UKP&I

CYBEROWL
a DNV company

Risk focus: Vessel cyber security

Guidance for crew

UK P&I CLUB
IS MANAGED
BY THOMAS
MILLER

Contents

Introduction **3**

Why maritime, why now? **4**

Common cyber threats and their impact **5**

Top 5 most common cyber threats to shipping 5

Common entry points and pathways **8**

7 'deadly sins' of insecure behaviour 9

How are shipowners and managers securing vessel systems? **11**

Identifying and assessing the cyber risks of key IT and OT systems 11

Developing protection measures 11

Developing detection and monitoring measures 12

Preparing response and contingency plans 12

Conducting regular training and exercising the response plans 13

How can you help reduce the risk? **14**

Industry standards and regulations **16**

General regulations and guidelines, based on size of vessel 16

Regulations based on age of vessel 16

Regulations based on cargo and route of vessel 17

Other survey requirements 17

How the crew can ensure compliance **18**

Maintaining hygiene in daily operations 18

Preparing for an audit / inspection 18

About us **19**

UK P&I Club 19

CyberOwl 19

Introduction

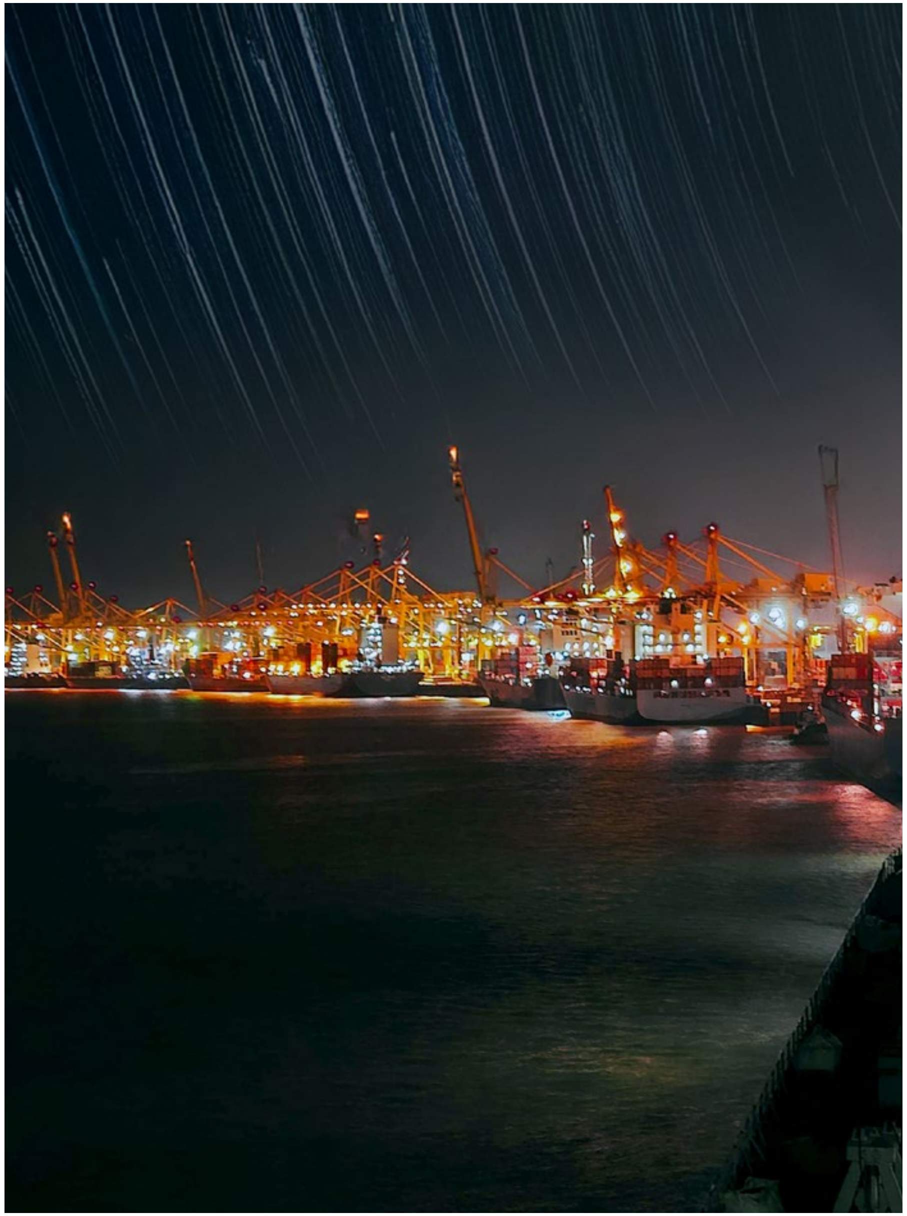
Since publishing the 2018 edition of Risk Focus: Cyber, the maritime sector has become more connected than ever before. There is an ongoing race to connect, digitalise and deliver smarter vessel systems that enable more remote access and support. The introduction of low earth orbit technology, such as Starlink and OneWeb, is enabling and accelerating this trend. However, this increased connectivity has also made vessels and their crews vulnerable. As such, the regulatory landscape has become more complex, with new requirements continuing to be applied to ensure systems on board vessels are secure and do not affect safe navigation and fleet operations.

