
**Industry Expertise:
Loss Prevention**

Maritime Cyber Risk Management Guidelines

This article is intended to assist members with the understanding and implementation of cyber risk management measures so that they can demonstrate that their procedures adequately address the cyber threat in accordance with the IMO and industry guidelines.



Captain Akshat Arora
Senior Surveyor

T +65 6506 2809

E akshat.arora@standard-club.com



Eleni Antoniadou
Claims Executive, Offshore Division

T +44 (0)20 3320 8864

E eleni.antoniadou@standard-club.com

Executive Summary

Technology has become essential to the operation and management of systems critical to the safety and security of shipping. This technological advancement also means increased exposure of the maritime sector to a greater risk of cybercrime.

Threats are posed by malicious acts (such as hacking or malware introduction) or by the unintended effects of benign acts (such as sharing user credentials or performing system updates by connecting to unsecured devices). In general, these actions reveal vulnerabilities that have to be addressed.

In 2017, the International Maritime Organization (IMO) adopted resolution [MSC.428 \(98\)](#) to require shipping companies to incorporate Maritime Cyber Risk Management into their safety management systems (SMS).

The IMO has set a timeline, by encouraging the flag states to verify this during their shipping companies' first Document of Compliance (DOC) audit after 1 January 2021. Although the IMO resolution only 'encourages' cyber risk management compliance, it is vital to understand that cyber security is essential to business and critical to the safety, integrity and reliability of maritime assets and operations.

The IMO guidelines on cyber risk management ([MSC-FAL.1/Circ.3](#)) provide five functional elements of the risk management framework: identifying risk, detecting risk, protecting assets, responding to risk and recovering from attacks. Based on these guidelines, shipping companies are recommended to undergo a cyber risk analysis to assess threats and vulnerabilities, as well as the impact of hackers on systems critical for the safe operation of their ships. Based on the risk analysis, shipping companies should implement mitigation strategies to strengthen assets both ashore and on board their ships.

Introduction

The maritime industry, like most other sectors, is increasingly dependent on digitalisation, connectivity and automation to improve its efficiency and reliability. Commensurate with the pace of this transformation is the increase in cyber threats.

As technology continues to evolve, the complex shipboard systems are more integrated than ever before. The risks, however, are dependent not only on systems and processes, but also on how they are used – the weakest link when it comes to cyber security is still the human factor.

The current pandemic has forced organisations and individuals to embrace remote work practices with even greater reliance on electronic systems. The crisis has also given an opportunity to malicious cyber actors to exploit the situation, as they seek to deliver malware and ransomware and to steal user credentials.

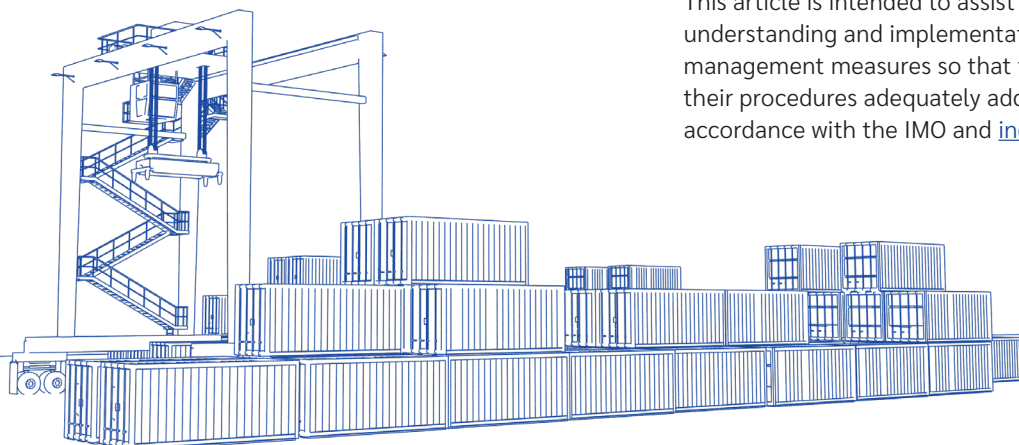
Cyber-attacks on shipping companies have been on the rise in the recent past. Likewise, there have been increasing numbers of incidents relating to interference with ships' navigation equipment. The potential consequences of such attacks may range from significant substantial disruption to financial losses and reputational damage.

This clearly demonstrates that cybercrime is an emerging threat, and unauthorised access or malicious attacks may have severe repercussions. As such, having proper cyber security management is a business-critical requirement.

Cyber risk management measures are required to be aligned with existing requirements contained in the ISM & ISPS Codes – the procedures relating to cyber risk management should be reflected in the safety management system (SMS) of the company, while the physical security aspects of cyber security should be addressed in the Ship Security Plan (SSP).

