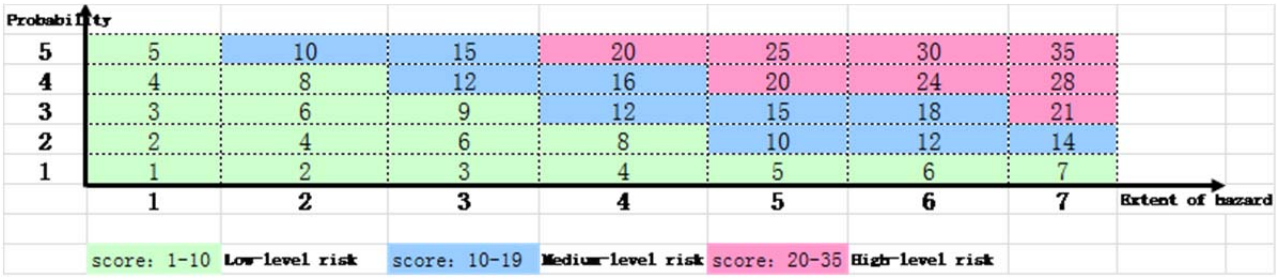

Figure 3.4.1-2 Risk Levels in the Case of a Large Number of Risks

It should be noted that, for high-level risks, measures should be taken immediately for downgrading to medium- or low-level risks; for medium-level risks, security measures and investment should be improved as much as possible; and for low-level risks, necessary security measures need to be developed.

3.4.1.1 Risk probability

The risk probability should be assessed based on the experience and risk development trend. In addition, the results favoring safety should be adopted if possible.

Where the network system is maintained and managed fully or partly by a partner, and the shipping company cannot assess the performance of the partner, the partner should submit an assessment report for review. In this case, the company's cyber risk management system should properly incorporate the partner's cyber risk management.

The probability of cyber risks is affected by the network status, environment and user. When the risk probability is analyzed, the network status and environment factors should be considered, such as:

- Network control methods used on board;
- Data exchange of network connection: two-way (uplink and downlink) and one-way (uplink or downlink);
- Confusion about duties due to participation of interested parties in ship operations, and inadequate investment in hardware;
- Network interfaces between ships and related parties in global supply chains;
- Remote monitoring interface of equipment;
- Sensitive information shared with ashore partners;
- Computer systems in critical equipment for ship safety control and pollution prevention;
- Removable media used by technicians, suppliers, port officials, terminal representatives, agents, pilots, etc.;
- Allowable access of personal devices to ship systems or networks;
- Third-party software (e.g. ship management, stability, hull stress, chart update, and CCTV).

3.4.1.2 Risk hazard

The hazards arising from maritime cyber risks should be assessed at least from three aspects: confidentiality, integrity, and availability (CIA model), considering the hazards related to ship operation, asset safety, personal safety and pollution prevention.

- Confidentiality: Illegal connection or disclosure of information and data of ships, crew, cargoes and passengers;
- Integrity: modification or destruction of information and data related to the safety and effectiveness of management and operation;
- Availability: failure in information and data recovery or use of system services and operations.

The importance of the above-mentioned items is related to the purpose of information or data. For example, the assessment of IT systems involving business operations should focus on their confidentiality and integrity, and that of OT systems should focus on the integrity and availability.

3.4.4 Examples of risk assessment

In order to facilitate understanding and reference for all parties, this document provides the following examples of risk assessment of ships with simple networks.

S/N	Risk Source	Hazard	Cause	Probability	Extent of Hazard	Risk Level
1.	Office computer requiring no access to the Internet	Computer failure or data loss, affecting normal operation	Virus	Medium	Medium	Medium
2.	Access of ship equipment to the Internet	Disclosure of ship information, business information and personal information	Trojan and backdoor program	High	Medium	High
3.	Access of ship equipment to the Internet	Modification of equipment parameters, resulting in equipment failure, route deviation, etc.	Malicious attack, Trojan, and backdoor software	Medium	High	High
4.	Access of office computer to the Internet	Disclosure of ship information, business information and personal information	Trojan and backdoor program	High	Medium	High
5.	Access of office computer to the Internet	Computer failure or data loss, affecting normal operation	Virus, Trojan and backdoor program	Medium	Medium	Medium
6.	Internet access of crew for entertainment	Disclosure of personal information, ship photo, and work document	Trojan and backdoor program	Medium	Medium	Medium
7.	Internet access of crew for entertainment	Virus spreading in ship LAN, making other terminals infected with virus	Virus, Trojan and backdoor program	Medium	Medium	Medium
8.	Internet access of passenger for entertainment	Virus spreading in ship LAN, making other terminals infected with virus	Virus, Trojan and backdoor program	High	Medium	High

For the Internet access of ship equipment, it should be noted that hazards caused by cyber risks to IT and OT systems are different and must be assessed separately, with examples are as follows.

