Department for Transport

Cyber Security Code of Practice for Ships

July 2023

Department for Transport
Great Minster House
33 Horseferry Road
London SW1P 4DR

This publication is also available on our website at
www.gov.uk/government/organisations/department-for-transport

Any enquiries regarding this publication should be sent to us at
www.gov.uk/government/organisations/department-for-transport

Contents

1. Foreword 4
2. Introduction 6
3. Introducing the Cyber Security Top 10 for Shipping 10
4. Cyber Security Top 10 for Shipping 14
5. Conclusion and Call for Action 50
Annex A: Terms and definitions 51
Annex B: Cyber Security and CSAs 54
Annex C: Developing a Ship Cyber Security Plan 56
Annex D: Cyber Security Tools and Software 66
Annex E: Maritime Autonomous Surface Ships 68
Annex F: Bibliography and References 71

1. Foreword

The Department for Transport originally issued the Cyber Security for Ships Code of Practice (COP) in 2017 with the support of the Institute of Engineering Technology (IET) and Defence Science and Technology Laboratory (DSTL). The document was designed to codify the recommendations for cyber security; providing guidance to a range of users from board level through to day-to-day ship operations. It aimed to provide a management framework for cyber security across Information Technology (IT), Operational Technology (OT) and Communications Technology used within the industry.

This new release of the COP aims to support raising awareness of cyber security good practice in the industry. The following changes have been made:

- Cyber Security Top 10 for Shipping produced. This is strongly aligned to the NCSC's Cyber Assessment Framework.
- Baseline Risk Assessment of the shipping industry undertaken, see Risk Management Process (A2.a).
- High-level analysis of common security controls conducted. This looks at cost and effectiveness and can be found throughout Cyber Security Top 10 for Shipping.
- Guidance on assessing open-source or vendor-bought software, see Annex D: Cyber Security Tools and Software.
- Forward-look towards the risks to Maritime Autonomous Surface Ships, see Annex E: Maritime Autonomous Surface Ships

The importance of cyber security has been increasingly recognised as cyber attacks grow in prominence and severity [1]. Ships are becoming increasingly automated and dependent on digital technologies to support their operation [2]. This will likely lead to additional cyber security risks and heightened impact in the event of a successful cyber attack.

Figure 1: Statistics on UK's Maritime sector [92]

An island nation with global interests, like the United Kingdom, is highly dependent on its maritime sector, with 95% of goods entering the country over maritime routes. Part of maintaining this economic prosperity will involve the sector equipping itself to defend against emerging cyber threats.

2. Introduction

Background

Cyber security is an ever-changing landscape, and therefore the shipping industry needs to be aware of developments. New technologies and evolving user behaviours require regular evaluation of the security controls in place.

Since the previous COP was issued the threat landscape has changed, for example ransomware attacks increased by around 60% in 2022 compared to 2020 [3] [4]. In 2022, there were at least fifty-seven known ransomware attacks on the maritime industry [5] reported in the press, with the likelihood that some remain unreported. Many attacks appear to have been related to IT security and perpetrated through supply chains. The significant growth in ransomware, and the attack vectors leveraged, highlights the importance of managing supply chains and basic cyber hygiene for organisations.

Engaging with published guidance will provide a strong foundation for any Cyber Security Plan; protecting the organisation and its assets against cyber threats. This COP has been written to provide clear and concise guidance to the user on understanding and managing their cyber risk. It will help tackle underlying concepts and improve the cyber security posture of a maritime organisation. Further information is available from many sources, see Maritime Security Regulations in the UK and Annex F: Bibliography and References.

This document is intended to complement existing standards and guidance within maritime security. It advocates a holistic approach to:

- The cyber security of a ship;
- Managing security risks within the overall organisation;
- Protecting and building resilience against cyber attacks by introducing maritime-appropriate controls;
- Detecting and responding to cyber attacks in a timely manner;
- Recovering quickly should an attack happen.

This will help maritime organisations embed cost-effective cyber security management into their ships and fleet as part of standard business process.

This COP does not consider the cyber security of the ports and port facilities to which the International Ship and Port facility Security (ISPS) [6] Code applies. The UK Department for Transport (DfT) published separate guidance on ports and port systems during 2016, and updated in 2020 [7].

Who should use the COP

This COP should be used by those responsible for cyber security within maritime organisations to protect ships (whether underway, docked or berthed), persons, cargo, cargo transport units and ship's stores from the risks of a security incident. It may also be of interest and of relevance to organisational roles involved in:

- The financial and operational management of a ship or fleet;
- Ownership of the ship;
- Insuring ships and their cargoes;
- Contractual arrangements with third parties;
- Determining policies relating to acceptable cyber security behaviours;
- The specification, design, construction and maintenance of ship(s);
- The specification, design, development, integration, commissioning, operation and maintenance of maritime systems, including associated software and technologies;
- Management of specific security tasks, including incident response and the handling of security breaches.

Maritime Security Regulations in the UK

In December 2002 the International Maritime Organisation (IMO) adopted a series of changes to the SOLAS Convention (Safety of Life at Sea Convention), introducing the International Code for the security of Ships and Port Facilities, referred to as the International Ship and Port Facility Security (ISPS) Code. The ISPS Code was historically implemented in UK through the EU regulation on enhancing ship and port facility security (725/2004). The Ship and Port Security (Amendment etc.) (EU Exit) Regulations, 2019, came into force on EU exit day (31st January 2020). Currently, SI 2019 No. 0308 [8] amends 2004/0725 (Regulation), SI 2004 No. 1495 [9], SI 2009 No. 2048 [10] and revokes 2008/0324 (Regulation).

Under the ISPS Code a ship is required to have a Ship Security Plan (SSP) which is derived from a Ship Security Assessment (SSA) of the security of the ship. The SSP is principally focused on minimising and managing physical and personnel risks, e.g., piracy and hazardous materials transported aboard.

The IMO introduced cyber security guidance in 2017, under MSC-FAL.1-Circ 3 [11] and Resolution MSC.428(98) [12] which recommended that cyber security should be a part of ship safety management systems. The resolution also encourages Flag States to ensure that cyber risks are appropriately addressed in Safety Management Systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021. The IMO has placed cyber security as a safety practice under the International Safety Management code. This is to reflect the overlap between security, safety, and the complementary nature of cyber security in the safe operation of a ship. The UK has recommended cyber security to be covered under the Ship Safety Management System (SMS) since the previous version of this COP was released in 2017.

Although the ISPS code or UK regulations do not require cyber security to be included within the SSP documents, it may be good practice to maintain Cyber Security Plans (CSP) and Cyber Security Assessments (CSA) as annexes. This will ensure cyber security is covered alongside other areas of risk. In line with security best practice, cyber security risks and plans should be reviewed at least annually, after an incident, or after new threat intelligence is published. This is aimed at reducing the cyber security risks to the ship and protecting its OT and IT systems.

This COP has been written to support organisations in producing their CSPs and CSAs. It makes extensive reference to good practice guidance such as NCSC's CAF, which aligns to the Government's Cyber Security Strategy for 2022-2030 [13], and the Government's National Strategy for Maritime Security [14].

The document also references industry guidance such as the 'Guidelines on Cyber Security Onboard Ships' (GCSOS) produced and supported by The Baltic and International Maritime Council (BIMCO), Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC) [15].

Case study: Ransomware attack

Recently a company operating several vessels experienced a ransomware attack. Attackers leveraged a vulnerability in a supplied service to gain remote access and compromise shore-side IT systems. This hugely impacted communication with external parties and operational timelines.

Although many systems were affected, the company had taken sufficient backups and was able to restore their systems without paying the ransom.

It took 6-8 weeks to restore systems to full working order and the incident caused significant financial impact. The company has not calculated the quantitative value of the disruption of the incident but in the reasonable worst-case scenario losses may have been as high as £10 million.

This type of incident demonstrates the importance of taking regular backups and storing them offline. It also demonstrates the need to consider risk holistically and to assess and manage the risk that suppliers introduce to your system. Controls like audits and adding security clause to contracts can further help mitigate risks in this area.

Source: Company wishes to remain anonymous.

3. Introducing the Cyber Security Top 10 for Shipping

Overview

Cyber security is about the management of threats and risks to information and technology. The end goal will vary depending on the environment under review, however commonly cyber security works to protect the confidentiality, integrity and availability of information and technology assets to safeguard the economy, privacy of individuals and at times, people's lives.

The maritime sector plays a critical role in supporting the UK. Ensuring the industry is cyber secure is important as the economic impact of a cyber attack on shipping could be large. Poor cyber security within the maritime sector can have significant costs, harms and disadvantages to organisations and the UK more generally.

Cyber Security Top 10 for Shipping

The Cyber Security Top 10 for Shipping "Top 10", see Table 1, has been developed to encourage wider adoption of good cyber security practices. They are easy-to-read concepts that cover the most important aspects of cyber security. Adopting them will both reduce the likelihood of successful cyber attacks, and their impact.

The Top 10 is designed to highlight and support practical steps that can be undertaken to embed good cyber security practice within the shipping industry. It is a summary of the information provided through the rest of the document, grouping cyber security aspects under ten headings. These cyber security concepts are broadly based on the NCSC's 10 steps to cyber security [16], NCSC's Cyber Assessment Framework (CAF) [17] and government guidance on how large to medium organisations should protect themselves in cyberspace. They have been customised for the maritime sector through stakeholder engagement and industry standards, literature and existing guidance.

ID	Top 10
1	Know your data
2	Understand your risks
3	Manage your assets
4	Manage Identity and access
5	Know your supply chain
6	Train your users
7	Manage your vulnerabilities
8	Build your resilience
9	Monitor your systems
10	Manage cyber incidents

Table 1: Cyber Security Top 10 for Shipping

Document structure

Where a section is related to the Top 10, this is clearly indicated using the coloured, numbered logo. A reference to further information can also be found on the right-hand side of the logo. This includes mapping to standards such as CAF [17] and NIST [18] controls.

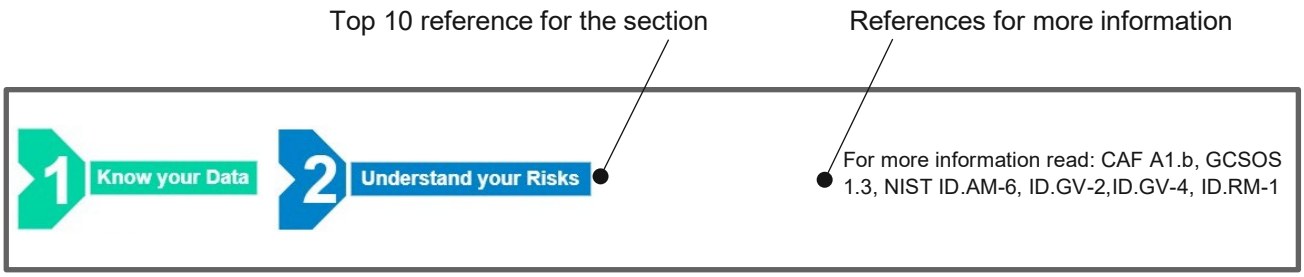


Figure 2: Example of a heading with its Top 10 reference

The Department for Transport can make available several posters of the Top 10 that may support organisations' awareness of the Top 10.

Each Top 10 section is broken down into a number of subsections, or measures, that highlight various factors within the Top 10 heading. These measures are heavily influenced by the NCSC's CAF [17] and as such the CAF reference has been retained where applicable.

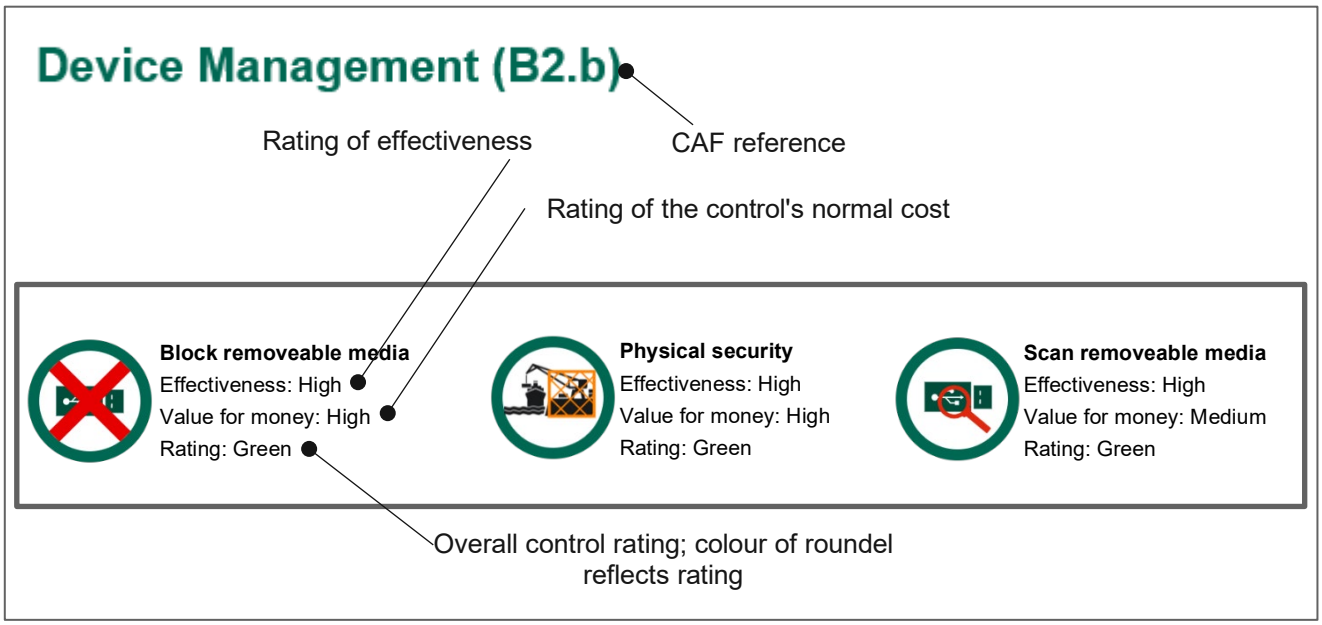


Figure 3: Example showing the Top controls for a heading

Under each measure you will find an analysis of controls mentioned within the measure, or other supporting controls. For example, the Device Management section contains 3 controls, see Figure 4. A scale of low, medium, high is used to rate each attribute.

Effectiveness is rated:

- High - if the control goes a long way in mitigating relevant attacks, and mitigates a broad range of attacks;
- Medium - if the control mitigates specific attacks well but not a broad range, and an attacker may be able to bypass the control;
- Low - if the control can only be partially technically enforced and would not fully mitigate an attack on its own. The control may be reliant on policy and not technically implemented.

Value for money is rated:

- High - if the control is low-cost and highly effective against the relevant risk;
- Medium - if the control is moderate-cost with some effectiveness against the relevant risk;
- Low - if the control is high-cost and has some effectiveness against the relevant risk.

The final 'Rating' is provided as a combination of the effectiveness and value for money. The following colour coding is used for each roundel:

- Green, final rating = optimised control with excellent risk reduction potential if implemented correctly;
- Yellow, final rating = better control than the baseline with a good risk reduction potential, where implemented correctly;
- Blue, final rating = good control baseline which likely reduces exposure to high risks if this control is implemented correctly.

These can be used as a starting point, however, ultimately the security context of the ship, organisation and risks will inform which controls are most appropriate.

Meeting the Top 10 and CAF

Top 10 covers a broad range of cyber security measures and implementing them will strongly improve the cyber security baseline for organisations. Once an organisation has got a good handle on the Top 10 measures, they may take the decision to continue improving their security posture and to aim at CAF compliance.

Whilst there is no requirement to demonstrate CAF compliance, it will provide assurance that your cyber security is holistic and aligned to industry and government recommendations.

4. Cyber Security Top 10 for Shipping

1. Know your Data

Data is an important business asset. Understanding the data that an organisation collects, handles and produces within its systems and operations provides a picture of the information assets that it holds. It is crucial to work out the data which is critical for the operation of the organisation, as this will have the biggest impact if it is breached. OT systems process different data types; from environment variable through to digital metrics. To help prioritise your OT systems, you must first understand the data they process and their operational environment. This will provide a foundation to support effective management of the data that the systems receive, and understand the risks to safety and security in the event of an attack.