It is becoming increasingly evident that human factors play a major role in managing the cyber risks of onboard systems. Based on analysis by CyberOwl, the leading maritime cybersecurity specialist, the majority of cybersecurity incidents can be traced back to human error *intentionally* or *unintentionally* creating cyber vulnerabilities. On the other hand, due to the technology environment on board vessels, humans still play a critical role in cyber incident response, with 26% of vessel cyber incidents during 2024 related to human factors and over 75% of these incidents requiring response actions that involve the crew.[1]

Given this, the 2025 edition of Risk Focus prioritises key guidance for crew on how to prevent and minimise cyber risks to onboard systems. This report also briefly looks at how cyberattacks have grown over the years, the key risks the industry is facing and how industry standards are helping to deal with these risks.

We have also included memorable posters that can be displayed on board and serve as reminders to the crew and visitors on vessels of the key dos and don'ts to mitigate cyber risks to systems on board vessels.

To download or order copies of posters or stickers click here.



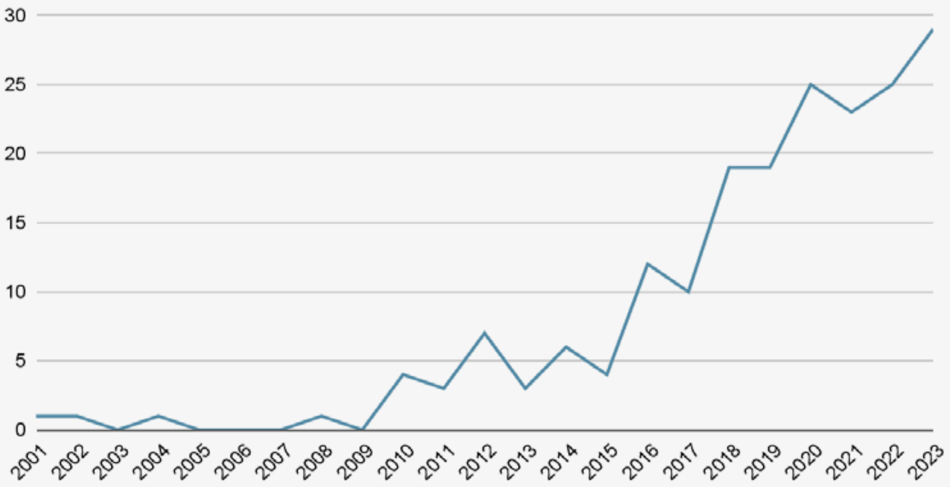
[1] Global Industry Report: The Lifecycle Dilemma by Thetius, HFW and CyberOwl.

Why maritime, why now?