S/N	Risk Source	Hazard	Cause	Probability	Extent of Hazard	Risk Level
1.	Internet access of AIS (OT)	AIS data failure, increasing risks of ship stranding or collision	Virus, Trojan and backdoor program	Medium	High	High
2.	Internet access of GPS (OT)	GPS data error, increasing the probability of ship stranding or yawing	Virus, Trojan and backdoor program	Medium	High	High

S/N	Risk Source	Hazard	Cause	Probability	Extent of Hazard	Risk Level
3.	Internet access of maintenance system (IT)	Insufficient maintenance, increasing the probability of equipment failure	Virus, Trojan, backdoor program, and compatibility	Medium	Medium	Medium

3.5 Precautions

3.5.1 Information (IT) system and operating (OT) system

During the identification and assessment of maritime cyber risks of the ship's IT and OT systems, attention should be paid to:

- ✓ Identification of current means of protection;
- ✓ Identification of weak links, personal factors, personal factors, rules of use, software patches, and firewall versions;
- ✓ Identification and assessment of weak links in critical operations of ships;
- ✓ Potential cyber attacks and their effects and probabilities, in order to facilitate the development of measures;
- ✓ Consulting of manufacturers and suppliers for their technical and management measures in cyber security;
- ✓ Immediate solution to network hazards arising from poor design or unreasonable configuration at the manufacturing stage.

Penetration tests of IT and OT system infrastructure can help to determine the compliance of protection levels. Through simulating cyber attacks, they have strong integrity. However, it is recommended to perform these tests to IT systems only. The OT systems may be subjected to passive tests, such as data scanning and transmission, instead of attempt to actively access the OT system or implant software.

3.5.2 Maritime network survey

During the maritime network survey, attention should be paid to the following aspects:

- ➢ Listing of key functions and systems of ships and their hazards to security;
- ➢ Listing of major manufacturers for key equipment in IT and OT systems of ships;

- Consulting of descriptions related to the network architectures, interfaces and connections of IT and OT systems of ships;
- Listing of contact information of manufacturers involved in cyber security, and communication with these manufacturers;
- Consulting of maintenance documents for IT and OT systems of ships;
- Contract requirements and responsibilities of the ship owner and management company in terms of network and equipment maintenance and technical support;
- Evaluation of the need for support of external experts, manufacturers, or service providers.

3.5.3 Risk assessment

Risk sources should be noted during risk assessment:

- Technology: such as software defects, software expiration, and software patches;
- Design: such as access management, and unmanaged network connections;
- Execution: such as configuration of computers, servers, routers and other network equipment;
- Improper measures or other human errors.

3.5.4 Recording and reporting

The quantitative assessment of risks and the security measures developed shall be recorded and reported. The report should include:

- Management summary: delicately summarize the assessment results, relevant recommendations and network security situations;
- Technical findings: to be reported in detail, including the risk source, possibility, degree of hazard, risk level, and corresponding security measures;
- Priority of measures: fully considering the effects, expenses and applicability, list the priorities of the security measures to be taken, excluding the company's services and products evaluated by third parties;
- Process record: detailing all stages, technical findings and weak links, names of the tools and software used, sample data after recovery from penetration test;

- Filing: necessary texts should be filed for reference.

3.5.5 Manufacturer

When required, assistance and collaboration should be sought from the manufacturer for joint improvement.

3.5.6 Partner

The connection between the networks of the partner and company or ship should be identified. If their networks are connected, risk assessment should be carried out through cooperation.

Attention should be paid to whether the use of networks or computers by the staff of the partner. If they are used by the staff of the partner, it is necessary at least to survey whether the partner has taken actions to guarantee the cyber security awareness of its staff.

IV. Maritime Network Management System

4.1 Basic principles

The maritime network management system, as an important part, should be run and improved within the safety management system of the ship or company.

The maritime network management system should have the functions of identification, protection, discovery, response, and recovery. For the reasonable design, conforming construction and normal use of the network, the management system should include the following items according to the set security level and risk assessment results:

- Developing and implementing security measures in daily use;
- Formulating emergency plans to reduce hazards arising from cyber incidents;
- Developing measures to guarantee the response capabilities and normal implementation of emergency plans;
- Formulating recovery plans;
- Investigating cyber incidents.

Security measures are to prevent cyber incidents and guarantee operations. When a cyber incident occurs, even if it causes hazards, the management system can help all parties concerned to respond reasonably and actively, implement contingency plans and recovery plans and maximize the availability of the network.

The development of security measures, assessment of risks and company's efforts for cyber security are to maintain the network at a security level recognized and accepted by everyone through avoiding and reducing risks and their hazards. Accordingly, the security measures developed should focus on the security.

4.2 Maritime network management system and security management system

IMO Resolution MSC.428(98) identifies cyber risks as specific threats, which companies should try to address as far as possible in the same way as any other risk that may affect the safe operation of a ship and protection of the environment. More guidance on how to incorporate cyber risk management into the company's SMS can be found in Annex 1 of these guidelines.

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

When incorporating cyber risk management into the company's SMS, consideration should be given as to whether, in addition to a generic risk assessment of the ships it operates, a particular ship needs a specific risk assessment. The company should consider the need for a specific risk assessment based on whether a particular ship is unique within their fleet. The factors to be considered include but are not limited to the extent to which IT and OT are used on board, the complexity of system integration and the nature of operations.

4.3 Security measures depth and in breadth

Due to the complexity, concealment and potential persistence of cyber risks, attention should be paid to the scope and depth of security measures in terms of risk detection and prevention of key systems and data, in order to improve the survivability and recoverability of systems and related data in maritime networks.

To enhance the depth, measures shall be developed and implemented at various levels to detect and prevent cyber incidents, such as:

- Physical security of the ship in accordance with the ship security plan (SSP);
- Optimization of network architecture, especially effective segmentation;
- Network firewall and antivirus software;
- Network intrusion monitoring tools;
- Software whitelist;
- Access and user controls;
- Password protection;
- Control over the use of removable media;
- Personnel's risk awareness and familiarity with appropriate procedures training.

