Loss Prevention Brochure
A Guide to Cyber Risk Management

船舶网络风险管理指导手册

CCS 中国船级社

中船保 CHINA P&I CLUB

目录 Contents

Necessity for Managing Cyber Risks

1 必要性

近年来，船舶技术越来越多地引入了数字化、集成化和自动化系统，船上的信息技术和操作技术正在越来越多地连接到互联网上，随着一些大型航运公司发生了代价高昂的网络风险事件，船舶的网络风险开始引起业内的关注。

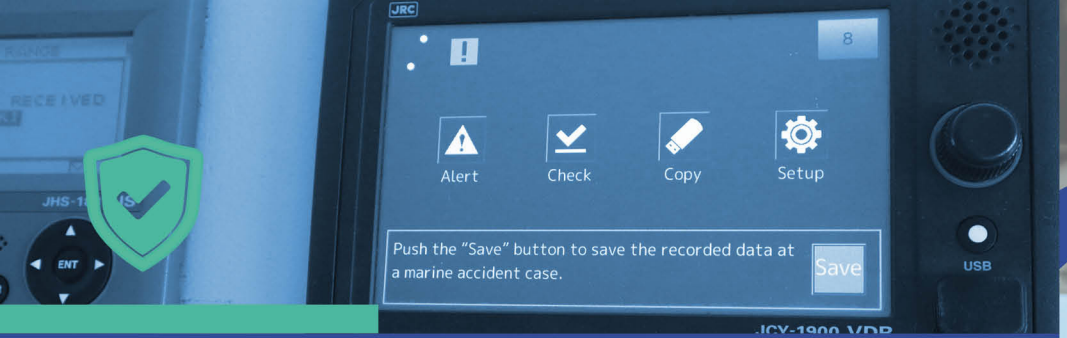
With digitalised, integrated and automated solutions increasingly applied in shipping, the information technology (IT) and operation technology (OT) systems on ships are now connected to the World Wide Web. However, some examples of cyber incidents at major shipping companies have taught us a brutal lesson about risk management.

国际海事组织（IMO）在第98届海安会上，针对海事风险管理进行了讨论，并通过了MSC.428(98)号决议。决议指出，经批准的公司安全管理体系（SMS）应根据国际安全管理规则（ISM Code）的目标和功能要求考虑网络风险管理，并鼓励成员国不迟于 2021 年 1 月 1 日之后对公司合规文件进行首次年度审核之前，公司安全管理体系纳入网络风险管理相关内容。

The IMO Maritime Safety Committee at its 98th session considered the necessity for maritime cyber risk management (CRM) and adopted Resolution MSC.428(98), which stated that an approved Safety Management System (SMS) should consider CRM in accordance with the objectives and functional requirements of the ISM Code. It further encouraged administrations to appropriately address cyber risks in SMS no later than the first annual verification of the company's Document of Compliance (DOC) after 1 January 2021.

IMO从风险管理角度考虑网络安全对船舶安全的影响，要求将船舶网络风险管理纳入船舶安全管理框架中。船舶网络风险不仅有可能对船舶造成安全威胁，也可能对环境、港口、人员和货物安全构成危险。同时，由于网络风险事件的不确定性，还可能导致租约方面的争议。如何避免网络风险事件的发生，以及发生网络风险事件后，如何保证船舶和人员的安全并防止海洋环境受到影响，这些都需要船舶建立一套全面的网络风险管理体系，以促进与国际标准和/或船旗国和港口管理要求的适当程度的合规。