Even with the regulatory mandates, there is a difference between being compliant and being secure – it is not sufficient to just 'tick the box', shipping companies need to effectively control the risk.

This article is intended to assist members with the understanding and implementation of cyber risk management measures so that they can demonstrate that their procedures adequately address the cyber threat in accordance with the IMO and [industry guidelines](#).



Understanding the cyber threat landscape

The sophistication of some of the recent cyber-attacks signifies that the threat landscape is dynamic and evolving at an unprecedented pace.

Social engineering involves fraudulent emails or false websites that invoke emotions and entice victims to click on a malicious link or open a malicious file. There are typically three approaches that attackers adopt:

- a) They may impersonate a senior member of staff and ask the victim to transfer cash to an account for an urgent but previously undiscussed reason.
- b) They may try to get the victim to visit a website that they control so that the victim's computer gets infected with a virus.
- c) They may send an attachment (often password protected, with the password in the email) that includes the virus within it.

In such cases, common sense and treating unexpected emails with scepticism can significantly reduce risks. Some organisations may utilise security software to filter access to the internet. However, due to the size of the internet, it is impossible for these systems to correctly classify every possible website.

Shipping companies utilise a variety of software and if they are not sufficiently robust, they can be penetrated by malicious cyber actors to manipulate or steal data.

On board ships, legacy systems and/or unprotected networks may not have the defences, updates or design to make them cyber resilient – these systems were not built at the time to tackle the evolving challenges of connectivity. As such, there is a risk for ship systems with unknown or insecure connections to be easily accessed by adversaries who may then seek to monitor, disrupt or even take control of the critical equipment. Seafarers commonly use portable flash drives (USB sticks) and other mobile devices for the transfer of data, which are notoriously risky from a cyber security perspective.

However, more modern vessels are not necessarily more secure. Increased digitisation of vessels comes with an increased number of connections, which consequently increases the threat landscape. Further, ships with modern equipment could be considered potentially high risk from an information security perspective as they can hold large amounts of data, which can be easily lost or stolen.

The IMO guidelines identify a list of potential vulnerable systems on ships, which include, but are not limited to:

1. bridge systems
2. cargo handling and management systems
3. propulsion and machinery management and power control systems
4. access control systems
5. passenger servicing and management systems
6. passenger facing public networks
7. administrative and crew welfare systems
8. communication systems.

Threats such as the jamming and spoofing of global positioning systems (GPS) signals, manipulation of Automatic Identification System (AIS) data and vulnerabilities in other satellite-based tracking systems indicate that the exclusive reliance on such electronic systems could pose substantial challenge for the vessel's safe navigation.

The U.S. Department of Transportation's Maritime Administration Advisories (MARAD) recently issued an advisory ([2020-016-Various-GPS Interference](#)) covering multiple instances of significant GPS interference reported worldwide in the maritime domain. The U.S. Coast Guard Navigation Center (NAVCEN) has a dedicated [website](#) to receive reports of GPS interference and to share information about effective navigation practices.

Even though the Electronic Chart Display and Information System (ECDIS) complies with the IMO regulations, the technology itself has been identified as vulnerable to hacking – a number of these systems run with administrative rights and no password protection; hence, they can be easily tampered with. With physical access, a malicious person could use the USB slot to upload a virus, access the underlying operating system and/or spread malware/ransomware.

Similarly, there is a risk of viruses spreading into cargo and machinery systems from unsuspecting and insufficiently trained users in combination with unsecured networks or insufficiently protected use of portable storage devices, eg when an infected removable media is connected to the ship's loading computer to upload a cargo plan provided by the terminal, or when a service technician applies software updates on the machinery and propulsion control system by connecting their infected computer.

The risks are generally limited on standalone systems as compared to those connected with uncontrolled networks or directly to the internet, eg cargo management systems interfaced with pumps, valves or other shipment tracking (such as reefer container monitoring systems) and machinery systems integrated with remote condition-based monitoring will be more vulnerable to cyber-attacks. Given the rise in cyber-related incidents, it is imperative to seek solutions to manage the threat.

Industry guidelines

As per the IMO guidelines on maritime cyber risk management ([MSC-FAL.1/Circ.3](#)), one of the accepted approaches to achieve this is by comprehensively assessing and comparing a shipping company's current, and desired, cyber risk management postures. Such a comparison may reveal gaps that can be addressed to achieve risk management objectives through a prioritised cyber risk management plan.

The IMO guidelines are not prescriptive in how these recommendations should be implemented, but refer to the [Guidelines on Cyber Security Onboard Ships](#) (produced by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and the World Shipping Council), [US-NIST framework](#) and [ISO/IEC 27001 standards](#) as sources of additional guidance.