Cyberattacks in the maritime sector have been steadily increasing and evolving. This has been confirmed by multiple sources analysing cyberattacks in the maritime sector in the last decade. One such database, compiled by researchers at NHL Stenden University, Netherlands, has catalogued around 165 incidents of cyberattacks on maritime systems to date. The creators of the database have disclosed that these open-source recorded incidents are just the "tip of the iceberg". However, the trend is clear: the number of attacks each year is increasing.

Experts assessing the security of systems on board vessels have long warned that these systems are vulnerable to cyberattacks. Given this, why are successful attacks increasing? Why now? Significant shifts in the maritime sector in recent years are contributing to this:

Publicly known cyber attacks on maritime systems, 2001-2023



Maritime Cyber Incidents by Year 2001-2023, based on data from Maritime Cyber Attack Database (MCAD), NHL Stenden University, Netherlands. https://www.nhlstenden.com/en/maritime-cyber-attack-database

- **Increased awareness of the sector**. The maritime sector has generally been operating under the radar, invisible to most people. The coronavirus pandemic fundamentally changed this. It suddenly raised awareness and understanding of the importance of shipping. In addition, a number of very high-profile incidents have further thrust shipping into the global spotlight.
- **Increasing connectivity and digitalisation**. Vessel systems and operations are changing towards more connected and digitalised environments in order to achieve improved operational efficiency and decarbonisation targets. This race to connect, digitalise and deliver smarter vessel systems can make vessels vulnerable to cyberattacks. The accelerating adoption of low earth orbit technology also makes it easier to access vessel systems remotely, where previously cyberattacks were made more difficult by limitations in connectivity and bandwidth.
- **A sustained period of profitability**. The maritime sector (across most cargo types) has experienced a few years of unprecedented revenue and profitability growth. This makes the sector attractive to criminal activity.
- **Increase in geopolitical tension**. In particular, the Russia-Ukraine conflict and tensions in the Middle East have led to a rise in malicious activity through the means of cyberattacks. This has included targeting of the maritime systems and communications infrastructure on which the sector relies.

Common cyber threats and their impact

A report by DNV[2] found that one in three maritime professionals experienced at least one cyber attack in the 12 months to October 2024. This equates to an average shipping company experiencing somewhere between 65 and 80 cyber risk events (incidents and near misses) a year. Analysis of these incidents reveals the Top 5 most common cyber threats affecting fleet management, vessel operations and systems on board vessels.

Top 5 most common cyber threats to shipping

1. Fraud through business email compromise

What is it? A type of attack that involves criminals gaining access to, or impersonating, a work email to trick someone into disclosing information or transferring money. There is increasing evidence of criminals varying their methods by using social media, messenger applications (such as WhatsApp or WeChat) or a combination of communication channels, in addition to email, to achieve their goals.

How does this affect shipping operations and crew? The most common impact of this threat is loss of funds due to unintentional transfers or payments to criminals. In 2024, the maritime sector experienced a broad spectrum of financial losses, with incidents resulting in amounts ranging from tens of thousands to millions of US dollars. While this type of attack most commonly affects shore-based finance or management teams, there have also been a notable number of incidents involving digital 'cash-to-master' transactions.

2. Malware, particularly ransomware

What is it? Short for malicious software, malware is a piece of software that is designed to intentionally harm a computer, network or server. The most common malware threat in shipping is ransomware, a type of malware that blocks access to a computer system or the data stored on it, until a ransom is paid. Malware is particularly risky because it is generally designed to spread across machines easily, either via the network or through removable devices such as USB, or via email.

How does this affect shipping operations and crew? According to analysis by CyberOwl, 60% of vessels cyber incidents during 2024 relates to malware. As ransomware results in locked or blocked access to computers or data, the impact is generally either operational downtime or higher workloads due to having to implement manual workaround processes. Even in cases where the ransom is paid, the threat actor may not be able to successfully unlock the affected systems or data. To date, the largest financial exposures to shipping companies have involved ransomware impacting cargo and scheduling systems or data, resulting in severe delays in vessel operations. Ransomware could also have a significant safety impact if the affected system is critical to the safe navigation of the vessel.