Important controls from the CAF to consider in this concept include:

- Roles and Responsibilities (CAF reference: A1.b)
- Understanding Data (B3.a)
- Secure by Design (B4.a)

Roles and Responsibilities (CAF reference: A1.b)

For more information read:
CAF A1.b, GCSOS 1.3, NIST ID.AM-6, ID.GV-2,4, ID.RM-1, ISO27001 5.2, 5.3, 5.4

No organisation can operate securely without clear guidance and leadership. This is needed at every step of operation and will affect every employee to a greater or lesser extent. Clearly allocated cyber security roles, responsibilities and tasks will aid this and drive the security culture of your company. Leadership should make business decisions such as determining what data is critical to the operations and success of the business or what cyber risks the business can tolerate as part of its operations.

An organisation's board may choose a variety of approaches to address this, for example the Chief Information Security Officer (CISO) may be appointed and is the nominated board member who holds responsibility for cyber security operations. Alternatively, the organisation may require its business area leads to report on security on a regular basis.

There is no one-size-fits-all approach. The key requirement is that the cyber security of the organisation is "owned" by the board.

Various roles will be required to ensure cyber security onboard a ship. Roles are likely to include a Ship IT Manager and Ship Security Officer. Roles should cover all system areas; OT, IT, onboard systems, port systems, third party assets and crew training. For smaller companies one individual may fulfil multiple roles, nevertheless separation of roles is important where possible. For example the IT and Security Officer should be separate persons, preventing the IT manager authorising changes to security protocols without the Ship Security Officer agreement.

A good test of whether roles and responsibilities are understood is: can they be documented? This will help avoid duplication and confusion between roles. GCSOS Figure 3 [15] provides a helpful matrix of the various cyber security roles you may employ within your organisation.

Understanding Data (B3.a)

For more information read:
CAF B3.a, GCSOS 2-5, NIST ID.AM-3, ID.BE-4, ID.RA-4, PR.DS-3, PR.IP-6, PR.PT-1, ISO27001 5.9, 5.12, 5.13, 5.19, 5.31

Data is an important part of any business and will no doubt be collected by your company for a variety of reasons, e.g., sensor data or personal user data. It is important that these reasons are valid and updated as the business changes. This will ensure that you understand what data you have, so you know what data you are responsible for. Some data will not be critical, but other data will have a big impact on the organisation if not secured e.g., card payment details. If critical data is breached you may suffer large regulatory fines and reputational damage. Annex B:Cyber Security and CSA lists a number of areas where the impact may be felt.

Consider how your data is stored: think about how and where it can be stored, as it can be very large as well as private in nature. Understanding this will impact the security controls you put around it e.g., encryption at rest and the storage location. You should also consider how available to make the data and what its use cases are. Security controls will need to take this into account. When you process personal data, you must ensure your practice is in line with GDPR [19].

It is important to understand operations, access needs and what would happen if it was not available, altered or stolen. Ask some simple questions:

- What data do you process?
- What would happen to your business if you did not have access to this data?
- Which systems do you store and process the data on?
- Do you have a classification system for your data, e.g., confidential, personal, sensitive?
- Do you have an information asset register?

If you are struggling to identify data assets, it might be helpful to look at each piece of equipment or system in turn, e.g., what data does the ECDIS system require to operate?

Encryption and VPNs

For more information read:
CAF B3.b and B3.c, NIST PR.DS-1,2,5, PR.PT-4, DE.AE-1

Encryption is the process of scrambling data in such a way only authorised parties can unscramble the data to read the information. Using encryption means that if information falls into the wrong hands it cannot be read.

When data is in transit e.g., travelling over a network, encryption is an important way to secure it from interception or impersonation. Encryption makes these attacks harder as the attacker needs information about how the encryption is achieved to understand the data or produce impersonated data.

If you encrypt data in storage, then the encryption algorithm should be suitably strong to prevent unauthorised access/decryption. Several widely used algorithms have been cracked, and so these should not be used e.g., SSL 3.0, MD5, TripleDES. Algorithms that are still considered secure (at time of writing) include TLS v1.2/v1.3, AES, twofish, SHA-2 or SHA-3 among others.

A Virtual Private Network (VPN) can be used for protection against eavesdropping and can give users encrypted communications over a network. It is often used to support remotely operated device access to a corporate network. For more information on VPNs and communication encryption, the NCSC has guidance available [20].

Top controls

Encrypt data and comms
Effectiveness: High
Value for money: High
Rating: Green

Virtual Private Network
Effectiveness: High
Value for money: Medium
Rating: Green

One-way comms
Effectiveness: Medium
Value for money: Low
Rating: Yellow

Secure by Design (B4.a)

For more information read:
CAF B4.a, NIST PR.AC-5, PR.DS-7, PR.IP-2, PR.PT-4, ISO27001 6.7, 8.20, 8.21

Secure by design is about factoring in security from the start of creating a network or system. This may include improving the ease of recovery, monitoring of systems, or limiting usage of Application Programming Interfaces (APIs).

Considering security from the offset creates a more robust system than only considering security before the system goes live. For example, when securing a system, you will need to think about:

- Secure coding;
- Architecture;
- Maintenance;
- Deploying updates;
- Testing releases.

The CAF refers to content-based attacks (that is any data entered into a system). You should mitigate all inputs as every entry point is a potential vector for attackers to inject code. One mitigation control is limiting the characters that users can enter and stripping unnecessary characters from input.

Network segmentation and Firewalls

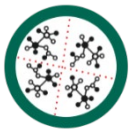
Network segmentation is an example of secure by design. By breaking up the network it reduces the potential attack surface as there are fewer systems reachable from any point in the network.

Network segmentation involves separating a network by isolating it into clusters of devices and systems that are logically similar. For example, this can be done by separating your onboard Wi-Fi from an OT network. Often this is done by grouping them per the type of information they hold. This way an attack on one part of the network would not impact all information systems.

Top controls

Block remotely available services
Effectiveness: High
Value for money: High
Rating: Green

Firewall
Effectiveness: High
Value for money: High
Rating: Green



Network segmentation
Effectiveness: High
Value for money: High
Rating: Green

2. Understand your Risks

Risks are everywhere and affect all assets and systems. Understanding the data and systems within an organisation is crucial to understanding its risks. Documenting the cyber risks then allows organisations to track them. It is important to consider your operating environment and recognise that vessels operate in a range of surroundings (e.g. in coastal waters, in unfriendly waters, in port or in open ocean). The environment should be factor into your risk assessment and may result in additional controls to ensure safe operational of the vessel against cyber attacks.

Organisations may benefit from using their existing business risk evaluation techniques on cyber so that financial and health and safety ship operational risks are all rated on a consistent scale.

Important controls from the CAF to consider in this concept include:

- Roles and Responsibilities (CAF reference: A1.b)
- Risk Management Process (A2.a)
- Secure by Design (B4.a)

Risk Management Process (A2.a)

For more information read:
CAF A2.a, GCSOS 2-6, NIST ID.RM-1, ISO27001 5.7, 5.24, 5.25, 5.26, 5.27, 5.29

Cyber security is all about risk management; identifying what risks an organisation faces, and dealing with them. Top 10 is designed to improve an organisation's understanding of risks, and help mitigate those common across the shipping sector. Consequently, companies who manage their risks well are likely to find they already comply with much of the Top 10, and therefore the CAF too.

Risks can be measured quantitatively (e.g., given a monetary value) or qualitatively (e.g., a subjective value based on a consistent scale, such as 1 to 5). With both approaches you should provide justifications for any assumptions you have made. Risk management within the shipping industry is generally undertaken qualitatively, in line with the ISPS code approach within a SSA. However, it may be useful to also consider a quantitative approach to provide business context on the financial costs associated with risks.

GCSOS sections 2-6 contains extensive guidance on how to construct your risk assessment. The main stages are:

Figure 4: Stages of risk management

A key part of the risk assessment is understanding the impact a vulnerability may have if exploited. Ships have both IT and OT systems, which have different cyber security postures. For example, the availability and safe operation of OT systems such as ECDIS or power management is of greater importance than the public WiFi network. There are several properties that factor into the cyber security of the ship and these should be considered when assessing the cyber security risks:

1. Safety is the property of ensuring systems are not hazardous to humans and property.

2. Availability is the property of ensuring information and systems can be accessed when they need to be used.

3. Resilience is the property of ensuring failure can be recovered from, with limited-to-no impact on operations.

4. Integrity is the property of ensuring information and systems are consistent and are not corrupted.

5. Operability is the property of ensuring a system is in a usable and functioning condition and is reliable when in use.

6. Confidentiality is the property of ensuring that information remains private.

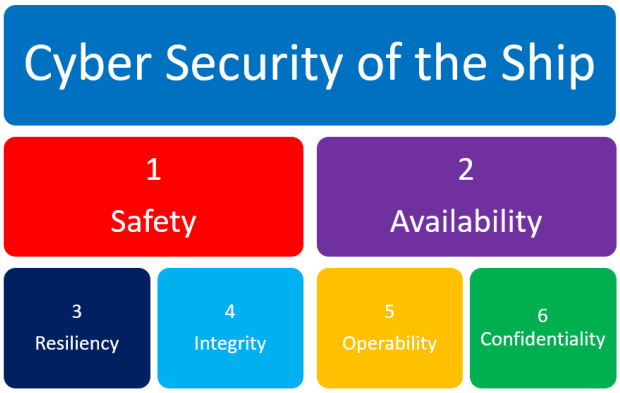


Figure 5: Visualisation of important properties for cyber security onboard ships

The updates to the COP include a risk assessment of the maritime sector that was conducted by an external consultancy. The results of this risk assessment can be shared by the DfT. It assessed the top cyber security risks to UK shipping as:

- Supply chain risk - attacks on suppliers and vulnerabilities built into supply chain components which can later be exploited may result in a risk that affects the overall function of the ship.
- Ransomware - ransomware may be installed on the vessel or attack the shoreside IT and lead to loss of critical information on a vessel (if data is unrecovered). If staff cannot access systems this may also impact a ship's OT so that it cannot operate safely.
- Poor software, firmware and hardware maintenance practices lead to risks that unpatched vulnerabilities in OT and IT may be used by an attacker to compromise the safe operation of a ship.
- Unsolicited emails used for phishing, spear-phishing are a route for credential harvesting for potential subsequent attacks, and may be used to compromise ship and ship-support systems.
- Escalation of privileges and compromise of credentials is generally plausible within the industry. This result from heavy reliance on maintenance staff from suppliers, use of common default credentials, password sharing and poor access control.

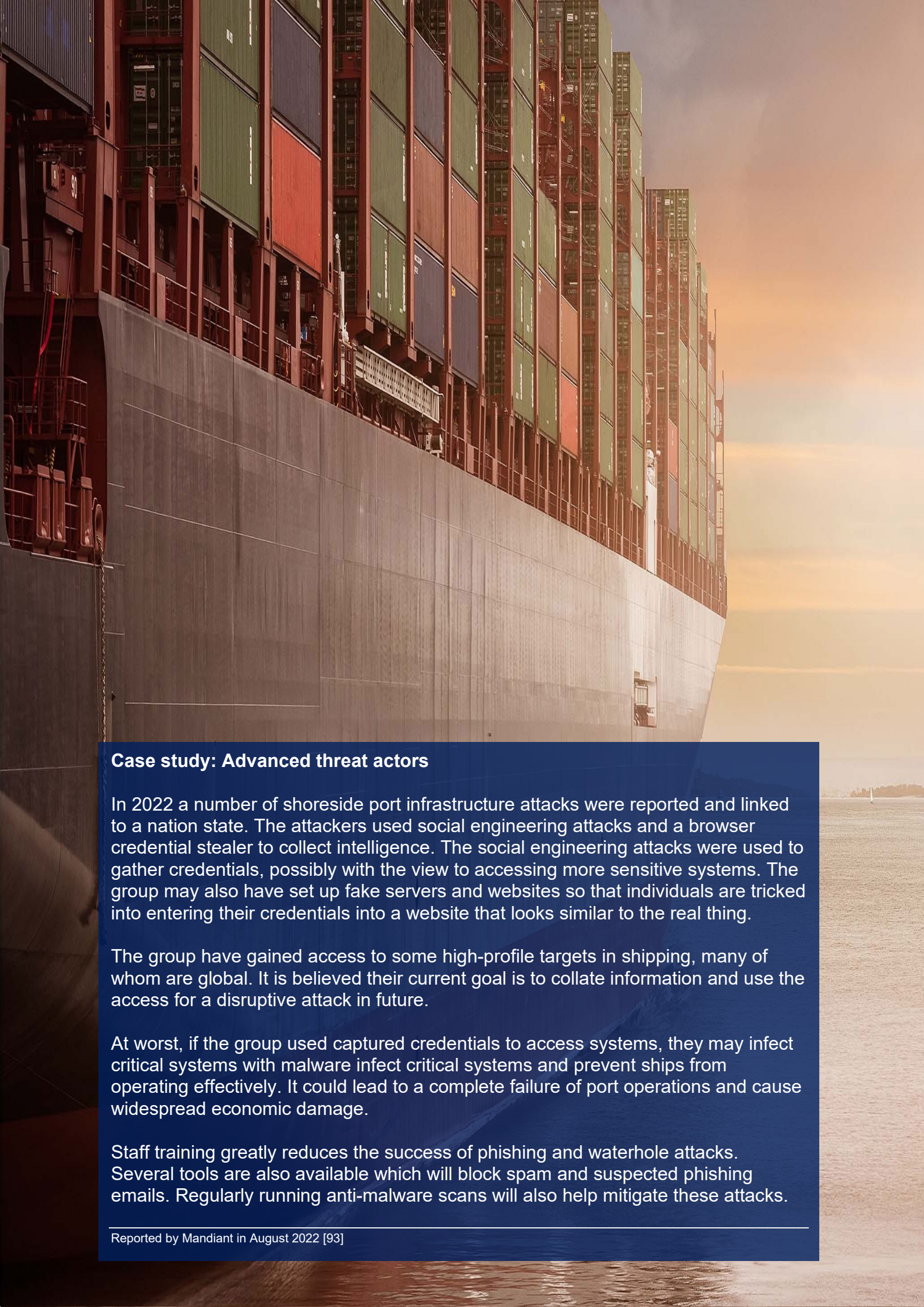
These risks are only examples and your system may have its own risks specific to your security context. You may use these risks to inform your own ship cyber risk assessment.

It is important that a risk assessment includes any risks inherited from suppliers, or caused by the supply chain. For example, a ship may use a piece of OT hardware that only the supplier can maintain and update, or the supplier may have built in a remote access route that a company is unaware of. This introduces several risks, for example:

- The OT hardware breaks whilst at sea and it cannot be fixed, rendering a ship stranded for several days;
- A supplier's network is breached and the attacker is able to use the remote access route to shut down the operation of the OT hardware, rendering a ship unable to sail safely;

- A supplier goes out of business, leaving the organisation operating the OT hardware with no updates or maintenance, meaning a ship cannot leave port until new software is installed.

Further details on threat actors, motivations and areas of risks with the shipping industry can be found in Annex B:Cyber Security and CSAs and Annex C:Developing a Ship Cyber Security Plan. These can be used to support cyber security assessments and other cyber security activities. Overtime the list will change as the cyber security threat landscape changes, and it should be reviewed accordingly.



Case study: Advanced threat actors

In 2022 a number of shoreside port infrastructure attacks were reported and linked to a nation state. The attackers used social engineering attacks and a browser credential stealer to collect intelligence. The social engineering attacks were used to gather credentials, possibly with the view to accessing more sensitive systems. The group may also have set up fake servers and websites so that individuals are tricked into entering their credentials into a website that looks similar to the real thing.

The group have gained access to some high-profile targets in shipping, many of whom are global. It is believed their current goal is to collate information and use the access for a disruptive attack in future.