The five NIST Cyber Security Framework domains could be considered as a part of the risk management process:

- **Identification** forms the basis for understanding systems, data and capabilities that, when disrupted, pose risks to operations. It is also vital to define roles and responsibilities.
- **Protection** against cyber-attacks includes traditional forms of information assurance capabilities, development of contingency plans and implementation of training, policies and procedures.
- **Detection** focuses on rapid discovery of cyber incidents and is most effective when utilising advanced analytical techniques. Done right, it helps fight cyber-attacks by anticipating them before they start.
- **Response** is triggered when a cyber incident is imminent or active. The ability to continue operations uninterrupted during a cyber event is a key performance indicator for success.
- **Recovery** requires determining what is needed to support a return to normal operations, including disaster recovery, continuity of operations and effective communications.

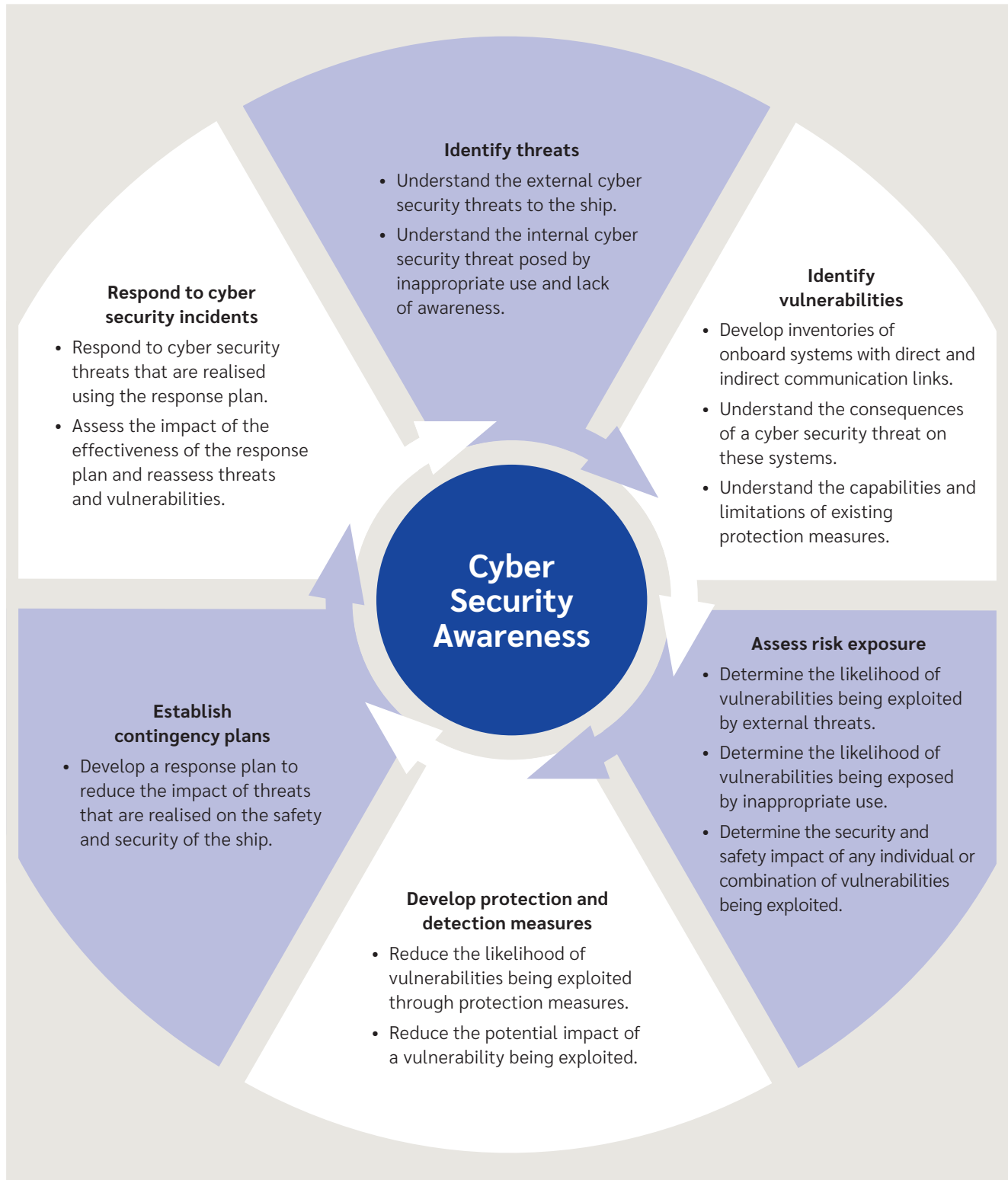
NIST Cyber Security Framework



Joint industry guidelines provide a clear mapping to the ISM Code and alignment to the NIST Framework: shipping companies need to understand the threats, identify

vulnerabilities, define internal processes, assign key roles and responsibilities, and develop contingency plans to detect and respond to a cyber event in a timely manner.