In order to expand the scope, the comprehensiveness of measures should be emphasized, so that the measures cover all systems that may be attacked, in order to avoid vacuum areas of management.

For ships with a highly integrated network system, technical means and procedures should be applied at various levels in each vulnerable system, to improve the depth of measures and thus avoid using weak links of one system to bypass the protections of other systems. This can meet the requirements for the scope of security measures. That is, weak links of different systems will not affect each other.

The depth and scope of security measures complement each other, which is an important guarantee for the maritime cyber risk management system.

4.4 Security measures

Attention should be paid to the following aspects during the development and implementation of maritime cyber security measures:

- Measures should be consistent with the actual situation of the network, and pertinent, operable and practical;
- Measures should be specific and easy to understand and implement;
- The responsible person has sufficient skills and awareness to perform his duties;
- The responsibilities of the master, responsible crew members and company's responsible person should be specified;
- The responsible person should have sufficient knowledge and skills;
- It should be confirmed whether the onboard network needs to be maintained by the service provider;
- Measures should be programmed, as part of the company's policy, system document and access control;
- The approach leading to the greatest benefits and a combination of approaches should be considered;
- Measured should be classified by priority;
- New ships are equipped with more convenient and effective technical measures than the existing ships available currently;
- Security measures in the network system design and configuration shall effectively improve the security and system flexibility;
- Sometimes there is no control as to who has access to the onboard systems, e.g. during dry docking, lay up or when taking over a new or existing ship. In such cases, it is difficult to know if malicious software has been left in the onboard systems. It is recommended that: (1) sensitive data should be removed from the ship and reinstalled on returning to the ship; (2) where possible, systems should be scanned for malware prior to use; (3) OT systems should be tested to check that they are functioning correctly.

To facilitate the incorporation into the management system, security measures are divided into technical security measures and procedural security measures.

Security measures should be developed according to the results of risk assessment. Annex 2 provides some examples for references to help all parties understand the relationship between these two kinds of measures.

4.4.1 Technical security measures

Technical security measures are mainly to, through hardware increase, software installation, permission management, requirement setting and the like, technically protect network systems and their management, and recover them in the case of damage.

Technical security measures include but are not limited to the following.

4.4.1.1 Limitation to and control of network ports, protocols and services

The devices, software and processes that can access network are specified in a list, to identify unauthorized network accesses when such accesses are controlled.

Routers should be locked to prevent attacks, and unused ports should be closed to avoid illegal connections.

4.4.1.2 Configuration of network facilities

In order to configure network facilities, such as firewalls, routers, and switches, it should be identified whether each system in the network needs to be controlled. Generally, the IT and OT systems of ships should be controlled.

Firewalls, security gateways, routers and switches should be configured in the networks to be controlled based on the actual situation.

Uncontrolled networks may pose risks due to lack of data traffic control and they should be isolated from controlled networks .Examples:

Networks that are critical to the operation of a ship itself, should be controlled. It is important that these systems - have a high level of security;;

Networks that provide suppliers with remote access to navigation and other OT system software on onboard, should also be controlled. These networks may be necessary for suppliers to allow upload of system upgrades or perform remote servicing. Shoreside external access points of such connections should be secured to prevent unauthorised access.;

- Uncontrolled networks usually include passenger networks, crew entertainment networks, wireless networks, etc.;
- The ashore CCTV system for monitoring is regarded as an uncontrolled network.

Security zones should be established through firewalls in onboard networks. The fewer connections inside security zones, the higher security will be achieved. Confidentiality systems and critical security systems should be in highly protected zones.

4.4.1.3 Restricted place (physical security)

In accordance with the ISPS, Security and safety critical equipment and cable runs should be protected from unauthorized access, Physical security is a central aspect of cyber security,

4.4.1.4 Detection, blocking and alerts

Identifying intrusions and infections is a central part of the control procedures.

A baseline of network operations and expected data flows for user and system 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.

The “Intrusion Detection System” or “Intrusion Prevention System” or firewall functions may be chosen to identify, log, report and attempt to hinder threats, malware, and codes. Dedicated onboard personnel should understand the alerts and their implications. Incidents detected should be directed to an individual or service provider, who is responsible for acting on this type of alert.

4.4.1.5 Satellite and radio communication

Cyber security of the radio and satellite connection should be considered in collaboration with the service provider. When establishing an uplink connection for a ship’s navigation and control systems to ashore service providers, consideration should be given on how to prevent illegitimate connections gaining access to the onboard systems.

The access interconnection is the distribution partner’s responsibility. The final routing of users to terminals is the responsibility of the ship owner. At the access point for this traffic, it is necessary to provide data security, firewalling and dedicated connection.

The VPN (Virtual Private Network) used should be encrypted. Furthermore, a firewall should be deployed in front of the servers and computers connected to networks. The distribution partner should advise on the routing and type of such connection. Onshore filtering of VPN connection is also a matter between the ship owner and distribution partner.

Satellite communication terminals and other communication equipment have been equipped with the management software that is provided by manufacturers and can be accessed and managed in the form of web pages. It is recommended for companies to take these factors into account during security assessment.

4.4.1.6 Wireless access control

Wireless access to networks on the ship should be limited to appropriate authorized devices and secured using strong encryption key, which is changed regularly.

4.4.1.7 Malware detection

Scanning software that can automatically detect and address the presence of malware in systems on board 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.