At worst, if the group used captured credentials to access systems, they may infect critical systems with malware infect critical systems and prevent ships from operating effectively. It could lead to a complete failure of port operations and cause widespread economic damage.

Staff training greatly reduces the success of phishing and waterhole attacks. Several tools are also available which will block spam and suspected phishing emails. Regularly running anti-malware scans will also help mitigate these attacks.

Reported by Mandiant in August 2022 [93]

3. Manage your Assets

An asset is anything that is of value to an organisation. Managing assets well needs an understanding of what assets such as systems, data and services are in use. If an organisation does not know about an asset, how can it protect the asset from a cyber attack? Having this information along with robust asset management procedures in place supports smart decision making on cyber risks.

Important controls from the CAF to consider in this concept include:

- Asset Management (A3.a)
- Policy and Process Development (B1.a)
- Device Management (B2.b)
- Secure Configuration (B4.b)

Asset Management (A3.a)

For more information read:
CAF A3.a, GCSOS 3, NIST ID.AM-1,2,4,5, PR.DS-4, PR.MA-1, ISO27001 5.9, 5.10, 5.11, 7.10, 7.13, 7.14

Asset management is about understanding what you have. This includes people, systems, data and supporting infrastructure e.g., cooling and power.

Once you have identified and inventoried your assets, the next step is to prioritise them. Not only will this help you understand what aspects of your company and ship are critical, but it will also help you prioritise funding, and understand which risks are the most pertinent i.e., those affecting your critical systems.

Asset management is important for ships, particularly for OT systems which often have a lifetime of over thirty years and rely on software to support their operations. Managing these assets, and understanding their lifespans will help you minimise the risks associated with them. For example, if the software that operates the OT does not have any further vendor support it can no longer be updated. This may leave you open to attack unless further controls are put in place.

Automatic asset discovery of devices added to a network can be helpful, particularly to ensure that assets are correctly registered, classified, visible and configured.

An often-forgotten part of asset management is disposal; once an asset is no longer viable it should be disposed of securely. Until an asset is destroyed it can still be compromised, e.g., an old unencrypted hard drive may be taken from a bin and plugged into a computer, revealing its contents. The exact mechanism for destruction will vary depending on the sensitivity of the data stored or processed by the asset. For further information you may want to consult NCSC [21] or CPNI guidance [22]. Wider guidance on successfully managing assets and their cyber security risks can be found on the NCSC's pages on asset management [23].

Alongside physical assets, people and skills also form a key security control. Staff need to be aware of their responsibilities so they can report discrepancies, and know what expected behaviour is. Regular training will help staff stay abreast of evolving security

threats, whilst giving them confidence in their own cyber security practices. Business Continuity and Disaster Recovery (BCDR) plan should include contingencies for when staff are unavailable. Documenting and automating processes can help to mitigate resource issues.

Policy and Process Development (B1.a)

For more information read:
CAF B1.a, GCSOS 1.3, NIST ID.SC-1, ISO27001 5.1, 5.31, 5.34, 5.35

Policies and processes refer to those that your organisation creates to cement its approach to cyber security. Documenting your approach like this means that staff understand you take cyber security seriously, keeps processes consistent and holds staff accountable. They should be practical to follow, fit the environment they are in and not hinder essential operations. Good practice is that policies are continually developed and improved on, including being reviewed at least annually. They should also be reviewed when there are changes to systems and after any attacks.

Policies you may use include:

- Risk Management policy - describes how risks are identified, assessed, treated and reviewed;
- Physical access policy - describes how physical access to assets is approved;
- Asset management policy - describes how assets are managed, see Asset Management (A3.a);
- Change control process - describes how changes to the systems and ship are approved;
- Access control policy - describes how access to systems is authorised and brokered;
- Personnel security policy - describes how security is embedded in onboarding processes.

For policies and processes to be effective, they must be practical for the people that are using them. Ideally you should test policies with actual users before implementing them to confirm that they work as expected, are understandable and applicable to the organisation's ways of working. It is likely that any inconvenient policies or processes will lead to users finding workarounds, therefore resilience should be built in systems so they remain secure when policies and processes aren't followed. For example, if staff are forbidden to use USBs by policy and USB ports are also technically blocked, then a member of staff is unable to bypass the policy even if they desired to.

It is recommended that you do not publicly publish your processes or policies, unless required to by law. If your attackers know your policies or plans for attacks as this can give them insight into the weakest parts of the system or may help them discover how or when an attack would be most disruptive.

Password policy

For more information read:
NCSC password guidance [94], GCSOS 7.3 (Multi/factor authentication (MFA) and passwords)

Implementing a strong password policy is important because, once an attacker guesses the password, they can access your systems. It is particularly important for systems connected to the internet, as thousands of attackers may attempt to hack them. Attackers can use their access to conduct malicious behaviour, which could be especially disruptive in the case of OT technology. Care should also be taken about how and where passwords are stored.

Brute force is an attack technique that involves trying passwords until one succeeds. Hackers inject common passwords into the password field until one works. An easy way to mitigate this attack, is by setting account time-outs after 5 incorrect password attempts, and specifying a minimum password length, e.g., 12 characters.

Lists of commonly used passwords are freely available online. You may wish to consider technical enforcement to prevent the use of these common passwords and/or dictionary words. Lists of default passwords for devices and appliances are also published online. If an attacker finds that you have not changed your default password then they can gain access to your system in a matter of minutes.

It is important that default credentials are changed where possible. These are especially common on OT devices. Sometimes privileged default credentials are not under your control but may be required for maintenance by an external supplier. If this is the case you should request that the supplier allow changes to default credentials and record a risk on the risk register until done.

To summarise, you should specify the following as part of your password practice (particularly as most of the controls are free):

- Minimum length requirement e.g., 12 characters;
- Password storage;
- Enforce password changes after known breaches;
- Changing default passwords, especially commonly found on OT;
- Use of Multi-Factor Authentication (MFA);
- Use single sign-on (SSO) to minimise the number of passwords users are expected to remember;
- Educating users on keeping passwords secure.

Removable media policy

For more information read:
GCSOS 7.3 (Physical and removable media controls), NIST PR.PT-2

A removable media policy would cover devices such as USB drives for data transfer. These can contain malware which could infect the IT or OT system if they are plugged into

one. For this reason, any removable media should first be scanned on a device that is not connected to the ship's network.

Policies could also include disallowing the use of removable media. It is likely that you will have different policies for different devices, with the strictest rules for critical systems or where there is no reasonable need for allowing removable media.

Top controls

Password policy
Effectiveness: High
Value for money: High
Rating: Green

Trusted technology and suppliers
Effectiveness: Medium
Value for money: Medium
Rating: Yellow

Private control information
Effectiveness: Medium
Value for money: Medium
Rating: Blue

Device Management (B2.b)

For more information read:
CAF B2.b, NCSC Device Security Guidance [95], GCSOS 3.2, NIST PR.DS-8, PR.PT-2, DE.CM-5, ISO27001 8.1

Device management focusses on trust in devices that connect to your networks, for example Personal Mobile Radios (PMR) and bring your own devices [24] (BYOD) that passengers and crew connect to onboard internet. One of the risks that passengers pose is they may plug their laptop into your network, thereby accessing IT or OT systems and disrupting them. Technical controls must be put in place to reduce this risk.

One way to confirm a device's identity is via certificates. This enables you to only allow known devices access to designated systems (e.g., those that are not for passenger or general use). If implemented, it is useful to have physical security around devices that hold certificates as they can be used for identity management.

If company devices are provided, it is recommended you use separate devices for critical applications and those that are for general purpose to support network segregation. This will give you the freedom to impose stricter controls on the admin device, such as no internet connectivity. Viruses can infect laptops, and in turn infect the systems those laptops connect to. By using separate devices for admin access and internet access you break this chain.

Top controls

Block removeable media
Effectiveness: High
Value for money: High
Rating: Green

Physical security
Effectiveness: High
Value for money: High
Rating: Green

Scan removeable media
Effectiveness: High
Value for money: Medium
Rating: Green

Secure Configuration (B4.b)

For more information read:
CAF B4.b, GCSOS 7.2, NIST PR.DS-6,8, PR.IP-3, ISO27001 8.9, 8.19, 8.27, 8.32

The setup of networks and information systems should be secure. Often settings are not secure by default e.g., they do not use encryption. It is worthwhile spending time investigating what you need to do to make them secure. You should look at what configuration adjustments are required to secure the system. You should also ensure that changes are closely managed and decisions are tracked so that you can reinstall a system from scratch if something goes wrong/stops working.

Best practice includes closing network ports that are not in use, and forcing traffic to be sent encrypted.

Any new software being downloaded should be verified and scanned; ideally only preapproved software should be allowed to be installed on devices. This will minimise the chances of malware, such as Trojans, entering the system. Trojans use the installation of other benign software as a vector into the system (the malicious code hides within a legitimate application or one that performs as expected).

A Configuration Management Database, or similar tool, can be used, which will ensure information is authoritative, accurate and available, as well as enabling change detection, automation and visibility of assets.

Top controls

Close unused ports
Effectiveness: Medium
Value for money: High
Rating: Green

Patch and update software
Effectiveness: High
Value for money: High
Rating: Green

Configuration management
Effectiveness: High
Value for money: Medium
Rating: Yellow

4. Manage Identity and Access

Control who has access to data and systems via managing access and identities is vital for reducing cyber security risk. Organisations must ensure their management of access covers all systems and data, internal and external users as getting it wrong can give hackers and other bad actors an easy route into systems to perpetrate a cyber attack.

Important controls from the CAF to consider in this concept include:

- Identity Verification, Authentication and Authorisation (B2.a)
- Privileged User Management (B2.c)
- Identity and Access Management (IdAM) (B2.d)

Identity Verification, Authentication and Authorisation (B2.a)

For more information read:
CAF B2.a, GCSOS 7.3, 3.4-6, NIST PR.AC-2,6,7, ISO27001 5.15, 5.16, 5.17, 5.18, 7.2, 8.3, 8.4, 8.5

Another important part of cyber security is controlling who can access your system, and what can they can do on it. When a user tries to access a system, they are typically subjected to some level of verification access control, e.g., verification, authentication and authorisation:

- Verification is assigning a user an identity in the system from information known about them. For example, using HR processes to confirm someone is who they have claimed to be and adding that person to a computer system.
- Authentication is verifying that a user is who they say they are. A common example is a username and password combination.
- Authorisation is about understanding what permissions or rights a user has. For example, what they are allowed to view, edit or delete.

Unless you control who accesses your systems you cannot prevent malicious actors accessing them. Nor can you trace incidents back to individuals when they occur. Privileged and administrator accounts are critical to protect. These accounts have a high level of permissions, so if an attacker gains access to these accounts they can be very destructive, very quickly. This may result in systems going offline, or databases being deleted. Where these accounts exist further verification checks using Multi-Factor Authentication (MFA) should be made.

As users will change over time, you should ensure your user list is up-to-date and retire any old accounts. Each user account is another chance for an attacker to gain access, so removing these when possible will tighten your security. To reduce the risks of unwanted access, you can also limit the number of users/accounts that have access to critical infrastructure, like control systems, to the minimum necessary. This means that there are fewer people with access, and therefore fewer people that could fall victim to a social engineering or other attack where their authentication details are obtained.

Physical security

Physical security in relation to cyber security includes ensuring that OT and devices are not accessible to unauthorised individuals. An attacker may use physical access to cause physical damage, attempt to use a device, or remove data storage for further investigation. Crew should supervise any external parties accessing a critical OT infrastructure in authorised areas.

Physical access cards may be used onboard or in offices. These can be lost or stolen so should be updated or deactivated if they are reported missing to prevent physical accesses using them. For this reason, it is important to keep a regularly updated asset register of all physical items, so that you can track exactly what has been handed out, and to who.

As staff leave, it is important that their access cards and door codes are handed back and/or deactivated.

Multi-Factor Authentication (MFA)

Factors are options that can be used to authenticate a user, for example their password or fingerprint. MFA combines several factors to make it harder to fake an authentication and break into an account. Typically, it combines a password or PIN (something you know) with a token, phone apps or fingerprint logins (something you have). MFA mitigates the risks associated with default or known credentials, as an attacker gaining a password is not enough to gain entry to a system.

This guidance recommends using MFA at least for remote and privileged access to networks; organisations should consider using it for all systems, where it is appropriate and does not compromise safety.

Remote Access

Where appropriate, if not required for the normal operation of the ship, remote operations should be disabled and remotely available services blocked. Remote access is a common way for a hacker to gain access to data or install malware on a system which may result in systems being taken offline, or a ransomware attack. It is an easy attack vector because there is reduced physical risk involved. Limiting the number of things that can be altered remotely will help secure these avenues of attack. However, it becomes harder to secure a ship as the level of remote access required increases.

If remote access is required for the operation of the ship, then network segmentation will be beneficial. i.e., controls to prevent an attacker moving easily between systems.

Top Controls

Access Control
Effectiveness: High
Value for money: High
Rating: Green

Block removeable media
Effectiveness: High
Value for money: High
Rating: Green

Multi-factor authentication
Effectiveness: High
Value for money: High
Rating: Green

Privileged User Management (B2.c)

For more information read:
CAF B2.c, GCSOS 7.3, NIST PR.AC-4, PR.AT-2, ISO27001 8.2

As privileged accounts have more control over systems than normal users, they are the most crucial accounts to secure. If an account were to be compromised, the attacker would gain the same level of access as your most trusted staff.

A variety of strategies exist to manage privileged users. It is recommended that you understand the risks within your system so you can adopt an approach that is proportional to your ways of working. For example, you may choose to use software-defined built-in roles to set your privileged users' rights.

This may include having admin users use separate accounts for admin actions and general use. Any major changes made by these privileged accounts should be logged and monitored for suspicious behaviour, and audited. Monitoring and auditing gives you the ability to review behaviour in slow time, and spot suspicious activity. A password manager could be used for safe storage of passwords which are not regularly used or when a user has many to remember.

Privileged users also give rise to insider threat, whereby those who know most about your systems are the most capable of disrupting it. If a privileged user were to reveal passwords and access mechanisms this may result in attackers gaining physical and logical access to your systems. There are many different ways of mitigating insider threat:

- Vetting procedures to ensure only trusted people are hired;
- Fostering a good working environment and ensuring privileged users can report incidents without being shamed;
- Logging all activities to deter poor or malicious behaviour;
- Documenting systems to ensure there isn't a single point of failure i.e., only one individual understands how to maintain a system.

Top controls

Multi-factor authentication
Effectiveness: High
Value for money: High
Rating: Green

Change default credentials
Effectiveness: High
Value for money: High
Rating: Green

Password Manager
Effectiveness: High
Value for money: High
Rating: Green

Identity and Access Management (IdAM) (B2.d)

For more information read:
CAF B2.d, GCSOS 7.2, NIST PR.AC-2,4, PR.AT-2, PR.PT-1, DE.CM-3, ISO27001 5.15, 5.18

IdAM is important to maintain across all users and people that interact with the ship's networks. The minimum access rights should be given as a default to all users, with only elevated rights if required. You should document and audit this process.

Devices, users and systems that attempt to access systems should be reported and logged, as this can often be the first signs of an attack. As part of this you could slow repeated login attempts and lock accounts/devices after too many failures to protect against brute force attacks.

IdAM is a huge topic, with many different approaches that can be integrated into your business; you can find a lot of good resources on the web. The UK NCSC has made available a range of guidance on identity and access management, including a useful introductory primer [25] through to meeting the CAF standard for identity and access control [26]. The United States National Institute of Standards and Technology (NIST) Computer Security Resource Centre manages SP 800-53, which provides technical implementation guidance to meet US government cyber security standards. This guidance may be particularly useful for cyber specialists and system engineers to inform their approach to controls. NIST SP 800-53 IdAM guidance can be found under two main control families: access control [27] and identity and authentication [28].