Real-world case study

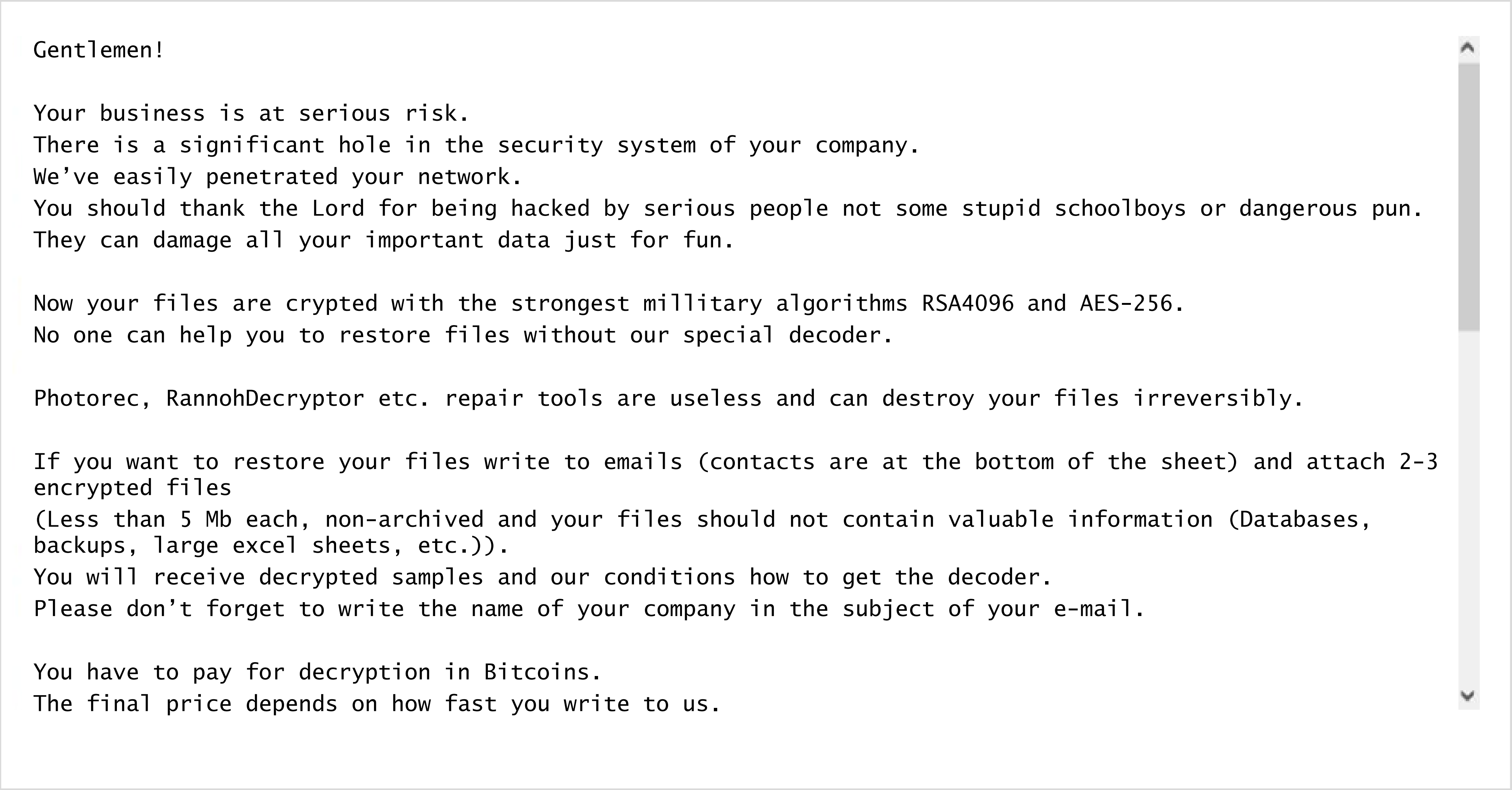
All four of the world's largest containership companies have been hit by malware and ransomware attacks over the past few years[3] – APM-Maersk (2017), COSCO (2018), MSC (2020) and CMA CGM (2020).