4.4.1.8 Secure configuration for hardware and software

Only senior officers should be given administrator profiles, so that they can control theset up and change user profiles. User profiles should be restricted to only within the allowable range. User profiles should not allow the user to alter the systems or install and execute new programs.

4.4.1.9 Email and web browser protection

Email communication is a vital part of communication between the ship and shore. Email and web browser protection serves to:

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

Recommendations include:

- email zipping or encryption;
- Disabling of hyperlinks on email systems;
- No use of generic email addresses;
- Configuration of system user profiles.

4.4.1.10 Data recovery capability

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

Retention periods and backup plans should be specified 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 for quick recovery.

4.4.1.11 Application software update

Critical security patches and updates of application software should be applied correctly and in a timely manner, in order to address security flaws of the system as early as possible.

4.4.2 Procedural security measures

Procedural security measures focus on how personnel use onboard systems. The measures containing sensitive information should be kept confidential and handled according to company policies.

Procedural security measures include but are not limited to the following.

4.4.2.1 Training and awareness

Training and awareness are the key supporting elements to an effective approach for the cyber security.

The internal cyber threats should be taken into account and emphasized. Depending on the responsibilities, the training and awareness of onboard personnel and ashore personnel should be properly classified. Personnel have a key role in protecting IT and OT systems may be careless to cause risks.

Partners should perform cyber security protection and training. If necessary, ship owners and management companies should consult partners to verify network protection.

The materials for cyber security publicity should be easy to use by all personnel, with the recommendations as follows:

- Risks related to emails and how to behave in a safe manner;

- Risks related to Internet usage;
- Risks related to the use of own devices;
- Prevention of software installation and maintenance on company hardware using infected hardware or software;
- Safeguarding of information, passwords and digital certificates;
- cyber risks in relation to non-company personnel;
- Detection of suspicious activities or devices and how to report a possible cyber incident;
- awareness of the consequences or impact of cyber incidents to the safety and operations of the ship;
- Understanding of daily security measures;
- Protective measures to be taken before connection of service providers' removable media to ship systems;
- No downgrade of other requirements by using anti-virus software and anti-malware software.

The personnel undertaking duties in cyber risk management should know the signs when a computer has been compromised, such as:

- an unresponsive or slow to respond systemunexpected password changes or authorized users being locked out of a system;
- unexpected errors in programs;
- unexpected or sudden changes in available disk space or memory;
- emails being returned unexpectedly;
- unexpected network connectivity difficulties;
- frequent system crashes;
- abnormal hardware or process activity; and
- unexpected changes to browser, software, settings and permissions.

If the "Intrusion Detection System" is used, the responsible personnel should read system reports to find potential threats as early as possible.

4.4.2.2 Access for visitors

Visitors such as authorities, technicians, agents, port and terminal officials, and owner representatives should be restricted with regard to computer access whilst on board. Critical OT systems should be protected with obvious physical measures to avoid illegitimate use.

The access of visitors to onboard networks should be minimized. When necessary, it should be restricted in terms of user privileges.
The access of service providers for maintenance reason should be approved in accordance with security regulations.

The computers and printers used by visitors should be isolated from the protected networks and devices. To avoid the access of mobile devices, all unprotected computers and network ports should be locked or provided with isolation facilities at available ports.

4.4.2.3 Upgrade and software maintenance

Software and hardware should be technically supported and updated against potential vulnerabilities. For this reason, the use of hardware and software which is no longer supported or updated should be carefully evaluated as part of cyber risk assessment.

Software and hardware should be updated to to maintain a sufficient level of securityProcedures 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 in OT systems should be kept up to date.

Routers, switches, firewalls and OT devices will be running with their own firmware, which may require regular updates and so should be addressed in the procedural requirements.

Effective maintenance of software depends on the development and execution of maintenance measures in the lifecycle.

4.4.2.4 Anti-virus and anti-malware tool update

Procedural requirements should be established to ensure updates are distributed to ships on a timely basis, and that all relevant computers on board are updated.

4.4.2.5 Remote access

Procedures should be established to control the remote access to IT and OT systems. Guidelines should be formulated, specifying who has permission to access, when they can access, and what they can access.

Any procedures for remote access should include close co-ordination with the ship's master and other key ship personnel.

All remote access occurrences should be recorded for review in case of a disruption to an IT or OT system.

Systems, which require remote access, should be clearly defined, monitored and reviewed periodically.

4.4.2.6 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 onto systems with administrator privileges may enable existing vulnerabilities to be more easily exploited. Administrator privileges should only be given to appropriately trained personnel, who, as part of their role in the company or on board, need to log onto systems using these privileges. In any case, use of administrator privileges should always be limited to functions requiring such access.

User privileges should be removed when the people concerned are no longer on board. User accounts should not be passed on from one user to the next using generic usernames. Similar rules should be applied to any onshore personnel, who have remote access to systems on ships. when they change role and no longer need access.The access to onboard systems will be granted to stakeholders. Service providers are a risk because they often have both intimate knowledge of a ship's operations and full access to systems.

To protect access to confidential data and 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.

4.4.2.7 Physical and removable media

When transferring data from uncontrolled systems to controlled systems, there is a risk of introducing malware. Removable media can be used to bypass layers of defenses and attack systems that are otherwise not connected to the internet. A clear policy for the use of such devices should be formulated to ensure that such devices are not used to transfer information between uncontrolled and controlled systems under normal circumstances.