Zero trust

For more information read:
NCSC Zero trust Architecture [96], NIST Zero Trust Architecture [97]

Zero Trust is the principle that assumes any new access request is not to be trusted by default. It requires users to regularly re-authenticate against each new resource they access. Often users are authenticated based on context or using an access policy. This approach seeks to mitigate the risk that once an attacker is inside one system, they can easily access other systems.

Zero Trust is an emerging concept and there is more than one way to implement it, e.g., it can be configured on a single device or across an entire network.

Top controls

Access Control
Effectiveness: High
Value for money: High
Rating: Green

Password policy
Effectiveness: High
Value for money: High
Rating: Green

Change default credentials
Effectiveness: High
Value for money: High
Rating: Green

Case study: Ransomware attack

A company providing an IT service to several shipping companies fell foul to a ransomware attack. Shore-side customer services were affected. It is not known how the ransomware first made its way onto the supplier's system.

As a result of the attack, communications between ships, agents and suppliers were blocked. Emergency alternatives were used by some customers to reach ships e.g., alternative emails. As a result, the supplier suffered significant reputational damage, and some customers lost business data.

To mitigate this type of attack, ensure that supply chain risks are incorporated into your cyber security plan. Dependencies on suppliers should be articulated and managed. Work with suppliers regularly to ensure updates on security statuses are kept up-to-date.

Source: reported publicly in the press

5. Know your Supply Chain

Supply chains issues can damage a company significantly, many recent attacks have been perpetrated through suppliers. Risks could be inherited through supply chains, often without being documented. This can be managed through contracts, service level agreements and maintenance plans. When suppliers are used, it is important to have documented what access they have to your systems.

The important control from the CAF to consider in this concept is:

- Supply Chain (A4.a)

Supply Chain (A4.a)

For more information read:
CAF A4.a, GCSOS 1.8, 3.7, NIST ID.SC, ID.BE-4, PR.AT-3, ISO27001 5.6, 5.19, 5.20, 5.21, 5.22, 5.23, 6.6, 8.26

One of the current risks to the maritime sector is the supply chain. This is important as critical pieces of equipment such as the engine, propulsion systems, HVAC etc. are provided and maintained through contract by third-party suppliers. If the supplier is compromised, the equipment they supply may also be. Each piece of equipment or software that comes from a third party brings with it a set of unknowns, such as:

- Where is the company based?
- How is the product maintained?
- How is it fixed/ or incidents with it resolved?
- How is it operated and does it integrate with other systems?

Unless you undertake due-diligence, you will not understand how well the item has been produced, how it is managed and how it can be maintained. Once you know the answers to these questions, you are in a position to understand the risks that using the equipment poses. Although many of these risks will be small, it is important to think about security throughout the entire procurement process. That way you can make an informed decision as to which product you buy and whether extra security controls need to be in place.

When researching a supplier, include questions about their cyber security approach and policies. One method may be to measure their compliance against CAF. Another commonly used framework is NCSC's security principles for cloud products [29]. This will give you an understanding of whether they match your attitude to security and any potential risks they may introduce. The NCSC has also provided guidance on Mapping your Supply Chain.

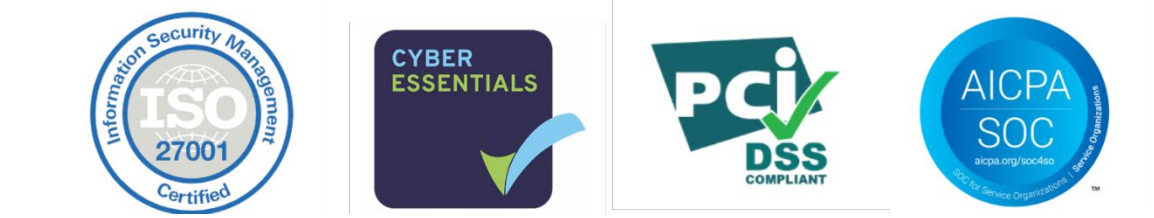


Figure 6: Cyber Security certifications: ISO27001, Cyber Essentials, PCI-DSS and SOC

You also want to look for third-party certifications, as these provide evidence that someone else, not just the supplier, is willing to attest to the supply company's security. Any certifications held should be in-date and cover the product you are potentially purchasing. For example, a company may hold ISO27001 or Cyber Essentials for their own IT systems but not for the products that they are selling. Cyber security certifications often held are Cyber Essentials (Plus), ISO27001 and PCI-DSS (where handling card payments).

Contracts with third-parties should include security clauses. These are likely to cover certifications that you expect your supplier to hold, Service Level Agreements and any other security policies they must adhere to.

Top controls

Trusted technology and suppliers
Effectiveness: Medium
Value for money: Medium
Rating: Yellow

6. Train your Users

Security only works if it works for people. Users are a crucial line of defence in cyber security. Giving users confidence in the operation of equipment and software they are using can support embedding a security culture in an organisation.

Important controls from the CAF to consider in this concept include:

- Policy and Process Development (B1.a)
- Cyber Security Training and Staff Awareness (B6.b)

Cyber Security Training and Staff Awareness (B6.b)

For more information read:
CAF B6.b, GCSOS 7.3, NIST PR.AT-1, ISO27001 6.3, 6.8, 8.7

Users are being increasingly targeted by cyber attackers. There is a high prevalence of social engineering attacks such as phishing. This emphasises the importance of training and user awareness. Educating users on what an attack could look like (and what damaging impact it could have) will help to reduce the chances of them falling victim to social engineering or other cyber security attacks.

Cultivate a positive reporting process for incidents so that users and staff feel comfortable coming forward if there is suspicious behaviour, or a policy breach, on systems. This will help spot an attack as soon as possible. A positive no-blame culture is a more effective security culture than staff fearing for their jobs if they report an incident. This aligns with the ISM Code which emphasises the need for a safety-led culture which can enhance the cyber security culture of an organisation.

There are many free or paid-for resources available online for training staff. The types of attacks they focus on will be dependent on the course and it may be good to write training based on specific security functions within an organisation. Resources are available to support more engaging training to avoid long lectures. The NCSC currently offers:

- Top tips for staff [30] - online training application that offers a high-level, relatable introduction to cyber security, and takes around 10-15 minutes to complete;
- Cyber security training modules for small businesses [31];
- Certified training courses [32] and university courses for cyber security education and development, which is a useful resource for awareness and specific cyber security training.

The training requirements for staff will vary dependent on the employee's role in the company. However, having some awareness of the harm that can be brought about by seemingly innocuous acts can help reduce the chance of them occurring, for example, not writing down passwords next to machines. This is common in shared machines, but is not good security practice, as it is trivial for anyone with physical access to gain access to OT and IT systems that keep the ship operating. Making sure staff know not to use the USB sticks used for data transfer for updates to systems, such as the ECDIS charts or in the Voyage Data Recorder (VDR) in their personal devices can reduce the likelihood of attack.

Top controls

User training
Effectiveness: Medium
Value for money: High
Rating: Yellow

Reporting process
Effectiveness: Low
Value for money: Low
Rating: Blue

Case study: Insider threat

Staff on a ship needed to transfer files to personal laptops. As they had no USB to hand, the USB from the Voyage Data Recorder (VDR) was used. Files were loaded onto it before being deleted and the USB replaced in the VDR.

Although no malicious behaviour was conducted, this demonstrates the ease with which insiders can load malware into the VDR. This may corrupt data on the VDR and allow malware to spread to other systems if the VDR network was not well segregated.

Staff awareness and training can help mitigate this mode of attack. Using dedicated USB sticks as well as disabling autorun/autoplay for USBs will also help.

Source: Company has asked to remain anonymous

7. Manage your Vulnerabilities

Vulnerabilities are weaknesses and potentially strengths. Keeping a record of vulnerabilities across the organisation supports cyber security strategies and allows organisations to have greater agility when responding to a changing threat landscape. Keeping systems protected from common flaws, such as by regular patching, makes it harder for attackers to get in.

The important control from the CAF to consider in this concept is:

- Vulnerability Management (B4.d)

Vulnerability Management (B4.d)

For more information read:
CAF B4.d, GCSOS 3.1-3.3, 8.2, NIST ID.RA-1, PR.DS-7, PR.IP-1,10,12, DE.CM-8, ISO27001 8.8, 8.34

Vulnerabilities are ways in which your systems may be exploited. As manufacturers find fixes for vulnerabilities, they release ‘patches’ for their software or equipment. System vulnerabilities are very common weak points for successful cyber attacks. This is why it is important to keep systems up-to-date and ‘patched’ because these will fix the vulnerabilities and limit the success of attacks.

New vulnerabilities in software often occur and are reported in the media e.g., the log4j vulnerability of early 2022. As the industry tends not to release details of vulnerabilities until a patch is released, by the time you are aware of the vulnerabilities, it is likely a patch is available. It is noted that these vulnerabilities therefore exist in your systems, and may be exploitable, before a patch is available. These are called zero-day vulnerabilities.

You should regularly test and monitor your systems for new and publicly-known vulnerabilities. Publicly available Common Vulnerabilities and Exposures (CVE) databases such as CVE.org will help you assess CVEs. You can also find details of known vulnerabilities on the NIST national vulnerability database [33], where you can search for specific software components or libraries, e.g., log4j, as well as products using it. The responsibility for undertaking vulnerability monitoring is likely to sit within a shore-side IT team or with the supplier of OT. This will depend on the business organisational structure.

Ships might be vulnerable to attack during their maintenance windows, especially when OT systems are being updated. You should consider system shutdown during these times.

A vulnerability management process can be used to help keep vulnerabilities in check. This would be included as part of a system maintenance plan, which should cover system security. The goal is to keep systems protected in a systematic way and document any vulnerabilities that cannot be addressed.

When a system is updated or the configuration is changed in any way, it is important to run vulnerability scans in case any have been introduced. There are software products which offer this as a service, including many anti-malware solutions.

It is worthwhile remembering that vulnerabilities are used by attackers to gain entry into systems after they are made public. When patches are released, attackers may also use reverse engineering techniques to derive attack methods against unpatched systems. Access routes into systems may then be sold, so another entity can use this to further attack or target systems. For example, the ransomware as a service model often provides access routes for the criminal group's customers to leverage to get ransomware into a system.

Top controls

Restrict APIs
Effectiveness: High
Value for money: High
Rating: Green

Patch and update software
Effectiveness: High
Value for money: High
Rating: Green

Test systems
Effectiveness: Medium
Value for money: High
Rating: Green

8. Build your Resilience

Ensuring operations continue during a security event is important for cyber resiliency. Resiliency is of particular importance for Operational Technology, supporting continued operation of safety-critical systems and aims to eliminate single points of failure. Have the right plans in place to help keep systems operating and data secure can support a cyber resilient approach to technology.

Important controls from the CAF to consider in this concept include:

- Resilience Preparation (B5.a)
- Design for Resilience (B5.b)
- Backups (B5.c)

Resilience Preparation (B5.a)

For more information read:
CAF B5.a, GCSOS 9, 10.2, NIST ID.BE-5, PR.IP-1,7-10, ISO27001 8.6

Resilience preparation is about the ability to restore operation after an incident (disaster recovery). For example, if you find that control of a critical system has been compromised, there may be a backup solution in place so that control of the ship is not lost. Without resilience preparation you are likely to spend a long time recovering and rebuilding from an attack.

One example of this is cross-checking navigational information in case of GNSS/GPS or AIS interference. Conversations with maritime stakeholders have indicated that this has recently been seen in the industry. By referring to more than one display for this information, differences may be spotted faster. It would also provide a practical solution if the main navigational method fails.

You should make sure you have the following things in place and tested:

- Business Continuity Plan (covering keeping business operations up and running);
- Disaster Recovery Plan (covering getting back up and running in the event of an outage);
- Backup Plan (covering back up of data and systems);
- Physical and Environment Security Plan (covering plans for environment or physical issues, such as flood, fire or power loss).

You can work with your suppliers to ensure that they support resiliency, such as establishing back-up approaches to keep data safe in the event of a ransomware attack, or building a network onboard a vessel such that there are limited blackspots. You should also ask your suppliers to confirm that they have the items in the list above in place.

Top controls

Cross-check and validate data
Effectiveness: High
Value for money: High
Rating: Green

Planning
Effectiveness: High
Value for money: High
Rating: Green

Design for Resilience (B5.b)

For more information read:
CAF B5.b, GCSOS 7.2, NIST PR.DS-4, PR.PT-3,5, ISO27001 7.5, 8.14

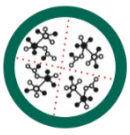
Design for resilience by building flexibility into systems. This can be done by building in redundancy, scalability and elasticity. Resiliency is important to ensure operations can continue during a cyber security incident, such that key properties of information security (integrity, confidentiality and availability) and operational security (safety, usability and reliability) can be maintained. For OT, resiliency is a central security outcome as it supports the continued operation of safety critical systems and aims to eliminate single points of failure.

Controls to design for resilience include:

- System limitations and weaknesses should be identified and mitigated where possible;
- Measures against keylogging, which include having drop down lists for form entry as well as keyboard input fields;
- Measures against screen recording and shoulder surfing, which include shielding passwords as they are entered;
- Server redundancy to increase resilience to DDoS attacks, as smaller amounts of server space may be easy to overwhelm;
- Communication and navigation spoofing or jamming can be mitigated in a variety of ways, including use of certain antennae and oscillators;
- Virtualisation or sandboxing can add to resilience when browsing, as well as disallowing remote accesses or remote changes to systems;
- Increasing physical security can increase general resilience to attacks.

The IACS UR E26 deals with cyber resilience on ships [34] for the secure integration of both OT and IT and is a good resource for industry specific details on cyber resiliency.

Top controls



Network segmentation
Effectiveness: High
Value for money: High
Rating: Green

Physical security
Effectiveness: High
Value for money: High
Rating: Green

Anti-jamming / Anti-spoofing
Effectiveness: Medium
Value for money: Medium
Rating: Yellow

Backups (B5.c)

For more information read:
CAF B5.c, GCSOS 10.3-10.4, NIST PR.IP-4, DE.DP-1, ISO27001 8.13

Data backups are extremely important to keep for numerous reasons, but are crucial if an organisation is required for restoring a compromised system or comparing changes. It can also be very useful when updating critical systems to have a backup of the data and configuration in case something goes wrong. Ransomware often encrypts data as part of the ransom demand, so having a backup of the data may help restore operations without paying the ransom.

Backups are expensive and, on a ship, it can be difficult to align to good practice, e.g., you cannot store a backup offsite for a ship underway. Nevertheless, it is recommended that organisations consider how regularly they create backups and where the backups are stored. Good practice is that backups should be separate to where the original copies of the data are stored. The National Cyber Security Centre (NCSC) recommends a 3-2-1 strategy [35].

Top controls

Backup data
Effectiveness: High
Value for money: High
Rating: Green

Cross-check and validate data
Effectiveness: High
Value for money: High
Rating: Green

Planning
Effectiveness: High
Value for money: High
Rating: Green

Incident case study: Unknown supply chain access

Whilst at sea, a passenger cruise ship suffered a blackout. The incident was resolved promptly however whilst investigating the underlying cause it was discovered that a certain supplier had remote access to the equipment on the ship that they had supplied. This was previously unknown and unreported.

This remote access opened a new attack vector that was not monitored or managed by the ship's company. If the supplier had been hacked this connection may have been used to also hack the supplied equipment onboard. Depending on the level of access given to the supplier, there may have been large costs involved. This might come from replacing equipment and compensating passengers.

The type of attack can be mitigated by talking to suppliers about the access they want or require. Any access they require should be monitored, not just left to the supplier to manage. Logically separating critical networks from non-critical networks will also build defence-in-depth and help prevent attacks spreading.

Staff training greatly reduces the success of phishing and waterhole attacks. Several tools are also available which will block spam and suspected phishing emails. Regularly running anti-malware scans will also help mitigate this attack.

Source: conversation with interviewees during the preparation of this document

9. Monitor your Systems

Monitoring allows an organisation to see what is going on in its systems. Good monitoring allows an organisation to gain further insight into its systems, detecting incidents, events and threats while offering an additional defensive capability by timely flagging of incidents and potentially active defence such as taking automatic steps to mitigate risks.