Cyber security awareness – Closing the loop (from Guidelines on Cyber Security Onboard Ships)

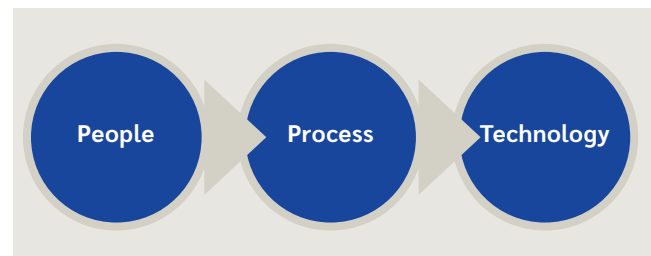


The other considerations that go into the preparation of a cyber risk management plan are national and international regulations (such as GDPR), commercial aspects and insurance implications.

- Rightship's inspection and assessment report (section 4.7) and the OCIMF Tanker Management Self-Assessment (TMSA-3), under elements 7 and 13, require shipowners and operators to incorporate cyber risk security policies and procedures within the shipping company and their vessels' operating procedures. TMSA-3 also relates to business operations under the Ship Inspection Reporting Program (SIRE). These requirements are generally more stringent than the IMO guidelines, as operators need to incorporate software and system configuration management procedures and demonstrate their involvement in the testing and implementation of up-to-date security technology. Even though compliance may be voluntary in principle, meeting these requirements is a fundamental commercial imperative for operators seeking regular charters.
- The Digital Container Shipping Association (DCSA) is an independent organisation consisting of major container shipping companies. It was established to drive technology standards and frameworks that will enable carriers to bring innovative solutions to market. As part of one of its initiatives, DCSA has published its [cyber security implementation guide](#).
- BIMCO's [cyber security clause](#) 2019 obliges the contractual parties to the charter to notify one another of any cyber security incident. The clause is designed to address situations where a party is struck by a cyber security incident and that incident affects the party's ability to perform its contractual obligations. It is drafted in a way for it to be easily incorporated into a wide range of contracts, acting as a means of allocating cyber security related responsibilities, liabilities and obligations for contractual performance.
- BIMCO and the International Chamber of Shipping (ICS) have issued a [Cyber Security Awareness Poster](#) and [Cyber Security Workbook for On Board Ship Use](#) with a view to supporting the ship's staff in case of a potential cyber incident. This document provides easy-to-use checklists on how to protect, detect, respond and recover from a cyber incident, and thereby offers a practical guide for the master and the officers.
- In April 2020, the International Association of Classification Societies (IACS) published [Recommendation on Cyber Resilience](#) to ensure a set of standardised criteria for new builds. It applies to the use of technical systems that provide important functions on board such as control, alarm, monitor, safety and internal communication.
- In addition to the above, members are recommended to refer to the flag state circulars, technical guidance issued by their classification societies and P&I club bulletins.¹

Building cyber security resilience

In the shipping industry, cyber risk management should focus on the security and resilience of integration, automation and network-based systems both ashore and on board the fleet. It should extend to include shipping companies' ability to withstand and swiftly recover from cyber events that disrupt usual business operations. Effective cyber security resilience is built on following mainstays:




People

The awareness gap is, perhaps, one of the main reasons why cyber threats and associated risks spread so quickly. There is a common misconception that cyber security is a matter for the company's IT department. IT departments do play an important role in implementing mitigation measures such as firewalls, anti-virus software and intrusion detection systems, and it is true that these defences assist in preventing many attempted attacks. However, the competency of all involved staff – both ashore and on board – is the primary defence against cyber risks.

The IMO guidelines ([MSC-FAL.1/Circ.3](#)) underline that effective cyber risk management should start at the senior management level and should be embedded as an organisational culture at all levels – ship and shore. They emphasise ensuring appropriate levels of cyber risk awareness at all levels of an organisation. The level of awareness and preparedness should be appropriate to the roles and responsibilities in the cyber risk management system.

Currently, there is no mandatory training requirement for cyber security under the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW); however, there are requirements in the ISM Code that staff should be qualified for their tasks. The training is a protection and control measure that forms the basis of cyber risk management – it helps to ensure that personnel understand how their actions will influence the effectiveness of the company's approach to cyber security.

Certain flag states may have additional requirements, eg the [UK's Cyber Security Code of Practice for Ships](#),



which applies to all UK-registered ships as well as foreign ships in UK waters. It requires a cyber security officer (CySO), who is responsible for all cyber security aspects on the ship and for liaising with the company security officer (CSO) to develop, implement, monitor and regularly review the Cyber Security Plan (CSP).