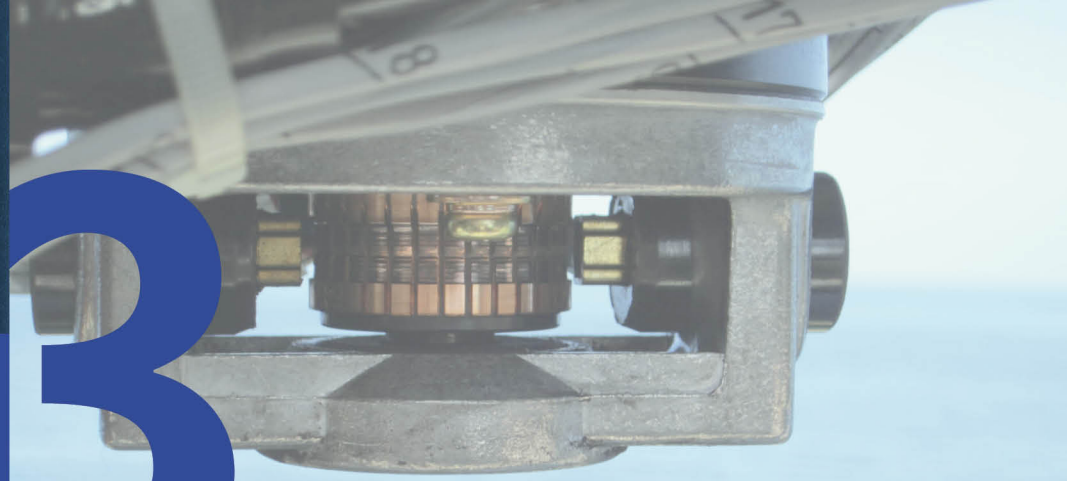
IMO highlighted the effect of cyber security on safe and secure shipping operations from the perspective of risk management. Not only ships and cargos, but also personnel, port facilities, and the marine environment will be exposed to risks in the event of a cyber-attack. The execution of charterparties may also be affected. To mitigate the risks and to comply with international guidelines and/or regulations of relevant flag states and port states, it should be acknowledged that a complete CRM system is necessary for all ships.



鉴于船舶网络风险对人员、船舶、货物和环境等存在的潜在影响，船舶网络风险管理是指识别、分析、评估和管理船舶网络相关风险，并通过权衡利益相关方采取行动的成本和收益，将其接受、避免、转移或减轻到可接受的水平的过程。船舶网络风险管理涉及保护包括信息技术、操作技术以及数据化资料在内的关键数据免受未经授权的访问、操纵和破坏，涵盖涉及船舶安全的关键数据的可用性或完整性丧失等风险。

Given the potential impact of cyber risks on personnel, ship, cargo and the environment, CRM is defined as the process of identifying, analysing, assessing, 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. CRM, covering the risks in maintaining the availability and integrity of data concerning ship security, is carried out to protect those data and the IT/OT systems from unauthorised access, manipulation, or disruption.

2 定义
Definition of Cyber Risk Management



3 目的
Objectives of Cyber Risk Management

船舶网络风险管理的目的是针对船舶面临的网络风险，通过考虑国际海事组织、主管机关、船级社和海运行业组织所建议适用的规则、指南和标准，制订网络风险防范措施，为船舶营运提供安全做法和安全工作环境，提高岸上及船上人员的网络安全管理技能，包括网络安全及环境保护方面的应急准备，从而保证海上安全，防止人员伤亡，避免对环境，特别是海洋环境造成危害以及对财产造成损失。

By taking into account applicable regulations, guidelines and standards suggested by the IMO as well as relevant administrations, classification societies and international associations, CRM is carried out to offer a best practice for ship operations and a safe working environment for all through a set of preventive measures, to improve management level including emergency preparedness of the crew and shore-based employees, and finally to avoid any marine pollution, or personal injury, or loss of properties.