Detecting cyber security incidents can help to reduce the impact or the losses that the event may cause and help stop the event escalating. Some attacks require an attacker to first gain entry to a system. This might only be possible if protective controls fail. Thus, monitoring the system and the status of the protective controls can prevent an attack from executing on a system. An example would be ransomware, where an attacker will use a compromised route into the system to access and then leverage the access to attack the data. Detection of early indicators of compromise will mean that the ransomware is unlikely to be successfully deployed and an organisation will not lose access to data or face the prospect of being asked to pay a ransom.

For many attacks, if the intruder could be detected before the attack, or indicators of compromise understood then measures can be taken to minimise the disruption and loss.

Security event detection and management is challenging. It can be hard to find the right balance between the disruption caused by too many alerts and the impacts of missing true positives e.g., if every new user is flagged as a potential event, suspicious activity may go unnoticed.

One model that may help with detection is the Cyber Kill Chain. A cyber kill chain represents the phases that an attack usually passes through. By considering the adversary's likely actions at each phase, it is possible to list the detections associated with each and to plan for appropriate responses.

Common attacks tactics and techniques can be found in the MITRE ATT&CK framework [36], which covers Enterprise IT as well as Industrial Control Systems. However, they may not all be applicable to all organisations. Keeping up-to-date with cyber attacks, specifically those that impact shipping, will be a useful way of understanding new attack trends. This will help build a robust risk assessment and understanding of the cyber landscape.

Important controls from the CAF to consider in this concept include:

- Monitoring Coverage
- System Abnormalities for Attack Detection (C2.a)

Monitoring Coverage (C1.a)

For more information read:
CAF C1.a, GCSOS 8.1, NIST DE.CM-1,3,4,6,7, ISO27001 7.4, 8.15, 8.34

Monitoring of an organisation's networks and systems can help spot anomalies and unusual behaviour. Early detection of an attack may reduce its impact. For example, monitoring may help an organisation spot attempts to access its network, meaning the IT

support function can disable the associated user account before further compromise happens. As well as detecting security issues and vulnerabilities, monitoring can be a tool used to discover how effective policies and controls are as these can be measured.

Effective monitoring allows insight into systems by detecting incidents, events and threats, and supports timely flagging of incidents. Some tools have the ability to actively defend systems by taking automatic steps to mitigate risks. For example, you may use a Security Event and Incident Management function which ingests logs and events and threat intelligence to address incidents across shore-side and ships.

Monitoring systems is challenging, as often an organisation has multiple logs and events at multiple different tiers to be concerned with. Automating and/or using specialist monitoring software may be the best way to collate and manage information. The risk assessment as well as the asset list should be used to form the basic building blocks of which systems are most important to monitor. This will help prioritisation based on value for money and which data poses a greater risk, should a cyber security incident occur. For example, a system which has no access to the internet and is only used by a couple of trusted users, such as the alarm system, is unlikely to benefit from extensive monitoring as the risk of compromise assuming robust adherence to the operating procedures is likely low.

To monitor systems effectively, skilled staff are required to analyse behaviour and make judgment calls on whether or not additional action is required. It may not be practical for small and medium size enterprises to operate their own Security Operations Centre, and organisation may outsource this to another company or prioritise specific systems, to manage the volume of monitoring alerts. In this case organisations are advised to follow good supply chain practice and undertake assurance on the monitoring service.

The NCSC offers the Cyber Security Information Sharing Partnership (CISP) which allows collaboration between UK private sector organisations and government departments on threat intelligence and information sharing. You can also find further NCSC guidance on security monitoring for operators of essential services [37].

Top controls

Anti-malware
Effectiveness: Medium
Value for money: Medium
Rating: Yellow

Firmware and device monitoring
Effectiveness: Medium
Value for money: Medium
Rating: Yellow

Network monitoring
Effectiveness: Medium
Value for money: Medium
Rating: Yellow

System Abnormalities for Attack Detection (C2.a)

For more information read:
CAF C2.a, GCSOS Annex 2 (Protect), NIST DE.AE-1,5, DE.DP-5, RS.MI-3, ISO27001 5.27, 8.16

An important part of detection and monitoring is understanding what normal system behaviour looks like and what common cyber attack methods are. It is recommended that

all access to systems is monitored and logged. Learning from past attacks (both internal and externally observed) will also help to identify what malicious activity could look like.

If there are changes in an organisation's systems or networks then it is recommended that the organisation reviews and updates how anomalies are detected, to stop expected, consistent changes being falsely flagged.

Below are some examples of what could be monitored to detect system compromises:

Figure 7: Potential indicators that your system has been compromised

Taking steps to filter out abnormalities will provide network integrity, and potentially protect against threats. Where malicious packets, or behaviour, has a regular pattern this can be filtered or blocked to reduce its impact. For example, an organisation may choose to regularly drop packets from certain countries, or to block packets for a set period of time from particular untrusted networks. Traffic volumes outside a particular range may also be blocked to prevent unavailability or disruption of systems.

Top controls

Network filtering
Effectiveness: Medium
Value for money: High
Rating: Green

Network monitoring
Effectiveness: Medium
Value for money: Medium
Rating: Yellow

OT operations monitoring
Effectiveness: Medium
Value for money: Medium
Rating: Yellow

10. Manage Cyber Incidents

No system is 100% secure and incidents will happen. Organisations should define what incidents they are concerned and plan for them. Plans should be tested, incident types simulated and lessons learnt from this testing. Incidents can also have significant impact on staff and organisations affected by them.

This section offers guidance on how to reduce the impact of an attack. No systems are completely free from cyber attacks and therefore minimising their impact when they do occur will help aid recovery and keep the subsequent costs and losses to a minimum.

Government has an online web form that directs organisation's to the appropriate authorities to report cyber security incidents [38]. Operators of essential services experiencing a cyber security incident may skip this web form and report details of the incident directly to the National Cyber Security Centre [39], who can advise further.

Important controls from the CAF to consider in this concept include:

- Response Plan (D1.a)
- Testing and Exercising of Response and Recovery Plans (D1.c)

Response Plan (D1.a)

For more information read:
CAF D1.a, GCSOS 10, 10.2, NIST ID.SC-5, RS.RP-1, RS.CO, ISO27001 5.24, 5.29, 5.30

Planning for cyber attacks and having policies and processes in place to mitigate their impacts supports a mature security posture. This could include backup plans to mitigate loss of data following an attack. It may also include a clear reporting process for attacks, hopefully lessening their impact by managing breaches quickly.

Response plans should be tested, improved and adapted over time. Having a plan will help staff know what to do during an incident particularly when they cover a variety of attacks.

A comprehensive response plan will contain:

- An understanding of which systems and data are critical;
- Response to likely scenarios and attacks, including detection, reporting process, analysis of the incident, containment, remediation and lessons learned;
- Roles and responsibilities of all parties needed to execute the plan;
- Integration with third-party response plans;
- Communication and escalation routes within the company and with third parties.

Another important strategy is to adapt or create a response plan based on lessons learnt from a previous incident and from tabletop or simulated incidents. Lessons learnt are commonly related to a plan not working as expected, e.g., in the case of a task being fulfilled by a named person but they are on leave, or where there is a gap in the capability.

Running a mock incident and cyber drill will highlight these gaps before an actual incident occurs.

Major security incidents can impose significant stress on those involved as well as a sharp increase in the amount of work required of a, typically, limited cohort. Consideration should be given to managing that workload as well as the potential mental health impacts on the staff involved.

Top controls

Backup data
Effectiveness: High
Value for money: High
Rating: Green

Reporting process
Effectiveness: Low
Value for money: Low
Rating: Blue

Testing and Exercising of Response and Recovery Plans (D1.c)

For more information read:
CAF D1.c, GCSOS 10, 10.2, NIST RS.AN-5, ISO27001 5.3

Testing and exercising plans with staff is essential to have a robust response. Organisations may run exercises with varying ranges of involvement; from table-top (e.g., discussion) to simulations (inviting in ethical hackers to simulate an attack on your equipment in order to test your controls). Within the maritime sector table top exercises may be the most effective route as it could be disruptive undertake walk throughs or

Figure 8: Various ways to test your recovery and response plans

simulations using ethical hackers.

Exercises will help test response and recovery plans and may highlight practical weaknesses or gaps in staff knowledge. These scenarios can be carried out based on real incidents making them as true to life as possible.

After an attack it is recommended that plans are reviewed. It is an opportunity to improve them based on what went well and what did not so that future incidents can be managed more effectively.

Top controls

Planning
Effectiveness: High
Value for money: High
Rating: Green

5. Conclusion and Call for Action

The cyber landscape within the UK and the world at large is constantly evolving with attackers leveraging new techniques and vulnerabilities to achieve their objectives. Cybercrime is particularly attractive as it offers lucrative incentives and can be difficult to trace, being independent of borders for example. Additionally, factoring in geopolitical tensions and the increasing digitisation of society, the general level of cyber threat will continue to increase in the future.

As threats emerge, the shipping sector within the UK, needs to be prepared to meet them. The purpose of this COP has been to provide guidance and support to enable you and your organisation to achieve this effectively with the resources and tools available. Following the Top 10 will help organisations meet this goal. However, organisations will need to embed processes to stay abreast of these emerging threats. Cyber security assessments should be constantly reviewed and improved to ensure controls are appropriate to emerging threats.

Cost is always a key factor when improving the security of systems. Throughout the document the emphasis is to highlight controls and security measures that provide both value for money and effectiveness. Often the simplest of changes can provide a huge improvement in security posture (e.g., changing default passwords on a router). All businesses should aim to implement these.

The COP also highlights changes in the use of OT. The increasing levels of connectivity with external systems and the internet, need careful thought to reduce the likelihood of an attack on maritime systems. Consider what is effective and appropriate for your organisation, your operating environment, vessels and equipment.

When paired with technical controls, procedural and physical controls create a strong armoury for any organisation to withstand cyber attacks. Documenting processes and policies is key to producing repeatability and empowers staff with the confidence to act in a more secure fashion.

In any cyber defence strategy, the key points are to identify what systems and assets are critical for your organisation. This helps build a foundation on which you can create a robust risk assessment, effectively prioritise your resources, and reduce risks to a level acceptable for your organisation.

Annex A: Terms and definitions

Overview

This section contains various terms and definitions that will help the readers to be acquainted within the document.

Definitions

Term	Definition
Asset	Item, thing or entity that has potential or actual value to an organization. [BS ISO 55000:2014 [40], 3.2.1]
Cyber Assessment Framework (CAF)	A National Cyber Security Centre (NCSC) framework [17] which gives cyber security guidance for organisations responsible for important services and activities, including shipping.
Hack	To gain unauthorized access to data in a system or computer
Malware	Malicious software. This is often designed to harm a system and includes viruses, ransomware, worms and trojan horses.
Operational technology (OT)	The technology commonly found in cyber-physical systems that is used to manage physical processes and actuation through the direct sensing, monitoring and or control of physical devices. For example: motors, valves, pumps, etc. In a vessel these systems include: plant and machinery, RF communications, on and off board sensors and navigation systems.
Personnel	Individuals employed by an organization including contractors or temporary staff used to fulfil roles that may be undertaken by that organization.
Ship	A passenger ship carrying more than 12 passengers or a cargo ship engaged in an international voyage including high-speed craft and mobile offshore drilling units (MODUs). Generally, the provisions of the SOLAS Convention apply to cargo ships of, or over, 500 gross tonnage (gt). The Maritime Security Measures apply to passenger ships, as above, and to cargo ships over 500gt. [ISPS Code [6], Section 1.8, p.12]
Ship security assessment (SSA)	A risk assessment undertaken by, or for, a company security officer as a prelude to the preparation of a ship security plan or the review, or amendment, of an approved ship security plan. [ISPS Code [6], Section 1.8, p.12]
Ship security officer (SSO)	The person on board the ship, accountable to the master, who is designated by the Company as responsible for security of the ship, including implementation and maintenance of the ship security plan, and for liaison with the company security officer and port facility security officers. [ISPS Code [6], Section 1.8, p.12]
Ship security plan (SSP)	A plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident. [ISPS Code [6], Section 1.8, p.12]
SOLAS Convention	The International Convention for the Safety of Life at Sea, 1974, as amended. [ISPS Code [6], Section 1.8, p.12]
Threat	A potential cause of an incident or hazardous situation that may result in harm to an asset, person, system or organization.

Vulnerability	A weakness (for example, systematic, procedural, physical or technical) of an asset, or group of assets, that can be exploited by one or more threats.

Acronyms

Term	Definition
AIS	Automatic Identification Systems
BIMCO	The Baltic and International Maritime Council
BCDR	Business Continuity and Disaster Recovery
BYOD	Bring your own devices
CAF	Cyber Assessment Framework
CISO	Chief Information Security Officer
CiSP	Cyber Information Sharing Partnership
CPNI	Centre for the Protection of National Infrastructure
CSA	Cyber Security Assessment
CSP	Cyber Security Plan
CVE	Common Vulnerability Exposure
CySO	Cyber Security Officer
DDoS	Distributed Denial-of-Service
DfT	Department for Transport
DSTL	Defence Science and Technology Laboratory
ECDIS	Electronic Chart Display and Information System
GCSOS	Guidelines on Cyber Security Onboard Ships from the consortium including BIMCO
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GNSS	Global Navigation Satellite System
IACS	International Association of Classification Societies
ICS	Industrial Control Systems
ICS	International Chamber of Shipping
IDAM	Identity and Access Management
IET	Institute of Engineering Technology
IMO	International Maritime Organisation
INTERCARGO	International Association of Dry Cargo Shipowners
INTERTANKO	International Association of Independent Tanker Owners
ISO	International Standards Organisation
ISPS	International Ship and Port facility Security
IT	Information Technology
IUMI	International Union of Marine Insurance
MFA	Multi-factor Authentication
MSC	Maritime Safety Committee of the IMO
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
OCIMF	Oil Companies International Marine Forum
OT	Operational Technology

PIN	Personal Identification Number
PMR	Personal Mobile Radio
SCADA	Supervisory Control and Data Acquisition
SOLAS	Safety of Life at Sea Convention
SSO	Single Sign-on
Sybass	Superyacht Builders Association
USB	Universal Serial Bus
VDR	Voyage Data Recorder
VPN	Virtual Private Network
WSC	World Shipping Council

Annex B: Cyber Security and CSAs

Why is cyber security important in shipping?

Cyber security in shipping should ensure that vessels run smoothly and securely. It itself should remain unseen whilst supporting the achievement of business objectives. If implemented correctly, it can prevent significant harms and operating costs. As the maritime industry looks to increase automation and leverage more advanced technology to operate ships, the argument for a robust approach to cyber security is further strengthened. Ship Owners, Operators and Officers in charge hold accountabilities, responsibilities, and legal roles for protecting the ship, unlike in the automotive sector where the manufacturers hold liability.

Poor cyber security within the maritime sector can have significant costs, harms and disadvantages to organisations and the UK more generally, for example:

- Financial impact - This may arise if a ship is prevented from sailing and hence loses revenue. Remediating a cyber event may also incur charges such as obtaining specialist support, requiring suppliers to come onboard to address issues, or replacing equipment. A cyber event could also lead to regulatory fines, e.g., data protection fines and/or legal actions.
- Ability for the ship to operate safely - This may be the result of an event which prevents the update of the Electronic Chart Display and Information System (ECDIS) system, or timely receipt of information by port authorities.
- Cost to the workforce resolving incidents - Cyber security incidents can take a significant toll on the workforce. Staff are at risk of burnout and damage to their mental health depending on the severity and length of the incident.
- Supply chain impact - Some cyber events may cause long term disruption to shipping and have a major impact on the supply chains into and out of the UK. A cyber event with a supplier also can have a major impact on business operations. Supply chain should be considered as part of the assessment of cyber security risks.
- Public safety impact - This may result in danger to other vessels or passengers e.g., a chart is maliciously tampered with causing a ship to become grounded on a sand bank. The grounding causes injury to passengers onboard.
- Reputational impact - An organisation's reputation can be damaged after a cyber event particularly where personal data is leaked or an organisation cannot meet obligations to its customers. Considering reputational damage during the cyber

assessment can support you in taking steps to reduce this impact and improve your communication.
- Environmental impact - If a cargo management system is attacked this may result in negative environmental impact. If the attack is not detected the ship may be inappropriately loaded and release cargo into the environment during sailing. There may also be financial implications to rectify the situation.