In the case of Maersk, the outcome of the malware attack resulted in significant operational disruption in 76 ports across the globe and nearly 800 vessels,[4] including containerships carrying tens of millions of tonnes of cargo, representing close to a fifth of the entire world's shipping capacity. For the Maersk crew, this led to confusion around planned journeys, loss of access to applications that they relied on and a heightened security risk for crew safety.

[2] DNV Maritime Cyber Priority Report 2024/25

[3] Article on ZDNET: "All four of the world's largest shipping companies have now been hit by a cyber attack."

[4] Article on Tradewinds: "Every second counts in cyber attack on automated ports and ships."



```
Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We’ve easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous pun.
They can damage all your important data just for fun.

Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet) and attach 2-3
encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information (Databases,
backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don’t forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
```

Example screenshot of a ransomware note (source: CyberOwl)

3. Data theft

What is it? Unauthorised stealing (access, transfer and storage) of data. Generally, this data contains personal, confidential, sensitive or financial information. In shipping, this can include passwords, the personal or financial data of crew or employees of the shipping company, commercially-sensitive data on the cargo, or the vessel's schedule or customers.

How does this affect shipping operations and crew? The impact of data theft depends on how the threat actors decide to use the stolen information. Example impacts in shipping and logistics include criminals using the stolen information to target cargo theft[5] or carry out espionage activities,[6] or fraudsters using the personal and company data collected to attempt acts of fraud against the crew or employees of the shipping company, or their friends and family.

Real-world case study

The Port of Lisbon experienced a cyber attack that involved data theft in 2023.[7] The attack was attributed to LockBit, one of the most prolific and widespread cyber criminal gangs at the time. Data stolen included financial reports, audits, budgets, contracts, cargo information, vessel logs, crew details, customer personally identifiable information, port documentation and email correspondence. LockBit threatened to publish all the data unless the Port of Lisbon met its ransom demands of $1.5 million.

4. Knocking down systems through denial of service (DoS)

What is it? An attempt to disrupt or shut down the normal function of a computer system by overwhelming it with a flood of requests or communications. This can result in the target computer system slowing down in performance or completely crashing, or legitimate access to that system being blocked.

How does this affect shipping operations and crew? Within the maritime sector so far, DoS attacks have been primarily targeted at paralysing port or terminal management systems and container booking systems. There is limited evidence of DoS attempts on systems on board vessels to date. One reason for this could be limitations in satellite connectivity and bandwidth to enable a successful DoS attack. However, with increasing satellite connectivity, it is becoming increasingly important to be vigilant, given the potentially devastating impact of rendering systems inoperable or cutting off all communication to shore.

5. Falsifying AIS or GNSS data via 'spoofing'

What is it? AIS spoofing is the deliberate manipulation of automatic identification system (AIS) data to deceive AIS tracking systems regarding a vessel's identity, position and other information. GNSS spoofing involves broadcasting fake or counterfeit satellite signals to deceive a Global Navigation Satellite System (GNSS) receiver. US Coast Guard Navigation Center reports[8] demonstrate an increase in such activity during 2023 and 2024 in regions with geopolitical conflict, such as the eastern Mediterranean, Black Sea, Red Sea, coastal waters of China and the Persian Gulf.

How does this affect shipping operations and crew? Such manipulation affects the reliability of equipment reliant on the accuracy of positioning, navigation and timing data. It creates confusing and potentially dangerous situations by misleading the user with false information, such as altering a vessel's identity, position or speed. If crew members are not properly trained to identify and handle such situations (for example, by reverting to visual navigation, reliance on dead reckoning positions or celestial navigation techniques), the safety of the vessel's navigation could be seriously compromised.

[5] Article on Seatrade Maritime News: "Cyber-attack allows pirates to target cargo to steal."
[6] Article on Maritime Executive: "Chinese spy malware found in European shipping companies' systems."
[7] Article on Port Technology: "Cyberattack threatens release of Port of Lisbon data."