基本原理

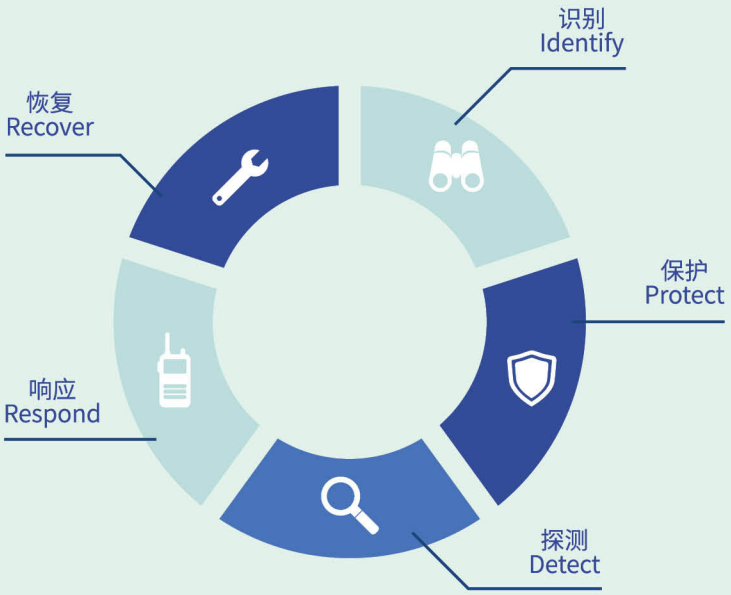
Principle of Cyber Risk Management 4

船舶网络风险管理的基本原理是基于IMO相关决议及通函要求，实施适当水平的网络风险管理，提升网络安全防御能力，保持网络弹性，对网络进行持续监测，以预防、应对网络事故并在发生网络事故后恢复。

The principle of CRM is to prevent, handle, and recover from cyber incidents by developing cyber security capabilities and constantly supervising cyber resilience in accordance with relevant IMO resolutions and circulars.

根据网络安全框架，网络风险管理的主要功能要素包括：识别、保护、探测、响应和恢复。

The Cybersecurity Framework describes five functional elements of CRM – identify, protect, detect, respond, and recover.



- **识别** - 定义网络风险管理的人员角色/职责，并识别系统、资产、数据和能力，当这些系统被破坏时，会对船舶运营构成风险；
  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.

- **保护** - 实施风险控制流程和措施，以及应急计划，以防范网络事件，确保船舶操作的连续性；
  Protect - implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.

- **探测** - 制定和实施必要的活动，及时发现网络事件；
  Detect - develop and implement activities necessary to detect a cyber-event in a timely manner.

- **响应** - 制定并实施活动和计划，为因网络事件而受损的航运业务或服务提供恢复能力和恢复系统；
  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.

- **恢复** - 确定备份和恢复受网络事件影响的航运操作所必需的网络系统的措施。
  Recover - identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

船舶网络风险管理的方法是通过采用网络风险管理基本原理，实施适当水平的网络风险控制，建立网络安全能力，并持续监控整体网络弹性，以预防、响应和恢复网络事件，将网络风险管理纳入船舶安全管理体系。

The approaches to CRM include exercising a proper level of risk control, incorporating risk control processes into ship SMS, and implementing activities to provide resilience and to restore systems upon the occurrence of a cyber-event.

船舶网络风险管理方法可通过如下步骤实现
To be more specific, CRM can be carried out through the following steps

5 管理方法 Approaches to Cyber Risk Management

识别资产：全面识别船上的所有资产包括设备、系统、网络和数据流，以便了解哪些需要纳入管理系统。
Identify assets: pinpoint all assets on board ships including equipment, systems, networks and data flows to understand what need to be managed.

识别威胁：了解船舶面临的外部网络风险威胁，了解因使用不当和缺乏网络安全意识而导致的内部网络风险威胁。
Identify threats: understand the external cyber security threats to the ship, and the internal threats posed by inappropriate use and poor cyber security practices.

识别漏洞：列明带有直接和间接通信链接的船载系统清单，了解网络风险威胁对船载系统造成的后果，了解现有保护措施的功能和局限性。
Identify vulnerabilities: develop inventories of onboard systems with direct and indirect communications links. Understand the consequences of a cyber security threat on these systems. Understand the capabilities and limitations of existing protection measures.

评估风险：确定漏洞被外部威胁利用的可能性，确定因不当使用而暴露漏洞的可能性，确定任何单个或组合漏洞被利用的风险和对安全的影响。
Assess risk exposure: determine the likelihood of vulnerabilities being exploited by external threats. Determine the likelihood of vulnerabilities being exposed by inappropriate use. Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.

制定保护措施：通过制定保护措施减少漏洞被利用的可能性，减少漏洞被不当利用的潜在影响。
Develop protection measures: reduce the likelihood of vulnerabilities being exploited through protection measures. Reduce the potential impact of a vulnerability being exploited.