It is therefore recommended that all company personnel (ship and shore) should receive basic training on cyber hygiene in support of the company's cyber risk management policies and procedures. Personnel who have been assigned with cyber security duties should receive a type and level of cyber training appropriate to their responsibility and authority.

The Standard Club supports the [Be Cyber Aware at Sea](#) initiative and collaborated with Fidra Films in 2017 to launch a video to raise awareness of the increasing maritime cyber threat landscape. The [video](#) is freely available on [YouTube](#). Members are encouraged to distribute it to their fleets and reinforce its messages.

Processes

The requirement for the assessment and management of risks is fundamental to the ISM Code and a key element of any risk analysis process is to determine the likelihood and impact.

A company's SMS should include instructions and procedures to ensure safe operation of the ship and protection of the environment in compliance with the relevant international and flag state requirements. Bringing cyber risks into this viewpoint could be challenging as they are usually harder to quantify, understand and relate to the surrounding physical world.

For this reason, a key step in the cyber risk assessment process is to understand the potential impact. By incorporating a clear impact assessment in the risk analysis approach, there will be a better understanding of how losses relating to information confidentiality,² integrity³ and availability⁴ can further compromise safety.

In the context of cyber security, the likelihood of a cyber security incident is independent of the frequency of past occurrence(s). Instead, it would depend on the following factors:

- Discoverability – How easy would it be for an adversary to discover the vulnerability of an asset? This is dependent on the availability of information about the vulnerability and the exposure of the vulnerable asset.
- Exploitability – How easy would it be for an adversary to exploit the vulnerability of an asset? This is dependent on the access rights, complexity, as well as the technical skills required to carry out the attack.

- Reproducibility – How easy would it be for an adversary to reproduce the attack on the asset? This is dependent on the complexity of the exploit customisation and the environmental conditions required to carry out the attack.

For ease of comparison between cyber and non-cyber related risks, it is recommended to use the same matrix and rating scales as for other safety/environmental risks.

It is essential to understand that the risk assessment process is not a one-time exercise. As cyber threats and vulnerabilities are constantly emerging, process effectiveness should be reviewed regularly.

The risk analysis process needs to be continuously updated with the implementation of up-to-date protection and detection measures that reduce the likelihood and impact of any cyber security incident.

Technology

The right solution for each organisation will be different. To assess the risks, it is essential for all companies to evaluate their information technology (IT) and operational technology (OT) system capabilities.

Information technology (IT) covers the spectrum of technologies for information processing, including email systems, planned maintenance systems, procurement systems, crew welfare systems, electronic manuals and certificates, etc.

Operational technology (OT) encompasses hardware and software that monitors and manages physical equipment and processes, such as bridge navigation systems, cargo handling systems, propulsion and machinery management systems, access control systems, communication systems, etc.

In general, we can say that while OT systems control equipment, IT systems manage data.

Traditionally, OT and IT systems have been separated, but with the internet, these are increasingly integrated. This means that any cyber-attack could have an immediate and widespread impact. Disruption of OT systems may impede the ship's operation or cause risk to the safety of life, property and environment, while disruption of IT systems could lead to significant risks ranging from reputational damage, legal disputes and financial losses.

The IMO recommends a holistic approach to maritime cyber security, ie both the IT and OT systems should be addressed in the cyber risk management plan and appropriate defence measures should be established against cyber incidents involving either of these.

Mitigation of risks

The company's mitigation strategy to counteract cyber threats should be a multilayered approach comprising protection measures that consider the role of people, processes and technology:

People

- Understanding what can go wrong and how
- Understanding the necessary actions that must be implemented to establish and maintain an agreed level of cyber security
- Understanding how to identify cyber threats and how to respond
- Running virus scans on any files and removable drives that access shipboard computers
- Only opening emails and attachments from senders that are known and trusted
- Reporting suspicious or unusual problems
- Knowing what to do if important IT/OT systems do not work – where and how to get assistance
- Knowing what redundant controls and manual overriding possibilities exist in the OT systems to prevent an incident
- Restricting connection of personal laptops, tablets, removable media or phones with the ship's operational systems.