Undertaking a Cyber Security Assessment (CSA)

A CSA is designed to present a documented understanding of cyber security onboard the vessel. It covers what the likely threats and vulnerabilities are as well as the systems and data in use on the ship and their criticality. This enables the identification and measurement of cyber security risks to the ship. It will support decision makers in prioritising risks mitigations and security controls whilst considering what is feasible and remaining in budget. The GCSOS provides detailed guidance on how to undertake the steps required to complete a CSA and is specific for shipping. This COP provides additional information around risks, threats, vulnerabilities and approach controls which may be helpful when completing a CSA. To ensure that the CSA is holistic and relevant to the vessel operations, you should include input from the operators of the vessel who have expertise in safely operating a vessel.

A CSP is designed to track any issues identified in the CSA, any gaps in controls, further measures taken to protect against cyber risks, and to detect and minimise the impact of cyber security incidents. The CSP should consider the impact of measures set out in the security plan for the ship and its systems. Cyber security is best considered as part of the wider security of a system and vessel i.e. ensuring consideration of physical and technological, personnel and processes will provide the best coverage of cyber security. Therefore, it is recommended that the CSP covers:

- Any risk mitigation measures;
- Any residual risks to the ship from cyber security not otherwise mitigated or transferred;
- If an appropriately senior ship or company officer has accepted the risk associated with any residual risks not otherwise mitigated or transferred;
- The policies that set out the security-related business rules derived from the SSP;
- The processes in place and how they are implemented onboard when using the ship's assets;
- The procedures with detailed instructions for repeatable and consistent mechanisms for the implementation and operational delivery of the processes;
- Responsibilities onboard;
- Responsibilities within the wider organisation around cyber security including the Cyber Security Officer (CySO) and escalation routes;
- Plans in place for incidents including business continuity and disaster recovery plans;
- Testing plans in place for the CSP; and
- Legal jurisdiction questions during a voyage.

The CSP is a living document and should be returned to regularly e.g., at least annually, to ensure that cyber security plans remain relevant and up to date.

Annex C: Developing a Ship Cyber Security Plan

Background

Under the ISPS Code [6], a ship is required to have a Ship Security Plan (SSP) which is derived from the Ship Security Assessment (SSA) which explores the risks to a ship. It is recommended that cyber security is incorporated into this approach by maintaining a Cyber Security Assessment (CSA) and Cyber Security Plan (CSP) under the SSA and SSP, respectively. This ensures that cyber security risks are collated alongside other risks, while also allowing specialist cyber security advice to be combined into these documents. It is recommended that such plans are reviewed annually to support the protection of the ship and its OT and IT systems. The recommended relationship between the SSA, SSP, CSA and CSP is shown in the diagram below.

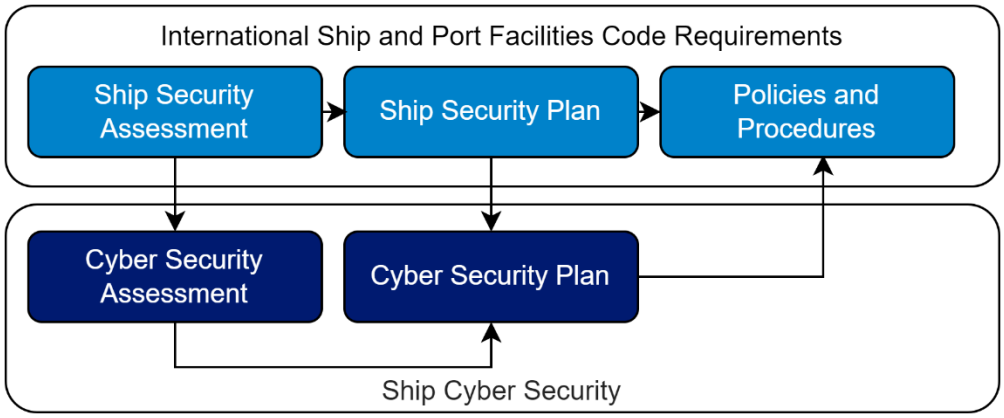


Figure 9: Relationship between ISPS Code required security documentation and the recommended Cyber Security approach

This approach was originally advocated in the 2017 version of the COP for Shipping and aligns well with industry recommendations, for example, the IMO's Safety Committee recommended this approach at MSC 101/24. Incorporating cyber security into general risk management is also considered as good practice by the NCSC and NIST. It is important to

establish governance and oversight of cyber security risks within businesses rather than simply holding the risks in the cyber security or IT team.

The CSA principally meets CAF objectives A and B. The rest of this annex provides guidance on undertaking a CSA. Further relevant guidance, which is also specific for shipping, can be found in BIMCO's GCSOS.

Undertaking a Cyber Security Assessment for Ships

A CSA is designed to understand the cyber security posture onboard the vessel and inform actions to be taken. Before starting a CSA, it is recommended that any gaps in information required to complete the assessment are highlighted. It is necessary to understand:

1. The different assets which support the operation of the ship;

2. The criticality of the assets and systems in the ship;

3. How the critical assets and areas of the ship support the operations.

For example, a CSA of an oil tanker or LNG may focus more heavily on the fire suppression system than say a CSA for a dry bulk carrier. A fire suppression system is likely to be critical for the operation of a ship carrying highly flammable cargo such as oil or LNG. The fire suppression system will consist of several different assets: hardware (sprinklers/foam/carbon dioxide); cabling used for support; a control system; and a monitoring system around the ship. Figure 10 highlights important information and some IT and OT systems used for the safe operation of a ship.

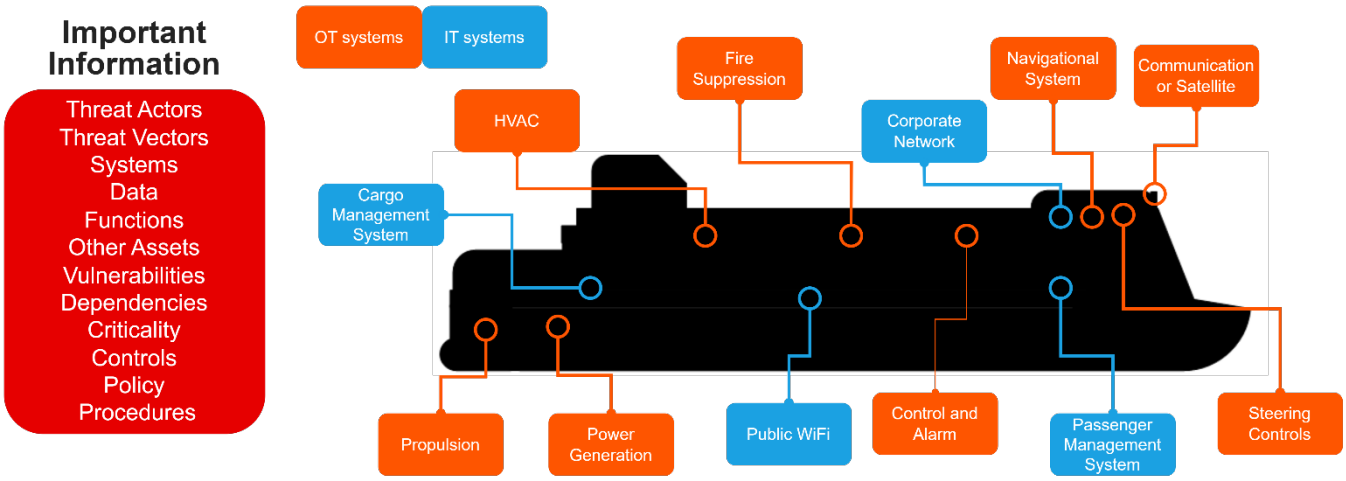


Figure 10: Important information to collect before starting a Cyber Security Assessment and potential systems to consider as part of the assessment

Sometimes all the information may not be available or may be created as part of the assessment. For example, it may not be appropriate to have written a policy, such as an acceptable use policy, before you have completed an assessment. This is because a good

policy is related to the risk faced. Nevertheless, if a system uses a username and password to control access, it is recommended that the company's password policy is considered to ensure that the system meets company requirements.

Risk Management

As laid out in Risk Management Process (A2.a), a 6 step process can be used to complete your risk assessment. Each step is described in detail below, including worked examples.

Figure 11: Risk management process

Step 1: Assessing Threats

When assessing the likely threats to a ship, consider the type of ship, the cargo, age and systems in place. A passenger cruise ship has a very different threat profile to a fishing vessel. Nevertheless, for all vessel types, considering both threat actors and threat vectors will support the assessment of the threat that the vessel is under. Figure 12 highlights some possible threat actors and some plausible motivations and methods. The threat actor approach can be helpful to support engagement with non-cyber professionals where it is easier to relate to actors than it is to risks. Categories of threat actors are not exclusive e.g., Hackers may also be passengers.

The threats that organisations may want to consider include:

- Nation States and Intelligence Services are likely significant for some organisations, with the threat actor having high capability. If the threat actor is motivated then the options to mitigate the threat will be limited.

- Organised Crime Groups and Ransomware as a Service operators are generally motivated by financial reward and cover a broad range of activities from people and drugs smuggling, through to the harvesting and selling of personal data to cyber attackers for ransom. They operate in various ways, from co-opting insiders (through financial incentives or threats to the person) to leveraging vulnerabilities within systems and processes. General cyber security good practice can support mitigating the threat, and discussions with law enforcement may be necessary should an organisation assess that it is under significant threat from these groups.
- Vendors and suppliers. This group includes sellers, support and servicing staff from vendors or suppliers that may be aboard for maintenance, installation etc. They may have the ability to gain access remotely, poor software and firmware maintenance practices, and may perform functions critical for an organisation to operate. Good supply chain management and cyber security hygiene (such as changing default credentials and having security updates in place) can reduce the threat.
- Company employees at all levels such as system administrators, IT support, end users and senior management. Most staff are unlikely to have significant active offensive capability, although specialist personnel such as IT staff may have greater capability. Most employee threats are the result of accidents / unintended consequences of other actions, including non-compliance with procedures and being a victim of social engineering. The employee threat can be reduced by improved cyber security training, vetting, protective monitoring and ensuring policies and procedures work as intended.
- Support staff such as cleaners and port security. These staff may come aboard the vessel during harbouring and have a variety of roles in support ship. They may have significant unsupervised access to the vessel as part of their duties. Controlling physical access within the physical environment of the ship can reduce the threat.
- Hackers and Hacktivists have variable capability dependent on the specific skillset of the individual or group involved. If motivated by a relevant cause, they may make a greater effort to acquire the capabilities and access required to target a particular vessel. Reducing the attack surface and good cyber security hygiene can reduce the level of threat from these actors.
- Passengers. For ships that carry a lot of passengers with connectivity services offered, the threat profile is different. Passengers on board are likely to have multiple devices connected to passenger networks. The majority of passengers would be low skilled and low motivation beyond a general interest in how the ship works. Some may have greater level of capability and interest than expected.

Figure 12: Assess Threats

In addition to actors, it is important to assess threat vectors when modelling threats and vulnerabilities in your systems and ships. Some threat vectors to consider include:

- Escalation of privileges
- Supplier Maintenance windows
- Signal interference, jamming or manipulation
- Social engineering and targeting of staff
- ICS and SCADA poor practice
- Physical theft and brute force
- Misuse of systems by staff
- Malware and Ransomware
- Misconfiguration of systems
- Exploitation of a vulnerability

Step 2: Identify your Risks

Use the assessment of threat to identify the risks to assets, systems, and data in this step of the CSA. The risk assessment should consider the nature of harm that may be caused to: the ship, shipboard personnel, passengers, other assets and personnel. The

assessment should also consider the societal, environmental, and commercial benefits the ship exists to deliver.

The cyber security risk will depend on the likelihood that a threat actor can exploit one or more vulnerabilities and cause harm or reduce the benefits intended to be realised by the ship's operation. Risks can be assessed by combining the evaluation of threats from the previous step along with known (and unknown) vulnerabilities, such as using default passwords or allowing all access to consider the potential harm and reduced benefits.

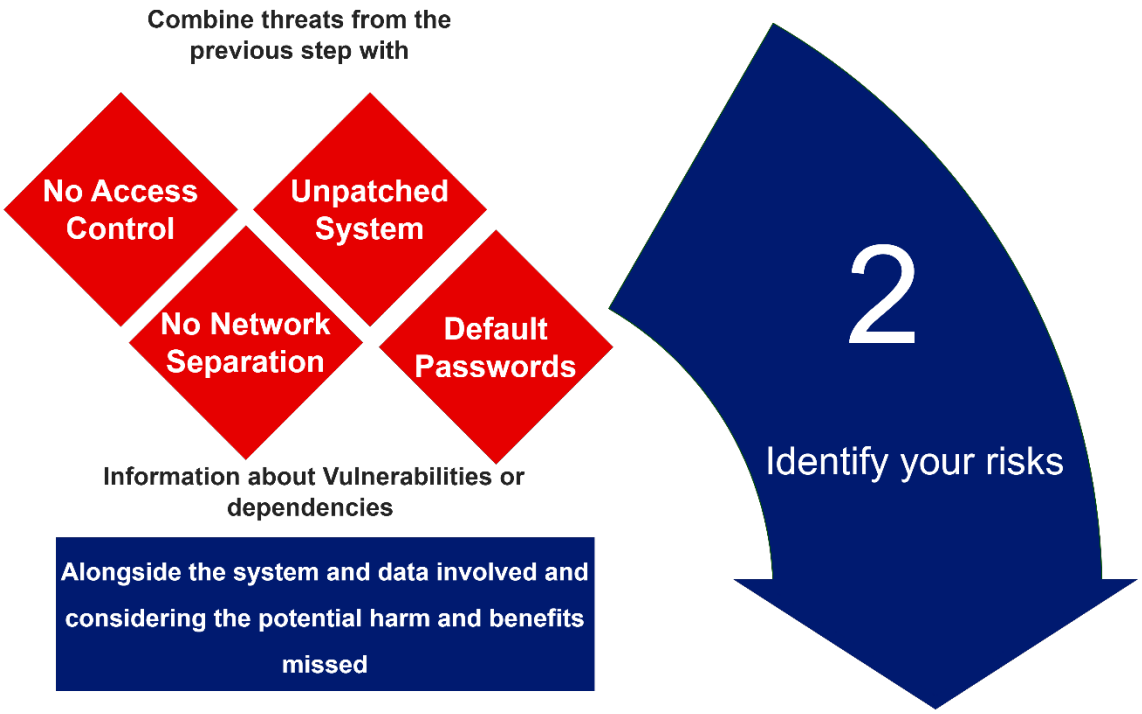


Figure 13: Identify your risk, combining threats from the previous step along with vulnerabilities.

Step 3: Measure the Risk Severity

Existing business risk evaluation techniques can be used on cyber security risks so that health and safety, financial and ship operational risks are all rated on a consistent scale. Risks can be measured quantitatively or qualitatively, e.g., given a monetary value or a value based on a consistent scale such as 1 to 5. Both quantitative and qualitative approaches have positives and negatives, but often a quantitative risk assessment approach to achieve a monetary value of the risk can be helpful when prioritising spending on controls. The challenge with a quantitative approach is calculating an accurate likelihood or probability of a risk occurring and an accurate impact value.

Typically, a qualitative risk matrix such as shown in Figure 14 is used to place risk within the wider business content and rate the level of risk. This style of risk assessment is generally used, and far easier to conduct than quantitative. In the example below, the risks within the top right corner (dark red in the image below) would be rated as very high or critical risks which are likely to have significant impact on the operation of the ship as well as high probability of occurring within the risk review period.