建立应急预案：制定优先级应急预案，以减少任何潜在的网络风险。
Establish contingency plans: develop a prioritised contingency plan to mitigate any potential identified cyber risk.

响应和恢复网络风险事件：使用应急预案对网络风险事件进行响应和恢复网络功能，对应急预案的有效性进行评估，并对网络风险威胁和漏洞进行重新评估。
Respond to and recover from cyber security incidents: respond to and recover from cyber security incidents using the contingency plan. Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.

Vulnerable Onboard Systems

易受网络风险影响的船载系统

6

数字和互联网时代的船舶已经和计算机整合为一组复杂的工业系统和嵌入式系统，不再与任何计算机网络进行物理隔离，因此无法避免数字化系统故障。船载系统程序中的操作错误、软件缺陷、未经授权访问的系统入侵、管理公司对船舶网络未能采用有效的风险控制程序等，都会使船舶操作技术的可用性和完整性受到影响。如，电子海图显示和信息系统（ECDIS）中的海图数据被破坏；船舶软件维护或打补丁过程中出现故障；或对船舶的操作至关重要的外部传感器数据丢失或被操纵，例如包括全球导航卫星系统（GNSS）数据在内的船舶关键数据的丢失或被恶意操纵等。

Ships in the Internet era have become a complicated industrial system with computer networks embedded in each one of them, the corollary being that there can be system failures occasionally, for example due to an operational error, a software bug, an unauthorised access, or a weak CRM procedure. Then the availability and integrity of IT/OT systems will inevitably be affected – the chart data in an Electronic Chart Display and Information System (ECDIS) may be corrupted, or the software maintenance and patching process may fail, or critical data of external sensors including Global Navigation Satellite Systems (GNSS) may be lost/manipulated.

随着船舶网络风险管理体系的实施，船旗国和港口国将逐步开展有关船舶网络风险管理的检查评估，船舶网络风险评估将可能包括但不限于如下内容：

With the implementation of CRM procedures on ships, relevant flag administrations and port states are expected to carry out assessment on compliance with CRM regulations. The assessment may include the following questions:

船舶网络风险评估的常见问题

FAQ in Cyber Risk Assessment

7

船舶有哪些系统面临网络风险?
What systems onboard are at risk?

船舶网络事件的潜在影响有哪些?
What is the potential impact of a cyber incident?

谁是船舶网络风险管理的责任人?
Who is responsible for cyber risk management?

船舶操作系统和其工作环境是否受互联网影响?
Are the OT systems and their working environment affected by the Internet?

船舶是否有远程访问操作系统?如果有，如何监控和保护远程访问操作系统?
Is there remote access to the OT systems and, if so, how is it monitored and protected?

船舶信息系统是否受到保护，远程访问是否受到监视和管理?
Are the IT systems protected and is access being monitored and managed?

船舶正在使用的网络风险管理最佳实践是什么?
What cyber risk management best practices are being used?

船舶信息系统和操作系统培训情况如何?
What is the cyber risk training level of the personnel operating the IT and OT system?

8

船舶网络风险管控建议

Recommendations on Cyber Risk Control

对于潜在的船舶网络风险，公司和船舶应基于对船舶网络风险的管控，同时兼顾到人员、货物和港口的安全，因此建议会员船东从如下几个方面做好船舶网络风险管控：

To prevent severe consequences that are potentially suffered by ships, ports, personnel and cargos, member shipowners are recommended to have in place control measures by:

- 建立健全符合要求并适合船舶运营的网络风险管理体系并确保有效实施；
  Establishing a compliant and appropriate CRM system and ensuring that it is effectively implemented;

- 船舶确保网络风险管理文件得到妥善保管，保证人员在上岗前、新聘船员在开航前阅读到与之相关的职责、程序和须知，提升船舶网络风险防御能力以降低网络风险；
  Keeping properly cyber security documentation on ships and ensuring that crews and new hires understand the procedures taken and their responsibilities;

- 加强船员网络风险管理培训，提高船员网络风险意识；
  Carrying out seafarer training to improve their cyber security awareness;

- 签订运输合同考虑网络风险条款。
  Considering a cyber security clause when entering into carriage contracts.