There are, however, situations where it is unavoidable to use these media devices. In such cases, there should be a procedure in place to check removable media for malware and/or validate the legitimate use by digital signatures and watermarks.

Policies and procedures relating to the use of removable media should include the computers that are not connected to the Internet. If it is not possible to scan removable media (e.g. the laptop of a maintenance technician) on board, scanning could be done prior to boarding and the results and time should be recorded. If necessary, companies should consider notifying ports and terminals about the requirement to scan removable media before use on ships. These documents include but are not limited to:

- cargo files and loading plans;
- national, customs, and port authority forms;
- bunkering and lubrication oil forms;
- Ship's store and provisions list;
- Engineering maintenance files.

4.4.2.8 Equipment disposal, including data destruction

Obsolete equipment can contain data which is sensitive or confidential. Procedures should be formulated to ensure that the data and information held in obsolete equipment is properly destroyed prior to disposing of the equipment, ensuring that vital information cannot be retrieved.

4.4.2.9 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 and taken as part of contingency plans.

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

The implementation of contingency plans and procedures should not be affected by cyber incidents. 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 and shutdown of communication links. The impact of cyber incidents on operations and assets should be evaluated according to the CIA model. Generally, the damage to IT systems may affect the continuity of daily work, but not affect the safe operations of ships. If only IT systems are involved in cyber incidents, priority should be given to incident investigation and system recovery.

The damage to OT systems of ships has significant impact on safe operations of ships, so effective measures should be taken immediately to protect the safety of crew and ships and prevent pollution. In general, contingency plans should include the operations in other modes in the case of damage to critical systems. As the ship safety is involved, related operations and contingency procedures should constitute part of the SMS or the information in the SMS should be referenced.

Nonconformity reporting procedures related to cyber incidents in the SMS should specify the object of reporting and extent of authorization in order to promptly execute contingency plans on board.

Onboard personnel should be aware that the damage caused by cyber incidents to OT systems would be treated as equipment faults. Cyber incidents included but are not limited to:

loss of availability of electronic navigational equipment or loss of integrity of navigationrelated data;

loss of availability or integrity of external data sources, including but not limited to GNSS;

loss of essential connectivity with the shore, including but not limited to the availability ofGlobal Maritime Distress and Safety System (GMDSS) communications;

loss of availability of industrial control systems, including propulsion, auxiliary systems andother critical systems, as well as loss of integrity of data management and control;the event of a ransomware or denial or service incident.

The responsible personnel, measures (antivirus, isolation and system recovery) to be taken on ships, and contact information should be specified. When a cyber incident cannot be settled on a ship, ashore support should be sought, including remote operations (advanced tools, administrator settings, and shutdown of services) and operational recommendations (advanced tools, administrator settings, and shutdown of some services). All cyber incidents should be handled immediately after equipment is locked. Backup plans should be restored.

4.6 Effective response

A team, which may include a combination of onboard personnel, company's personnel and/or external experts, should be established to take the appropriate action to restore the IT and/or OT systems so that the ship can resume normal operations. The team should be capable of implementing security measures and responding to foreseeable cyber incidents.

- An effective response should at least consist of the following steps: Initial assessment. The team should find out how the incident occurred, which and how IT and/or OT systems were affected, to what extent the controlled data is affected, and to what extent any threat is caused.
- System and data recovery. Following an initial assessment of the cyber incident, IT and OT systems and data should be cleaned, recovered and restored, so far as is possible, to an operational condition by removing threats from the system and restoring software.

- Incident investigation. To comprehensively understand the causes and consequences of a cyber incident, an investigation should be undertaken by the company to prevent reoccurrence.
- Prevention of reoccurrence. Considering the outcome of the investigation mentioned above, the current procedures should be improved, as part of correction.

When a cyber incident is complex, for example if IT and/or OT systems cannot be returned to normal operation, it may be necessary to initiate the recovery plan alongside onboard contingencyplans. When this is the case, the response team should be able to provide advices to the ship, including but not limited to:

- whether IT or OT systems should be shut down or kept running to protect data;
- whether certain ship communication links with the shore should be shut down;
- the appropriate use of any advanced tools provided in pre-installed security software;
- the extent to which the incident has compromised IT or OT systems beyond the capabilities of existing recovery plans.

4.7 Recovery plan

Cyber incidents cannot disappear or settle by themselves. For example, when ECDIS is infected with malware, another cyber incident will occur after the standby ECDIS is initiated, so it should be specified how to clean and recover the infected system.

Recovery plans are to recover IT and OT systems and their data to an operational state, and should be available in hard copy on board and ashore.

The recovery plan should be understood by personnel responsible for cyber security.

The details of a recovery plan will depend on the type and systems of the ship.

A data recovery capability is a valuable technical protection measure and normally in the form of software backup. The availability of software backup, either on board or ashore, should enable data recovery to an operational condition following a cyber incident.

Recovery of OT systems may be more complex especially if there are no backup systems available and may require assistance from ashore. Details of where this assistance is available and by whom should be part of the recovery plan.

If onboard personnel do not have sufficient expertise and skills, the recovery plan will be limited to obtaining quick access to technical support. Otherwise, more extensive diagnostic and recovery actions may be performed.

4.8 Cyber incident investigation

Experience lessons from previous cases will effectively improve response capabilities, so measures for information collection should be developed.