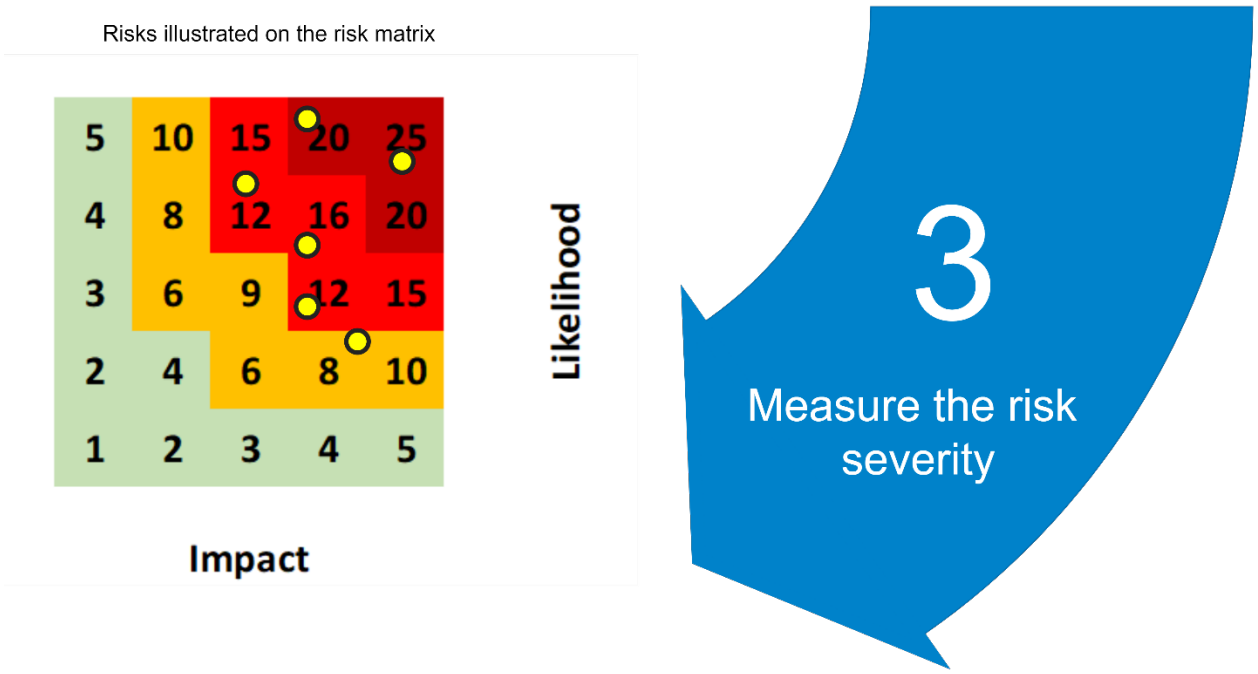


Figure 14: Measuring severity of the risk

Risks that are identified as part of the assessment may include but are not limited to:

- Malware infects a system through compromised USB. Cause: an attacker uploads malware to a USB and leaves it lying around near a ship. A staff member plugs this into a system and the malware is uploaded to the system. Effect: the system is infected with malware and may be not operational with confidentiality and integrity also at risk.
- An unpatched vulnerability is used to compromise a system. Cause: a high vulnerability has not been patched and it is used by an attacker to gain remote access to a service. Effect: an attacker can take remote control over an IT system (such as the Cargo Management System).
- Company data compromised by a data leak. Cause: a staff member uses their access to systems to download important company data they should not to a personal device, they then share this with another party. Effect: the company no longer has control of its data.
- A stolen access key card used to gain physical access. Cause: an attacker steals an access key card from a staff member when they are on shore. The attacker uses the key card to gain physical access to the ship and coupled with use of default credentials on several systems is able to alter the configuration of key equipment. Effect: The organisation has to spend time resetting all access cards and returning all configurations to operational.
- Default credentials used to compromise a system. Cause: the admin credentials on an installed system have not been changed from the default set by the supplier. Effect: an attacker leverages these to access the system and alter the configuration.

Step 4: Prioritise your Risks

Organisations will need to decide which risks to address first. Often the risk severity is the deciding factor, with the highest risk being treated first.

Organisations often set a risk appetite which is helpful when working on the activity to address risks. Risk appetites define the level of risk acceptable to the organisation. Any risk above this must be formally accepted or mitigated.

Step 5: Treat your Risks

Risks can be:

- Treated or mitigated. The implementation of controls or a plan to reduce the likelihood of the risk occurring or reducing its impact by changing the ways of working (for example, by reducing the criticality of a service).
- Tolerated or accepted. The risk is of a sufficiently low level to be accepted by the business and is tracked.
- Transferred or insured. The risk has been moved to another area of the business or insured against.
- Avoided. Stop activity which is the cause of the risk.

Risks that are treated or mitigated through the implementation of a control should be considered during this step.

Figure 15: Treatment of risks by the implementation of controls

The controls implementation is often assessed as part of the treatment plan. In the example above, six controls have been implemented and then RAG rated against their ability to remediate the risk:

- Access control, changing default credentials and blocking remotely accessible services were assessed as green because they have been implemented fully.They will likely reduce a number of risks and the residual risks will have been reduced significantly.
- Network segmentation has been partially implemented (for example, although the company has separate corporate IT and ship IT networks, some OT is connected to the internet via the ship network). The residual risk associated with these controls may have been reduced but not completely treated.
- Physical security, patching and updates have not been implemented and hence assessed as red. For physical security it may be that the access cards required to access the bridge are broken and therefore the door is propped open. On patching or updates it could be that the supplier of the software or hardware no longer releases patches.

Thus, risks reliant on these mitigating actions would not have been reduced and residual risks would still be at the level before treatment was agreed.

Step 6: Review your Risks

The final step of a CSA is to review the risks that have been assessed and articulate the residual risks that can inform the CSP.

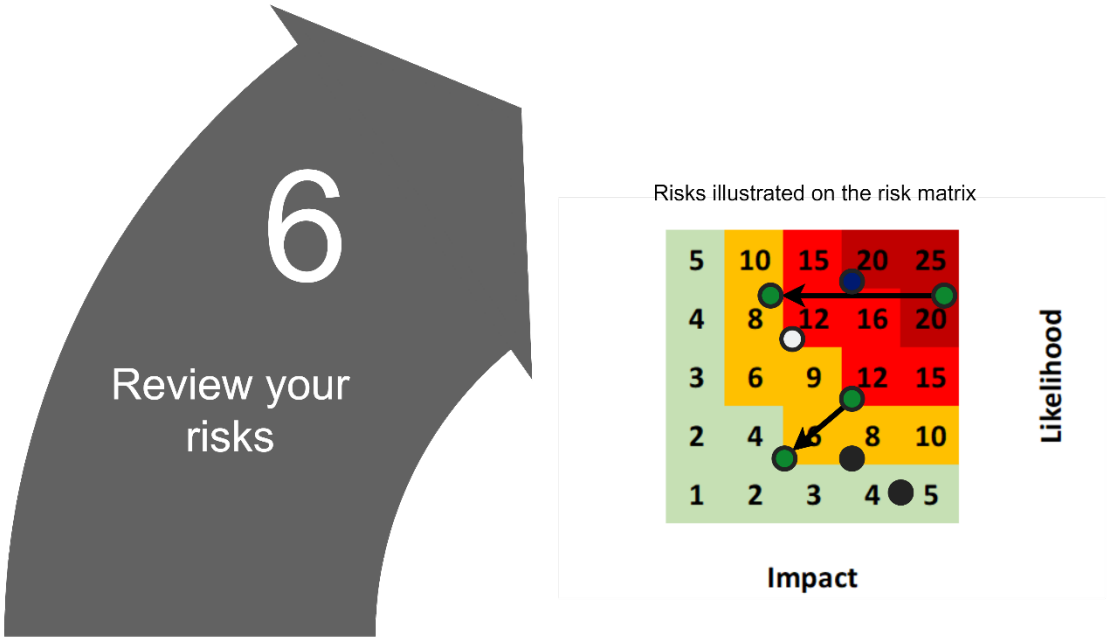


Figure 16: Review the risks and actions that have been taken

Cyber Security Plan (CSP)

A CSP is designed to track any issues identified in the CSA, any gaps in controls and further measures taken to protect against cyber risks, detect and minimise the impact of cyber events (CAF objectives B, C and D). The CSP should consider the impact of measures set out in the security plan for the ship and its systems. A holistic approach to the CSP will ensure that the document covers the physical, technological, personnel and process plans in place. Items to include are:

- Any risk mitigation measures;
- Any residual risks to the ship from cyber security not otherwise mitigated or transferred;
- Risk acceptance of any residual risks;
- The policies that set out the security-related business rules derived from the SSP;
- The processes in place and how they are implemented onboard when using the ship assets;
- Procedures with detailed instructions for repeatable and consistent delivery mechanisms;
- Responsibilities onboard and within the wider organisation around cyber security including the CySO and escalation routes;
- Plans in place for incidents including business continuity and disaster recovery;
- Testing plans in place for the CSP; and
- Legal jurisdiction questions during a voyage.

The CSP is a living document and should be reviewed regularly (typically annually) to ensure that cyber security plans remain relevant and up to date.

Figure 17: Annual review of the CSP and CSA

Annex D: Cyber Security Tools and Software

Overview

This annex has been provided for **guidance purposes only**, it provides a high-level and lightweight process for the assurance of both commercial and open-source software principally from third parties. Organisations can use a similar approach for hardware but further questions around supply chain and integration within a ship network will be pertinent.

The primary goal of software and IT tooling is to support the operation of business, i.e., they should be business enabling. Any software assurance process should foremost be considered from a business-enabling perspective and facilitation of the software to deliver on business goals. The goal of the assurance process is to ensure that any inherent security, commercial or data protection risks are identified and addressed prior to purchase (or use in the case of free software).

You should assure any new IT or OT product or service that is going to be used for business purposes, including both paid and open-source (“free”) products and services. (The terms and conditions for the use of free products or services may conflict with the company’s security, procurement, and data protection obligations).

Depending on the nature of the product or service and how it will be used, additional security checks will be required.

Assurance Process (Not an exhaustive list)

1. What is the product or service going to be used for e.g., what is the use case?

2. What is the business case for the software?

3. What type of product or service is it?

4. How many users of the product or service will there be?

5. What data will be stored and processed by the product or service?

- Confidential/Sensitive Personal information
- Personal Data
- Sensitive Organisation Information
- Organisational information
- Public Data

6. If processing personal data, have you undertaken a Data Privacy Impact Assessment?

7. How does the access control work for the software?

8. Will the software be connected to the internet?

9. Will the software be connected onto the ship's networks?

10. Who is responsible for the software?

11. Is the software open-source or provided by a vendor?

12. If Open-Source:

- What is the source?
- How often is the software updated?
- Are there any known security vulnerabilities?
- Does the licensing model prevent use?

13. If vendor:

- Have you reviewed the terms and conditions?
- How will the vendor provide patches?
- How long does the vendor commit to providing security updates?
- Does the vendor have the ability for users to report security issues?
- Does the vendor have any security certifications, such as ISO27001?

Annex E: Maritime Autonomous Surface Ships

Introduction

Recently Maritime Autonomous Surface Ships (MASS) have become of interest to shipping. Many ships already have some degree of automation inbuilt but this is expected to grow in the future. Using ships that change the requirements of personnel onboard not only reduces cost (through increasing onboard space, efficiency and reducing crew requirements) but also presents a smaller lifestyle adjustment and risk for crew members. The IMO [41] and Lloyd's Register of Shipping [42] have proposed a degrees of autonomy for MASS that may be useful when considering cyber risk.

The maritime accident report from Japan's Coast Guard [43] shows that over 80% of accidents in 2018 were due to human error, thus automation may represent an opportunity to increase the safety of vessels. With fewer people on a ship there is increased reliance on technology for communication, maintenance and decision making.

A level of automation is present on many modern ships, for example, automatic heading is mandated on any vessel of at least 10,000 GT. However, there are several barriers to the uptake of fully autonomous ships; fully autonomous vessels are much more complex due to the many systems (and, historically, crewmembers) required for safe sailing. Also ships on longer voyages often require onboard maintenance which would not be possible for an autonomous ship.

There are a range of ongoing projects in the automation sphere including Fugro [44], Ocean Infinity [45] and the Norwegian Forum for Autonomous Ships (NFAS) [46]. In the UK, the Maritime and Coastguard Agency are working with industry to ensure that any legislation or guidance is practical for MASS, with the MCA MGN664 providing the guidance to industry on the process for certifying innovative technology on vessels [47]. For the wide adoption of unmanned ships, there will need to be guidance and an increase in their presence in national and international rules and regulations, especially regarding liability and seaworthy assessments of machine code.

Cyber Security Approach to MASS.

Whilst automation carries benefits, the cyber security risk associated with increased automation may also increase due to further reliance on technology. This is especially true when a vessel is completely reliant on its cyber systems for complex tasks and decision

making. Remote Operation Centres (ROCs) should also be considered within the cyber security risk assessment as access routes and attack points especially as they are connected to the cloud and spread across multiple locations and jurisdictions.

Research from the University of Plymouth [47] argues that as the level of automation of the ship increases, simultaneously threat actors require less skill to provide the same level of threat. This is due to fewer humans onboard to intervene in an attack and regain physical control of the vessel.

The common cyber security strategies of combining controls across technology, policy or procedures, and people, will place greater reliance on technology as automation increases. In order to successfully defend against an attack the shipbuilders and operators' resources, cyber security support, and security enforcing controls available will need to be greater than the criminals' capability.

The ability of threat actors to compromise ships increases, for example, scenarios such as remote takeover of a ship. These cases become more likely if controls are not robust. Poorly skilled actors who may use scripts or programs developed by others, pose a bigger threat compared to less automated vessels if the security protocols remain the same.

The top risks for MASSs are expected to be common with other maritime cyber security risks, with the addition of several risks related to the remote-control requirement and sensor-based decision making for safe operations. It is therefore expected that the following risks may have increased as a result of increased automation and should be considered by organisations when adopting MASSs:

- Remote access;
- Poor configuration of security enforcing functionality;
- Communications interference including jamming or spoofing;
- Loss of navigation control;
- Loss of situational awareness;
- AIS, GPS or GNSS manipulation;
- Failure of collision control systems;
- Other sensor interference;
- Man in the middle or eavesdropped communications;
- Use of default credentials;
- Interference between onshore centres and vessels.

It is recommended that organisations:

- Increase the strength of their technical security before they increase the level of automation;
- Undertake capability building of workforce and proficiency of operators; and,
- Work closely with manufacturers and regulators to ensure that automated vessels align to cyber security good practice.

Several new controls are recommended to reduce the overall risk associated with automation. These include the implementation of secure development processes such as, self-recovery or fail-safe/secure after an attack or loss of navigational control, and integrity checks for remote operator commands.

Within the Top 10 for shipping that the following considerations should be made for MASS:

- (1) Understanding Data, MASS may use third party data sources and it is important to consider the risk to highly automated systems where data may be manipulated by third parties and impact operations.
- (7) Vulnerability Management, recommended considering system shutdown during maintenance which may not be possible or desirable for MASS as system are often design to be maintained remotely and remain in operation. You should undertake a risk assessment and ensure you have appropriate controls.
- (8) Design for Resilience, mentioned that backup may not be possible when a ship is underway but some MASS have this built in by design.

As remote operations are a changing field this annex does not provide an exhaustive list of threats, risks and controls but should act as a guide and provide insight into the new challenges that lie ahead with the adoption of MASS.

Annex F: Bibliography and References

The bibliography and reference list below provide details of the sources and other works consulted during the work to update this document, it is not exhaustive and does not include stakeholder interviews conducted.

[1] National Cyber Security Centre, “NCSC updates and resources for heightened threats,” [Online]. Available: https://www.ncsc.gov.uk/section/keep-up-to-date/heightened-threat. [Accessed January 2023].