9 Notice for Use of Key Devices

船舶关键网络设备使用指引

9.1 物理端口使用须知 Physical Ports

移动存储介质如U盘、移动硬盘等应确保无病毒后才可接入USB口；
Make sure removable media like a USB stick or a mobile hard drive are not infected before inserting them into an onboard system.

关键设备，如ECDIS、主机监控、货物控制、压载水管理等系统，设备及系统的USB/RJ45网口应采取物理或软件措施进行管控（例如禁用、加锁等），如有困难，也可采用签封（贴上签有日期和管理员姓名的封条）等其它管控方式，以防止私自接入；
USB/RJ45 ports of key equipment and systems eg ECDIS, engine governor, cargo management systems, ballast water systems shall be secured with physical protection or control software (blocking the ports or using locks). If these measures are not practicable, put on stickers with date and name of the administrator to avoid unauthorised access by rogue devices.

关键系统及设备的USB、Type-C、RJ45网口不得用作其他用途，如接入个人设备、照明、供电等。
USB/Type-C/RJ45 ports of key equipment and systems shall not be used for other purposes, for example as power supply to personal devices or illuminating devices.

9.2 ECDIS使用须知 ECDIS

ECDIS主机应进行必要的控制，防止非法接触，如将ECDIS主机和控制柜锁闭；
Protect the ECDIS computers from unauthorised access by eg locking the operating units.

建议配置专用UPS电源，避免由于断电而影响正常使用；
Have onboard an uninterruptible power supply (UPS) in case use of the devices are prevented by power failures.

ECDIS主机的USB、网线等接口，应采取物理措施进行管控，防止非法接入，也可采用签封（贴上签有日期和管理员姓名的封条）等其它管控方式，以防止私自接入；
USB and Ethernet port of ECDIS computers shall be secured with physical protection or stickers with date and name of the administrator to avoid unauthorised access.

多台ECDIS不可同时进行数据或系统升级，必须在一台升级完成，确认工作正常后方可升级另一台；
Software or system update cannot be performed on both ECDIS computers simultaneously. Make sure one is good for working before moving on to the other.

ECDIS必须使用专用的移动存储介质，不可随便使用其它移动存储介质，使用前，专用存储介质也需进行必要的扫描杀毒；
Allow only designated media device to be connected to ECDIS for data transfer and there should be a procedure in place to scan the device prior to the use of it.

如有第三方接触ECDIS，需经船长批准，并安排专人全程陪同。
For any third party that needs to access ECDIS, the operation should be authorised by the master and performed in the company of a designated crew member.

9.3 个人设备使用须知 Personal Devices

- 个人设备不得生产、复制、存储秘密文件；
  Personal devices shall not be used to produce, duplicate, or save confidential document.
- 个人设备不得接入船舶办公网络，只能接入船员网络；
  Implement network separation onboard. Personal devices shall not be connected to the administrative network but only to the crew/guest network.
- 如非必要，个人设备不做办公工具；
  Do not use personal devices for official use unless it is unavoidable.
- 使用授权软件，桌面操作系统应安装杀毒软件，并及时更新病毒库；
  Use only authorised software. Install antivirus software on desktop and keep it up to date.
- 及时更新系统补丁。
  Update security patches in a timely manner.

9.4 密码使用须知 Passwords

- 网络设备的管理员账户不得使用默认口令；
  Do not use default passwords for the administrator' s account.
- 账号和密码不能存储在计算上或使用自动登录功能，不能写在纸上挂于系统附近；不得以明文形式在电子邮件、传真中传播；
  Turn off automatic login. Do not record account names and passwords in the computer or put them on a paper next to the computer or disclose them in any email and facsimile.
- 密码应定期更改，时间不长于3个月；
  Change passwords at a regular interval no longer than 3 months.
- 密码长度不得少于8位，包括数字、大小写字母、标点和特殊字符组成；
  Each password should be strong enough – 8 digits minimum including numbers, uppercase/lowercase letters and special characters.
- 避免以生日、姓名拼音、手机号码等与身份隐私相关的信息作为口令。
  Avoid use date of birth, pinyin or spelling of names, mobile phone numbers or any other information related to personal identity as passwords.