Processes

- Procedures on taking backups and applying system updates – manually by a portable storage device, or remote or automatic updates via direct internet link?
- Data management – ensuring adequate protection (encryption) and retention of data based on the sensitivity of the information
- Software management:
 - Keeping unauthorised software away from the ship's systems
 - Requiring software updates, including security patches, to be applied and tested in a timely manner, by a competent person.
- Password management:
 - Ensuring that default passwords are changed after initial log-in
 - Ensuring that common/shared usernames and passwords are not used
 - Requiring minimum length (at least 8 characters) and complexity (eg uppercase characters, lowercase characters, numbers or symbols)
 - Deleting the user accounts of colleagues and crew who have left

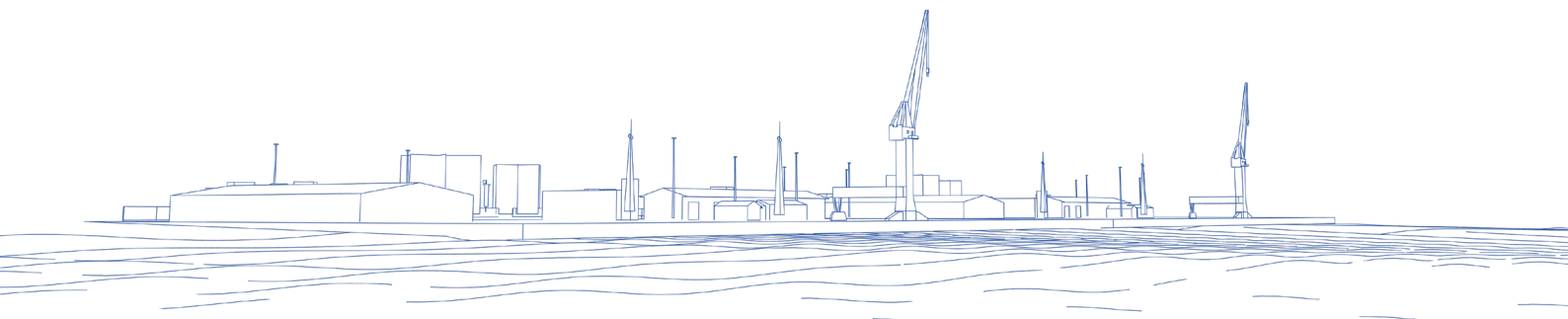
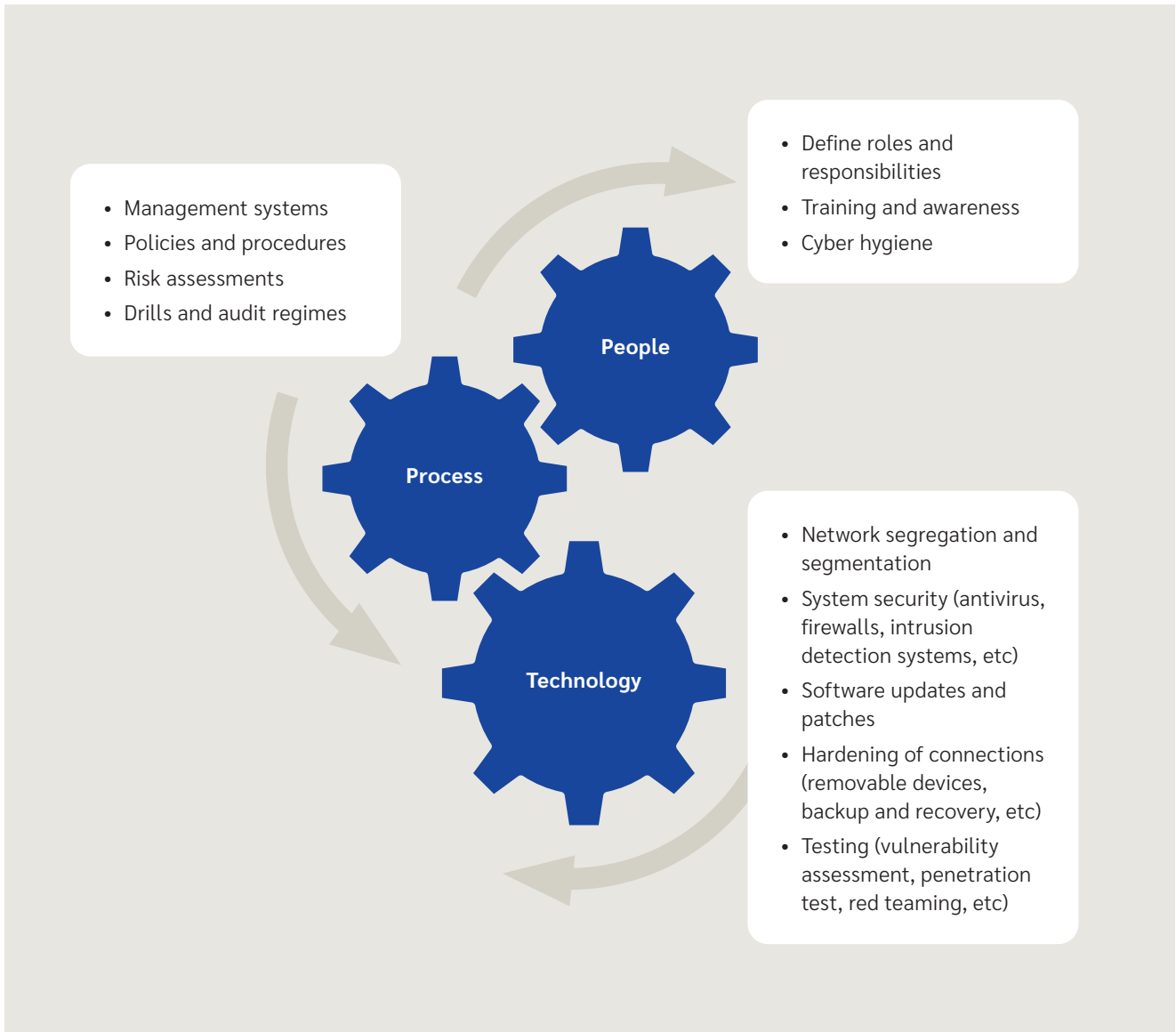
- Management of removable media (eg USB keys, external hard drives, CDs, etc):
 - Restricting/limiting the types of media that can be used and types of information that can be transferred
 - Improving the protection and ensuring the integrity/security of the device
- Communication and media management:
 - Setting protocols and channels for communication between the ship and the shore side
 - Segregating official and operational systems from personal and recreational use computers
 - Ensuring that critical work-related information is not shared on social media or personal email
- Incident management:
 - Reducing impact and restoring systems as soon as those have been attacked (business continuity)
 - Sharing lessons learnt from the incident to prevent the recurrence of similar incidents.