In order to comprehensive learn about a cyber incident and gain more information, cyber incidents should be investigated by companies in accordance with the procedures. If necessary, support from external experts should be sought. The information from an investigation can be used to improve the security management on board and ashore and also extensively help to deal with cyber risks in the industry. Any investigation should result in:

- a better understanding of the potential cyber risks on board and ashore;
- a summary of experience and lessons;
- improvement of security measures to prevent recurrences.

4.9 Management assessment and improvement

It should be recognized that maritime cyber risk management is process of continuous improvement and perfection. Considering the requirements of the ISM Code for periodical evaluation of the SMS, companies should evaluate the effectiveness of cyber risk management regularly and after cyber incidents, and conduct corresponding improvements based on the evaluation results.

Annex 1 Cyber Risk Management System and Safety Management System

The IMO Resolution MSC.428(98) makes clear that SMS should take into account cyber risk management when meeting the objectives and functional requirements of the ISM Code. The guidance provided in the Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3) provides generic recommendations regarding the elements (identification, protection, detection, response, and recovery) of cyber risk management. By reference to the "Guidelines on Maritime Cyber Risk Management" (MSC-FAL.1/Circ.3), this annex lists the recommended minimum measures that all companies should consider implementing so as to address cyber risk management in SMS.

A. Identify

Roles and Responsibilities for Identification	
Action	Remarks
ISM Code: 3.2 Update the safety and environment protection policy to incorporate cyber risks.	An updated safety and environment protection policy should demonstrate: ➢ a commitment to manage cyber risks as part of the overall approach to safety management and protection of the environment; ➢ an understanding that CRM has both safety and security aspects, but the emphasis is on managing the risks introduced by OT, IT and networks; ➢ an understanding that without appropriate technical and procedural risk protection and control measures, OT is vulnerable to disruption, affecting the safe operation of a ship and protection of the environment. Nothing in the updated policy should suggest that CRM is given any more or less attention than any other risks identified by the company.
ISM Code: 3.3 Update the responsibility and authority information provided in the SMS to include appropriate allocation of responsibility and authority for cyber risk management.	In general, IT personnel should understand potential vulnerabilities in computer-based systems and know the appropriate technical and procedural protection measures to help ensure the availability and integrity of systems and data. Operational and technical personnel should generally understand the safety and environmental impacts of disruption to critical systems on the SMS. Allocation of responsibility and authority may need to be updated, including: ➢ allocation of responsibilities and authorities which encourage cooperation between IT personnel (which may be provided by a third party) and the company's operational and technical personnel; ➢ incorporation of the compliance with cyber risk management policies and procedures into the existing responsibility and authority of the Master.
ISM Code: 6.5 Using the existing systems, identify any training which may be required for cyber management systems.	Training is a protection and control measures that forms the basis of CRM. It helps to ensure that personnel understand how their actions will influence the secure operation of the company's networks. The existing procedures for identifying training requirements should be used to assess the benefits and needs for: ➢ all company personnel to receiver basic cyber security training in support of the company's CRM policies and procedures;

	➢ company personnel, who have been assigned CRM duties, to receive a type and level of training appropriate to their responsibility and authority.

Identification of system, asset, data and capability endangering ship operation if damaged	
Action	Remarks
ISM Code: 10.3 Using the existing system, identify the sudden failure of equipment and technical systems (OT and IT) which may result in hazardous situations.	SMS will already identify the equipment and technical systems (including OT and IT), and capabilities, which may cause hazardous situations if they become unavailable or unreliable. The impacts should have already been documented. However, SMS, which incorporates CRM, will also need to address data in the context of sudden operational failure. Loss of availability or integrity of data used by critical systems can have the same impact as the system becoming unavailable or unreliable for some other reason. Consequently, it is recommended that the list of equipment and technical systems should be supplemented by a list of data used and its source(s).

B. Protect

Risk Control Measures	
Action	Remarks
ISM Code: 1.2.2.2 Assess all identified risks to ships, personnel and the environment and establish appropriate safeguards.	The full scope of risk control measures implemented by the company should be determined by a risk assessment, taking into account the information provided in these guidelines. As a baseline, the following measures should be considered before a risk assessment is undertaken. These technical and procedural measures should be implemented in all companies to the extent appropriate. ➢ Hardware inventory. Develop and maintain a register of all critical system hardware on board, including authorized and unauthorized devices on company controlled networks. The SMS should include procedures for maintaining this inventory throughout the operational life of the ship. ➢ Software inventory. Develop and maintain a register of all authorized and unauthorized software running on company-controlled hardware onboard, including version and update status. The SMS should be updated to include procedures for: ✓ maintaining this inventory when hardware controlled by the company is replaced; ✓ maintaining this inventory when software controlled by the company is updated or changed; ✓ authorizing the installation of new or upgraded software on hardware controlled by the company; ✓ prevention of installation of unauthorized software, and deletion of such software if identified; ✓ software maintenance. ➢ Map data flows. Map data flows between critical systems and other equipment/technical systems on board and ashore, including those

	provided by third parties. Vulnerabilities identified during this process should be recorded and securely retained by the company. The SMS should be updated to include procedures for:

	✓ maintaining the map of data flows to reflect changes in hardware, software and/or connectivity; ✓ identifying and responding to vulnerabilities introduced when new data flows are created following the installation of new hardware; ✓ reviewing the need for connectivity between critical systems and other OT and IT systems. Such a review should be based on the principle that systems should only be connected where there is a need for the safe and efficient operation of the ship, or to enable planned maintenance; ✓ controlling the use of removable media, access points and the creation of ad-hoc or uncontrolled data flows. This may be achieved by restrictions on the use of removable media and disabling USB and similar ports on critical systems. ➢ Implement secure configurations for all hardware controlled by the company. This should include documenting and maintaining commonly accepted security configuration standards for all authorized hardware and software. The SMS should include policies on the allocation and use of administrative privileges by ship and shore-based personnel, and third parties. However, it is not recommended that the details of secure configurations are included in the SMS. This information should be retained separately and securely by the company. ➢ Audit logs. Security logs should be maintained and periodically reviewed. Security logging should be enabled on all critical systems with this capability. The SMS should be updated to include procedures for: ✓ policies and procedures for the maintenance of security logs and periodic review by competent personnel as part of the operational maintenance routine; ✓ procedures for the collation and retention of security logs by the company, if appropriate. ➢ Awareness and training.

	➢ Physical security. The physical security of the ship is enhanced by compliance with the security measures addressed in the ship security plan (SSP) required by the ISPS Code. Measures should be taken to restrict access and prevent unauthorized access to critical system network infrastructure onboard.

Development of emergency plan	
Action	Remarks
ISM Code: 7 Update procedures, plans and instructions for key shipboard operations concerning the safety of the personnel, ship and protection of the environment which rely on OT.	SMS should already address procedures, plans and instructions for key shipboard operations concerning the safety of the personnel, ship and protection of the environment. In general, these plans should be unaffected by the incorporation of CRM into the SMS. This is because the effect of the loss of availability of OT, or loss of integrity of the data used or provided by such systems, is the same as if the OT was unavailable or unreliable for some other reason. Notwithstanding this, consideration should be given to developing instructions on the actions to be taken if disruption to critical systems is suspected. This could include procedures for reverting to back-up or alternative arrangements as a precaution whilst any suspected disruption is investigated.

	Procedures for periodically checking the integrity of information provided by OT to operators should be considered for inclusion in operational maintenance routines.
ISM Code: 8.1 Update emergency plans to include responses to cyber incidents.	SMS should already address emergency plans for the disruption of critical systems required for the safe operation of ships and protection of the environment. In general, these plans should be unaffected by the incorporation of cyber risk management into safety management systems. This is because the effect of common shipboard emergencies should be independent of the root cause. For example, a fire may be caused by equipment malfunctioning because of a software failure or inappropriate maintenance or operation of the equipment. Notwithstanding the above, consideration should be given to the development of a cyber incident module in the integrated system of shipboard emergency plans for significant disruption to the availability of OT or the data used by them. The purpose of the module could be to provide information on the actions to be taken in the event of a simultaneous disruption to multiple OT systems required for the safe operation of the ship and protection of the environment. In this more complex situation, additional information on appropriate immediate actions to be taken in response may be necessary.

C. Detect

Development and implementation of measures for timely detection of cyber incidents	
Action	Remarks
ISM Code: 9.1 Update procedures for reporting non-conformities, accidents and hazardous situations to include reports relating to cyber incidents.	SMS should already address procedures relating to non-conformities. When incorporating CRM into the SMS, company reporting requirements for non-conformities may need to be updated to include cyber related non-conformities. Examples of such non-conformities and cyber incidents: ➢ unauthorized access to network; ➢ unauthorized or inappropriate use of administrator privileges; ➢ suspicious network activity; ➢ unauthorized access to critical systems; ➢ unauthorized use of removable media; ➢ unauthorized connection of personal devices; ➢ failure to comply with software maintenance procedures; ➢ failure to apply malware and network protection updates; ➢ loss or disruption to the availability of critical systems; ➢ loss or disruption to the availability of data required by critical systems.

D. Respond

Development and implementation of measures and plans for operations or services affected by cyber incidents, to prolong the life and recover such systems or services	
Action	Remarks
ISM Code: 3.3 Ensure that adequate resources and shore-based support are available to support the DPA in responding to the loss of critical systems.	SMS should already be supported by adequate resources to support the DPA. However, the incorporation of CRM into the SMS should require that this resourcing includes appropriate IT expertise. This resource could come from within the company but may also be provided by a third party. In providing the adequate resources, the following should be considered:

	➢ company or third party technical support should be familiar with onboard IT and OT infrastructure and systems; ➢ any internal response team or external cyber emergency response team should be available to provide timely support to the DPA; ➢ provision of an alternative means of communication between the ship and the DPA, which should be able to function independently of all other shipboard systems, if and when the need arises; ➢ internal audits should confirm that adequate resources, including third parties when appropriate, are available to provide support in a timely manner to support the DPA.
ISM Code: 9.2 Update procedures for implementing corrective actions to include cyber incidents and measures to prevent recurrence.	SMS should already include procedures for responding to non-conformities. In general, these should not be affected by the incorporation of CRM in SMS. However, the procedures should help ensure that: ➢ consideration of non-conformities and corrective actions involves the personnel with responsibility and authority for CRM; ➢ corrective actions, including measures to prevent recurrence, are appropriate and effective.
ISM Code: 10.3 Update the specific measures aimed at promoting the reliability of OT.	SMS should already include procedures for operational maintenance routines to promote the reliability of equipment on board. A SMS, which incorporates CRM, should outline procedures for: ➢ Software maintenance as a part of operational maintenance routines: Such procedures should ensure that application of software updates, including security patches, are applied and tested in a timely manner, by a competent person; ➢ Authorizing remote access, if necessary and appropriate, to critical systems for software or other maintenance tasks, including authorizing access in general (including verification that service providers have taken appropriate protective measures themselves) and for each specific remote access session; ➢ Preventing the application of software updates by service providers using uncontrolled or infected removable media; ➢ Periodic inspection of the information provided by critical systems to operators and confirmation of the accuracy of this information when critical systems are in a known state; ➢ Controlled use of administrator privileges to limit software maintenance tasks to competent personnel.