[2] Allied Market Research, “Autonomous Ships Market by Level of Autonomy (Semi-autonomous and Fully-autonomous), Ship Type (Commercial, Passenger, and Defense), Component (Hardware and Software) and Fuel Type (Carbon Neutral Fuels, LNG, Electric, and Heavy Fuel Oil/Marine Engine Fue,” 2020.

[3] Sophos, “State of Ransomware 2022,” Sophos, 2022.

[4] Sophos, *State of Ransomware 2022 Infographic,* 2022.

[5] O. Jacq, “Advanced Database of Maritime cyber Incidents Released for Litterature (sic),” 2023.

[6] International Maritime Organisation, “International Ship and Port Facility Security (ISPS) Code,” 2004.

[7] Department for Transport, “Ports and Port Systems Cyber Security Code of Practice,” 2020.

[8] *UK Statutory Instrument 2019 No. 308,* 2019.

[9] *UK Statutory Instruments 2004 No. 1495,* 2004.

[10] *UK Statutory Instrument 2009 No. 2048,* 2009.

[11] International Maritime Organisation, “MSC-FAL.1-Circ 3,” IMO, London, 2017.

[12] IMO Maritime Safety Committee, *MSC Session 98 Resolution 428,* London, 2017.

[13] HM Government, “Government Cyber Security Strategy 2022 to 2030,” HM Government, London, 2022.

[14] HM Government, “National Strategy for Maritime Security,” HMG, London, 2022.

[15] BIMCO et al., “Guidelines for Cyber Security on Ships,” 2017.

[16] National Cyber Security Centre, “10 steps to cyber security,” 2021. [Online]. Available: https://www.ncsc.gov.uk/collection/10-steps.

[17] National Cyber Security Centre, *Cyber Assessment Framework v3.1,* London, 2022.

[18] JOINT TASK FORCE, “SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS NIST 800-53 rev 5,” National Institute for Standards and Technology, 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[19] National Cyber Security Centre, “GDPR Security Outcomes,” [Online]. Available: https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes.

[20] National Cyber Security Centre, “NCSC VPN device security guidance,” [Online]. Available: https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks.

[21] National Cyber Security Centre, “Secure Sanitisation Storage Media Guidance,” [Online]. Available: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media.

[22] Centre for the Protection of National Infrastructure, “Secure Destruction Guidance,” [Online]. Available: https://www.cpni.gov.uk/secure-destruction-0.

[23] National Cyber Security Centre, “Asset Management Guidance,” [Online]. Available: https://www.ncsc.gov.uk/guidance/asset-management.

[24] National Cyber Security Guidance, “NCSC Device Security Guidance for bring your own devices,” [Online]. Available: https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device.

[25] National Cyber Security Centre, “Introduction to identity and access management,” [Online]. Available: https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management.

[26] National Cyber Security Centre, “Cyber Assessment Framework v3.1, b.2 identity and access control,” [Online]. Available: https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/b-2-identity-and-access-control.

[27] NIST, “NIST 800-53 v5.1 Access Control Family,” [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/controls?version=5.1&family=AC.

[28] NIST, “NIST SP800-53 v5.1 Identity and Authentication Family,” [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/controls?version=5.1&family=IA.

[29] National Cyber Security Centre, “Cloud Security Principles,” [Online]. Available: https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles.

[30] National Cyber Security Centre, “Top tips training package v4,” [Online]. Available: https://www.ncsc.gov.uk/training/v4/Top+tips/Web+package/content/index.html#/.

[31] National Cyber Security Centre, “Small organisation training v4,” [Online]. Available: https://www.ncsc.gov.uk/training/v4/Small+organisations/Web+package/content/index.html#/.

[32] National Cyber Security Centre, “NCSC Certified Training,” [Online]. Available: https://www.ncsc.gov.uk/information/certified-training.

[33] National Institute of Standards and Technology, “National Vulnerability Database,” [Online]. Available: https://nvd.nist.gov/search.

[34] International Association of Classification Societies, “IACS requirements for UR E26,” [Online]. Available: https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/.

[35] J. L, “Offline backups in an online world,” National Cyber Security Centre, [Online]. Available: https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world.

[36] MITRE, “MITRE ATT&CK,” [Online]. Available: https://attack.mitre.org/.

[37] National Cyber Security Centre, “CAF v3.1 c.1 Security Monitoring,” [Online]. Available: https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/c-1-security-monitoring.

[38] “Where to Report a Cyber Incident,” [Online]. Available: https://www.gov.uk/guidance/where-to-report-a-cyber-incident.

[39] National Cyber Security Centre, “Report a Cyber Security Incident for Operators of Essential Services,” [Online]. Available: https://report.ncsc.gov.uk/.

[40] International Standards Organisation, *Asset management - overview, principles and terminology,* 2014.

[41] International Maritime Organization (IMO), “Autonomous shipping,” [Online]. Available: https://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx. [Accessed 9 December 2022].

[42] Lloyd's Register, “Design Code for Unmanned Marine Systems,” February 2017. [Online]. Available: https://www.cdinfo.lr.org/information/documents/ShipRight/Design%20and%20Construction/Additional%20Design%20Procedures/Design%20Code%20for%20Unmanned%20Marine%20Systems/Design%20Code%20for%20Unmanned%20Marine%20Systems,%20February%202017.pdf. [Accessed 2 December 2022].

[43] K. Wariishi, “Maritime Autonmous Surface Ships: Development Trends and Prospects - How digitalization drives changes in the maritime industry,” Mitsui & Co. Global Strategic Studies Institute, 2019.

[44] Fugro, “Remote and Autonomous Solutions,” [Online]. Available: https://www.fugro.com/about-fugro/our-expertise/remote-and-autonomous-solutions. [Accessed 1 December 2022].

[45] Ocean Infinity, “Ocean Infinity,” [Online]. Available: https://oceaninfinity.com/ourtechnology/. [Accessed 14 April 2023].

[46] Yara, “Yara Birkeland,” [Online]. Available: https://www.yara.com/news-and-media/media-library/press-kits/yara-birkeland-press-kit/. [Accessed 1 December 2022].

[47] Maritime Coastguard Agency, *(M+F) Certification process for vessels using innovative technology,* 2022.

[48] K. Tam and K. Jones, “Cyber-Risk Assessment for Autonomous Ships,” May 2018. [Online]. Available: https://core.ac.uk/download/pdf/154422886.pdf. [Accessed 5 December 2022].

[49] B. Soyer, A. Tettenborn and G. Leloudas, “Remote Controlled and Autonomous Shipping: UK Based Case Study,” Institute of International Shipping and Trade Law, Swansea University, 2021.

[50] S. Cho, E. Orye, G. Visky and V. Prates, “Cybersecurity Considerations in Autonomous Ships,” Nato Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2022.

[51] HFW, “Autonomous Ships: Known Knowns and Known Unknowns,” 2022.

[52] Rolls-Royce and AAWA, “Autonomous ships: The next step,” 2016.

[53] S. Morgan, “Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021,” Cybercrime Magazine, 21 October 2019. [Online]. Available: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/. [Accessed 16 November 2022].

[54] S. Adam, “The State of Ransomware 2022,” Sophos News, 27 April 2022. [Online]. Available: https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/. [Accessed 16 November 2022].

[55] J. Edwards and L. Cameron, “Letter from the Information Commissioner,” 7 July 2022. [Online]. Available: https://ico.org.uk/media/about-the-ico/documents/4020874/ico-ncsc-joint-letter-ransomware-202207.pdf. [Accessed 16 November 2022].

[56] “DarkTracer : DarkWeb Criminal Intelligence,” Twitter, [Online]. Available: https://twitter.com/darktracer_int. [Accessed 16 November 2022].

[57] J. McFadden, A. Barrows and C. Reschovsky, “2016 Highlights of Ferry Operations in the United States,” Bureau of Transportation Statistics, 2017.

[58] Ferry Scan, “Silja Europa,” [Online]. Available: https://www.ferryscan.com/ships/Tallink-Silja-Silja-Europa-21460. [Accessed October 2022].

[59] New York City, “Staten Island Ferry Facts,” [Online]. Available: https://www1.nyc.gov/html/dot/html/ferrybus/ferry-facts. [Accessed October 2022].

[60] CruiseMapper, “Spirit of Britain ferry,” [Online]. Available: https://www.cruisemapper.com/ships/Spirit-of-Britain-ferry-1898. [Accessed October 2022].

[61] Britannica, “Ship,” [Online]. Available: https://www.britannica.com/technology/ship. [Accessed October 2022].

[62] YachtWorld, “150 passenger ferry,” [Online]. Available: https://www.yachtworld.com/yacht/2012-ferry-150-passenger-7447816/. [Accessed October 2022].

[63] I. Urbanyi-Popiołek, “The Economic Aspects of the ferry operator activity – selected issues,” *Ekonomiczne Problemy Usług,* vol. 119, 2015.

[64] Ferries.co.uk, “Find ferries from England,” [Online]. Available: https://www.ferries.co.uk/ferries_from_england.html. [Accessed October 2022].

[65] ITF, “Cruise Ships,” [Online]. Available: https://www.itfseafarers.org/en/issues/cruise-ships. [Accessed October 2022].

[66] CruiseMapper, “Cruise Ship Passenger Capacity,” [Online]. Available: https://www.cruisemapper.com/wiki/761-cruise-ship-passenger-capacity-ratings. [Accessed October 2022].

[67] The Hustle, “The economics of cruise ships,” [Online]. Available: https://thehustle.co/the-economics-of-cruise-ships/. [Accessed October 2022].

[68] CruiseMapper, “Cruise Ship Cost to Build,” 2015. [Online]. Available: https://www.cruisemapper.com/wiki/759-how-much-does-a-cruise-ship-cost. [Accessed October 2022].

[69] Boating Geeks, “How Much Does a Cruise Ship Cost to Operate?,” [Online]. Available: https://boatinggeeks.com/how-much-does-a-cruise-ship-cost-to-operate/. [Accessed October 2022].

[70] Assets America, “How Much Does A Cruise Ship Cost? | Ultimate Breakdown Guide,” 2020. [Online]. Available: https://assetsamerica.com/how-much-does-cruise-ship-cost/. [Accessed October 2022].

[71] Freightos, “TEU Shipping Containers, Meaning & Capacity,” [Online]. Available: https://www.freightos.com/freight-resources/what-are-teu-and-feu-shipping-containers/. [Accessed October 2022].

[72] Cargo Ship Voyages, [Online]. Available: https://www.cargoshipvoyages.com/. [Accessed October 2022].

[73] Universal Cargo, “How Much Cargo Can the Largest Shipping Container Ship Really Hold?,” 2018. [Online]. Available: https://www.universalcargo.com/how-much-cargo-can-the-largest-shipping-container-ship-really-hold/. [Accessed October 2022].

[74] M. Li, “Wan Hai pays $53m to buy chartered 2,700 teu box ship,” February 2022. [Online]. Available: https://theloadstar.com/wan-hai-pays-53m-to-buy-chartered-2700-teu-box-ship/. [Accessed October 2022].

[75] MI News Network, “Cargo Waiting Outside Ports In 2021 Racked Up Millions In Interest Due To Port Congestion,” January 2022. [Online]. Available: https://www.marineinsight.com/shipping-news/cargo-waiting-outside-ports-in-2021-racked-up-millions-in-interest-due-to-port-congestion/. [Accessed October 2022].

[76] Drewry, “World Container Index - 13 Oct,” 2022. [Online]. Available: https://www.drewry.co.uk/supply-chain-advisors/supply-chain-expertise/world-container-index-assessed-by-drewry. [Accessed October 2022].

[77] International Chamber of Shipping, “Bulk carriers,” [Online]. Available: https://www.ics-shipping.org/explaining/ships-ops/bulk-carriers/. [Accessed October 2022].

[78] Suisca Group, “Types of cargo ships according to the load they carry,” [Online]. Available: https://www.suiscagroup.com/en/noticias/types-of-cargo-ships-according-to-the-load-they-carry/. [Accessed October 2022].

[79] Trading Economics, “Iron Ore,” [Online]. Available: https://tradingeconomics.com/commodity/iron-ore. [Accessed October 2022].

[80] AHDB, “International grain prices,” [Online]. Available: https://ahdb.org.uk/cereals-oilseeds/international-grain-prices. [Accessed October 2022].

[81] Eastgate Shipping, “Dry bulk contracting activity and price trends,” 2021. [Online]. Available: https://www.breakwaveadvisors.com/insights/2021/11/19/dry-bulk-contracting-activity-and-price-trends. [Accessed October 2022].

[82] L. Papaeconomou, “Survey Of Operating Costs In Dry Cargo Shipping,” 2020. [Online]. Available: https://seekingalpha.com/article/4369718-survey-of-operating-costs-in-dry-cargo-shipping. [Accessed October 2022].

[83] Deloitte, “Challenge to the industry | Securing skilled crews in today's marketplace,” 2011.

[84] R. Sapra, “Cargo oil heating practices,” 2016. [Online]. Available: https://www.standard-club.com/fileadmin/uploads/standardclub/Documents/Import/publications. [Accessed October 2022].

[85] Marine Insight, “A Guide To Types of Ships,” August 2021. [Online]. Available: https://www.marineinsight.com/guidelines/a-guide-to-types-of-ships/. [Accessed November 2022].

[86] M. Kaushik, “What are Platform Supply Vessels (PSVs)?,” Marine Insight, May 2019. [Online]. Available: https://www.marineinsight.com/types-of-ships/what-are-platform-supply-vessels-psvs/. [Accessed November 2022].

[87] S. Whiteford, “How Offshore Oil Rigs Work,” 29 April 2021. [Online]. Available: https://www.onesteppower.com/post/offshore-oil-rigs. [Accessed November 2022].

[88] Offshore Energy Today Staff, “Seadrill sees rig dayrates improving in 2019-20,” 27 November 2018. [Online]. Available: https://www.offshore-energy.biz/seadrill-sees-rig-dayrates-improving-in-2019-20/. [Accessed November 2022].

[89] R. Pallardy, “Deepwater Horizon oil spill,” [Online]. Available: https://www.britannica.com/event/Deepwater-Horizon-oil-spill. [Accessed November 2022].

[90] Harmony Marine Shipbrokers, “Offshore Vessels,” [Online]. Available: https://www.hmsbroker.com/sale-type/offshore-vessels/. [Accessed 8 November 2022].

[91] S. PICO, “Prices on offshore vessels at rock bottom,” Shipping Watch, February 2018. [Online]. Available: https://shippingwatch.com/Offshore/article10309085.ece. [Accessed November 2022].

[92] S. Jalili, A. Maheri and A. Ivanovic, “Cost Modelling for Offshore Wind Farm decommissioning,” Interreg North Sea Regain Decom Tools, 2022.

[93] Maritime UK, “State of the Maritime Nation 2022,” Maritime UK, London, 2022.

[94] Mandiant, “Targeting of Israeli Shipping,” Mandiant, 2022. [Online]. Available: https://www.mandiant.com/resources/blog/suspected-iranian-actor-targeting-israeli-shipping .

[95] National Cyber Security Centre, “NCSC password guidance: updating your approach,” [Online]. Available: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach.

[96] National Cyber Security Centre, “NCSC Device Security Guidance,” [Online]. Available: https://www.ncsc.gov.uk/collection/device-security-guidance.

[97] National Cyber Security Centre, “NCSC zero trust architecture collection,” [Online]. Available: https://www.ncsc.gov.uk/collection/zero-trust-architecture/.

[98] National Institute for Standards and Technology, “NIST zero trust architecture publication,” [Online]. Available: https://www.nist.gov/publications/zero-trust-architecture.

[99] International Association of Classification Societies, *Recommendation No. 178 on incorporating cyber security into safety management systems,* 2022.

[100] International Association of Classification Societies, *Recommendation No 166 on Cyber Resilience,* 2022.

[101] National Institute for Standards and Technology, *Guide to Operational Technology (OT) Security 800-82r3,* 2022.

[102] Immarsat, *Beyond Compliance Cyber Risk Management After IMO 2021.*

[103] Norwegian Maritime Cyber Resilience Centre (NORMA), *Cyber Annual Threat Assessment 2022.*