9.5 社交媒体使用须知 Social Media

- 不得在互联网社交媒体上（微信、微博、脸书等）发布列入保密范围的信息，以及不良网络信息；
  Do not release any confidential or negative information via social media (WeChat, Weibo, Facebook, etc).

- 不得从事危害网络秩序、网络安全的活动；
  Do not engage in any activity that endangers order and security of the Internet community.

- 不得制造、运行、传播计算机病毒等破坏程序或黑客程序；
  Do not produce, run, or spread any computer virus or malware.

- 发现网络异常或病毒木马，应第一时间断网（如拔掉网线、关闭无线），并通知管理员处理。
  Cut off internet access immediately (eg unplug the cable or turn off wireless connection) and inform the administrator upon spotting trojans, viruses or other cyber threats.

10 船舶网络风险事件的响应

船舶应成立一个包括船上人员、公司人员和/或外部专家的响应团队，承担恢复信息技术和/或操作技术系统的职责，以便船舶能重新正常操作。该团队需具备执行各项安全措施和响应可预见的网络事件的能力。

A response team of crew members, company personnel and/or external specialists shall be set up to undertake duties of restoring the IT/OT systems for the normal operations of the ship. The team should be capable of executing safety precautions and handling with foreseeable cyber incidents.

有效的响应至少包括如下内容
There are 4 key steps to an effective incident response

初始评估 Initial assessment

团队需识别网络事件的现象、信息技术和/或操作技术系统受损的范围和现状、受控数据受损的范围、后续危害；
The response team should find out what the cyber threat is; which and how the IT/OT systems were affected; to which extent the operational data were affected; and what threats may remain to the ship's operation.

系统和数据的恢复 Restoration of systems and data

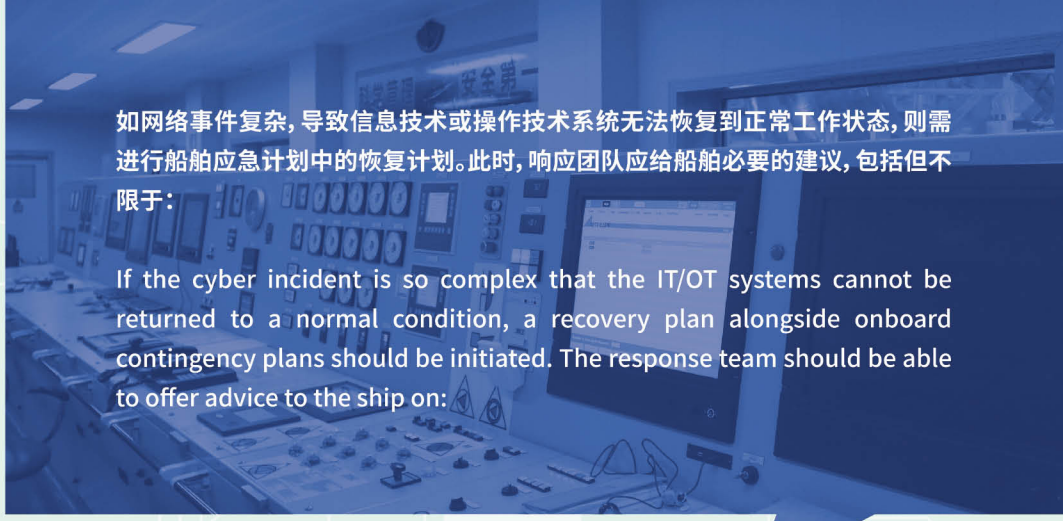
初始评估后，信息技术和操作技术系统及数据应当消除感染、恢复和复原，尽量达到可用的状态；
Remove the threat immediately after the initial assessment and restore the IT/OT systems to an operational condition so far as is possible.

事件调查 Investigation and analysis

为全面了解网络事件的原因和结果，应开展事件调查，以有效防止再次发生；
Investigate the cyber incident for its causes and consequences so that potential recurrence can be prevented.

防止再犯 Correction and eradication

作为纠正的一部分，应基于调查结果改进既有规定。
Improve the current regulations or procedures, as part of the corrective actions, considering the outcome of the investigation.