E. Recovery

Backup and recovery of ship systems subject to harm of cyber incidents	
Action	Remarks
ISM Code: 10.4 Include creation and maintenance of back-ups into the ship's operational maintenance routine.	SMS should already include procedures for maintaining and testing back-up arrangements for shipboard equipment. Notwithstanding this, it may not address procedures for maintaining and storing offline back-ups for data and systems required for the safe operation of the ship and protection of the environment. A SMS, which incorporates CRM, should include procedures for:

	➢ checking back-up arrangements for critical systems; ➢ checking alternative modes of operation for critical systems; ➢ creating or obtaining back-ups, including clean images for OT to enable recovery from a cyber incident; ➢ maintaining back-ups of data required for critical systems to operate safely; ➢ offline storage of back-ups and clean images, if appropriate; ➢ periodic testing of back-ups and back-up procedures.

Annex 2: Development of Security Measures based on Results of Risk Assessment

To help all parties develop security measures based on the results of risk assessment, the following table lists some examples.

S/N	Risk Source	Hazard	Cause	Extent of Hazard	Security Measures
1.	Office computer requiring no Internet access	Computer failure or data loss, affecting normal operation	Virus	Medium	Cyber security education, anti-virus software installation and update, and ship equipment interface management
2.	Internet access of ship equipment	Disclosure of ship information, business information, and personal information	Trojan and backdoor program	Medium	Cyber security education, Internet terminal list, firewall, antivirus software installation and update, service provider management, and ship equipment interface management
3.	Internet access of ship equipment	Modification of equipment parameters, resulting in equipment failure, route deviation, etc.	Malicious attack, Trojan, and backdoor software	High	Cyber security education, Internet terminal list, firewall, antivirus software installation and update, service provider management, and ship equipment interface management
4.	Internet access of office computer	Disclosure of ship information, business information and personal information	Trojan and backdoor program	Medium	Cyber security education, Internet terminal list, firewall, antivirus software installation and update, and office computer interface management
5.	Internet access of office computer	Computer failure or data loss, affecting normal operation	Virus, Trojan and backdoor program	Medium	Cyber security education, Internet terminal list, firewall, antivirus software installation and update, office computer interface management, data backup, and spare computer
6.	Internet access of crew for entertainment	Disclosure of personal information, ship photo and work document	Trojan and backdoor program	Medium	Cyber security education, firewall and Internet access software restriction
7.	Internet access of crew for entertainment	Spreading of virus within ship LAN, making other terminals infected with virus	Virus, Trojan and backdoor program	Medium	Cyber security education, firewall, and Internet access software and/or port restriction
8.	Internet access of passenger for entertainment	Spreading of virus within ship LAN, making other terminals infected	Virus, Trojan and backdoor program	Medium	Cyber security education, firewall, and Internet access software and/or port restriction

		with virus			

Common security measures described in this table include:

1. Cyber security education; 2. Internet access terminal list; 3. Firewall; 4. Anti-virus software installation and update; 5. Interface management; 6. Internet access terminal and/or port restriction; 7. Personnel management.

To learn about the status of the ship's firewall and anti-virus software regularly and when necessary, and provide necessary technical support and maintenance should be performed, the following should be considered:

8. Appointment of onboard network administrator; 9. Appointment of corporate network administrator; 10. Management of firewall and antivirus software log; 11. Purchase of security services from network service providers.

These measures are described as follows:

1. Cyber security education: Perform training or publicity based on the actual situation of onboard networks, so that participants have necessary cyber security knowledge;

2. Internet access terminal list: Detail Internet access terminals and specify the scope of management;

3. Firewall: Critical device for cyber security, controlling the permission of Internet access terminals and resist external hazards through settings, prohibiting the unauthorized networks from Internet access, and controlling the Internet access of authorized networks according to necessary policies;

4. Anti-virus software installation and update: Critical software for cyber security, protecting computers from being infected with virus;

5. Interface management: reduce the connections of USB flash disks, mobile hard disks, mobile phones and other facilities to devices and computers through interfaces, thus protecting the devices and computers from being infected with virus;

6. Internet access software and/or port restriction: Restrict Internal access software and/or ports according to the work and entertainment needs, while restricting Internal access terminals, to further ensure the security;

7. Personnel management: Check the identifies of personnel boarding, strengthen the management of identities of key service providers and maintenance companies, and lock key parts of ships when required or unmanned;

8. Appointment of onboard network administrator: Appoint the responsible person and perform training on knowledge updates for simple cyber security maintenance and parameter change with ashore support;

9. Appointment of corporate network administrator: Appoint the responsible person to provide ashore support for ships and facilitate communication;

10. Management of firewall and antivirus software log: onboard network administrator should regularly check the log for abnormalities and report to the company in a timely manner, and remote management may be implemented by the corporate network administrator if possible;

11. Purchase of security service from service provider: Considering the professional expertise of cyber security, the company may purchase security services from network service providers in order to obtain more professional services and regularly check the security of onboard networks.