Technology

- Upgrading outdated systems and legacy technology, and insecure and unencrypted connections to ensure appropriate infrastructure is employed
- Ensuring appropriate support is available to maintain system security and performance – antivirus, firewalls, intrusion detection systems, software whitelisting, content filtering, etc
- Maintaining systems for authentication and authorisation of users to ensure appropriate access to necessary information. Reviewing access privileges to ensure that they are consistent with the individual's roles and responsibilities
- Maintaining segregation and segmentation of networks – critical systems should operate over a segregated infrastructure
- Monitoring and reviewing the effectiveness and robustness of barriers – functional testing, vulnerability assessments, penetration testing, red teaming, testing recovery plans, drills and audits.

On board ships, the best approach should be driven by maintaining the basics. Seafarers are not expected to be cyber experts, but the appropriate measures can be established easily by raising awareness, developing a cyber sense, maintaining cyber hygiene and following correct procedures.

Multilayered approach to cyber risk management



The club's perspective

There is no express cyber exclusion in the club's rules and cover will respond to P&I liabilities, but only where the war risks exclusion is triggered. (Do, however, note the limits of cover in relation to paperless trading under rule 5.17.) For instance, an incident caused by the malfunction of a ship's navigation or mechanical systems due to a cyber-attack could lead to a third-party liability. In such cases, standard P&I cover will respond in the usual way, unless the act can be characterised as terrorism or war risk (which are excluded under the club's rules). Where there is a dispute as to whether an act constitutes an act of terrorism, the decision will be referred to the club's board.

In the event the cyber-attack is an act of terrorism or an excluded war risk, the club's P&I war risks cover would respond excess the primary P&I war risks cover, except in the event that it arises out of the use of a computer virus for inflicting harm. In the event of a computer virus used to inflict harm, owners can get limited cover within the scope of biochemical risks inclusion cover.

More widely, it is an underlying condition of insurance with the club that every ship complies with all statutory requirements and maintains the validity of all certificates of the ship's flag state. Note that the relevant rule (r. 15.1) expressly refers to the ISM Code, which will include the requirements for cyber security from 1 January 2021.

Consequently, given that there could be cases where parties seek to argue that a claim arose because of an inadequate level of cyber preparedness, it is therefore vital to be able to demonstrate that all reasonable steps have been taken to manage cyber risks in accordance with the provisions of the ISM Code. Of course, there will be a variety of ways to comply with these requirements and different flag states will have different criteria for their DOC/Safety Management Certificate (SMC) auditors when reviewing these procedures. It will be for the individual clubs to evaluate the risk, and they may choose to ask additional questions regarding compliance and adherence to best practice (eg BIMCO Cyber Security Onboard Ships).

Naturally, each case will be dependent on its facts and will be dealt with on a case-by-case basis, since the cover position will depend on the factual background of each case.