如网络事件复杂，导致信息技术或操作技术系统无法恢复到正常工作状态，则需进行船舶应急计划中的恢复计划。此时，响应团队应给船舶必要的建议，包括但不限于：

If the cyber incident is so complex that the IT/OT systems cannot be returned to a normal condition, a recovery plan alongside onboard contingency plans should be initiated. The response team should be able to offer advice to the ship on:

- 信息技术或操作技术系统是否应关闭或为了保护数据而继续运行；
  Whether IT/OT systems should be shut down or kept running to protect data;
- 船岸联系的特定连接是否应关闭；
  Whether certain ship communication links with the shore should be shut down;
- 使用已安装的防护软件中的高级功能；
  The appropriate use of any recovery tools provided in pre-stalled security software;
- 信息技术或操作技术系统的损坏超出现有恢复计划的范围。
  The extent to which the incident has compromised IT/OT systems beyond the capabilities of existing recovery plans.

11

船舶网络风险事件的修复
Recovery from Cyber Security Incidents

船舶网络数据修复是保障船舶在网络事件发生后重新恢复正常操作的一种重要手段，通常是通过软件备份数据的方式完成的，船舶网络数据软件备份应当能够在网络事件后将数据恢复到可用状态。

A CRM system with data recovery capability should be able to restore a system and/or data from a secure copy, and thereby allowing the normal operations of the ship.

船舶发生网络风险事件后，除由响应团队根据管理体系要求对网络风险事件进行响应外，由于网络事件不会自行消失和解决，船舶网络风险管理体系应当涵盖并明确如何清理和修复被感染的系统的恢复计划。该计划应根据船舶的船型和船舶系统以及船舶的特点进行制定，同时应考虑到船上人员的专业知识和技能水平，恢复过程如需岸基支持，恢复计划应当涵盖相关信息。

Following response to cyber incidents in accordance with established requirements, a recovery plan on how to clean and repair infected IT/OT systems should be specified in the CRM system as cyber threats would not remove themselves. The development of such a recovery plan should depend on the type of ship, its characteristics and the IT/OT systems installed with considerations on the expertise and skills of the personnel onboard. If assistance from ashore is needed, details of how such assistance can be available should also be covered.

12

船舶网络风险管理实施注意事项
Key Points about Cyber Risk Management

国际海事组织第428(98)号决议建议，船舶应在不迟于2021年1月1日之后的首次DOC年度验证时，将网络风险管理的内容纳入公司安全管理体系并实施以抵御潜在网络攻击或者事故。

As previously stated, Resolution 428 (98) encourages administrations to take into account cyber risk management in SMS no later than the first annual verification of the company' s DOC after 1 January 2021.

公司在将船舶网络风险管理纳入船舶安全管理体系时，不仅应考虑到风险管理的通用性，还应考虑具体船舶的实用性，避免出现内容模糊、指导性差、不具有可操作性等现象。

Companies who are working on incorporating CRM in their safety management system should give thought to not only general rules but also the execution of these rules on specific ships. A precise, instructive, and practicable procedure will be preferable.

面对网络风险的威胁，船舶基本上处于未防范或低防范状态，出于现实状况需要，公司应加强船长和船员网络风险意识培训，督促船舶加强网络风险管理。

For ships under zero or low level of protection against cyber threats, companies should step up training of masters and crew members on cyber security awareness as part of a proactive management procedure.

船舶应结合自身的信息技术和操作技术特点，参照公司安全管理体系要求制定和完善适合本船的络风险管理程序，并在实施过程中通过有效的反馈机制不断进行评估以确保船舶网络风险管理的有效实施。

An appropriate level of cyber risk control should be in place in accordance with the characteristics of the IT/OT systems as required by SMS. It is also important to ensure the implementation through an effective feedback mechanism.

海事网络风险管理是一个持续改进和不断完善的过程，船舶应当定期及在网络事件发生后，评估网络风险管理的有效性，并基于评估结果进行相应的改进。

With CRM being a process of continuous improvement, evaluations on the effectiveness of CRM should be carried out subsequent to a cyber event on a timely basis.

中国船东互保协会
中国船级社