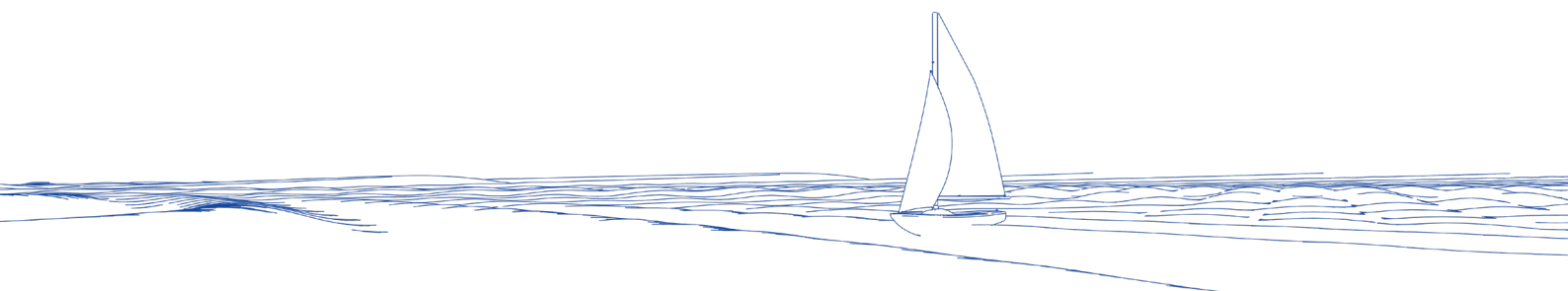
There could be incidents that do not incur third-party liabilities and are therefore not covered under the club's rules – for example, financial loss caused by ransomware or theft of data leading to repairs, fines and litigation. Some of these costs might come under a defence (FD&D) cover, but the key point is to assess the wide variety of risks and to focus on any insurance gaps that need to be filled.

Conclusion

Cyber risks are becoming an increasingly prevalent topic, and there is a wide range of comprehensive, informative and detailed guidelines available to assist members in developing a resilient approach to cyber security on board their ships.

With just a few months left until 2021, compliance with the upcoming regulations will require more than updating the SMS. Members are recommended to consider their exposure and address cyber threats in a systematic way, as part of the overall operational risk picture. Based on a systematic assessment, they should seek ways to efficiently close cyber security gaps by supporting the development of improvement plans, updating systems, increasing awareness and enhancing procedures.

- 1 <https://standard-club.com/media/2767840/cyber-risks-and-pi-insurance-implications.pdf>
<https://standard-club.com/media/2767719/cyber-security.pdf>
<https://standard-club.com/media/2608580/cyber-security-risks-for-charterers.pdf>
<https://standard-club.com/media/2533617/cyber-risks-and-pi-insurance-implications.pdf>
- 2 Loss of confidentiality is the unauthorised disclosure of information.
- 3 Loss of integrity is the unauthorised modification or destruction of information.
- 4 Loss of availability is the disruption of access to or use of an information system.



Keep up to date by visiting the Knowledge Centre section on our website standard-club.com

 **@StandardPandi**

 **@StandardClubPandi**

 **The Standard P&I Club**

The Standard Club Ltd is incorporated in Bermuda (No. 01837), authorised and regulated by the Bermuda Monetary Authority. Registered office: Swan Building, 2nd Floor, 26 Victoria Street, Hamilton HM 12. The Standard Club Ltd is the holding company of The Standard Club UK Ltd, The Standard Club Ireland DAC (both managed by Charles Taylor & Co. Limited) and The Standard Club Asia Ltd (managed by Charles Taylor Mutual Management (Asia) Pte. Limited).

The Standard Club UK Ltd is registered in England, No.17864, at The Minster Building, 21 Mincing Lane, London EC3R 7AG, authorised by the Prudential Regulation Authority FRN 202805 and is regulated by the Financial Conduct Authority and the Prudential Regulation Authority. The Standard Club Ireland DAC is registered in Ireland, No. 631911, at Fitzwilliam Hall, Fitzwilliam Place, Dublin 2; authorised and regulated by the Central Bank of Ireland. Managers: Charles Taylor & Co. Limited. Registered in England No. 02561548 is authorised and regulated by the Financial Conduct Authority FRN 785106. Registered office: The Minster Building, 21 Mincing Lane, London EC3R 7AG.

The Standard Club Asia Ltd. is a company incorporated in Singapore with limited liability (No. 199703224R), authorised and regulated by the Monetary Authority of Singapore. Managers: Charles Taylor Mutual Management (Asia) Pte. Limited, a company incorporated in Singapore with limited liability (No. 199703244C). Registered office: 140 Cecil Street, #15-00 PIL Building, Singapore 069540. The Standard Club Asia Ltd (Hong Kong Branch) is authorised and regulated by the Hong Kong Insurance Authority, registered in Hong Kong (No. F24636). Managers: Charles Taylor Mutual Management (Asia) Pte. Limited (Hong Kong Branch), registered in Hong Kong (No. F24645). Registered offices: Suite A, 29/F 633 King's Road, Quarry Bay, Hong Kong.