[8] US Department of Transportation Maritime Security Communications with Industry (MSCI) Advisory 2023-013-Various-GPS Interference & AIS Spoofing

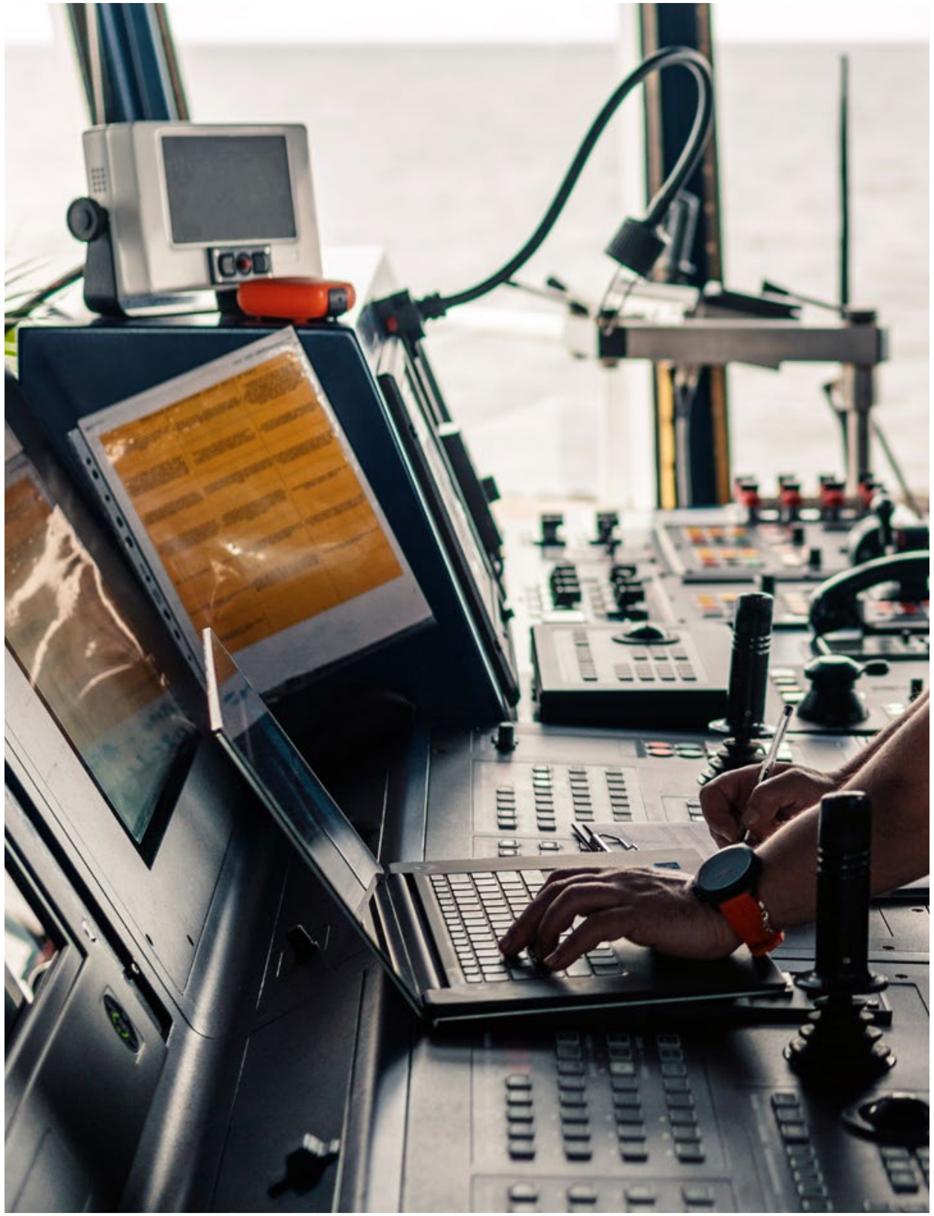
Common entry points and pathways

In order for a cyber attack to be successful, the threat actor needs to exploit points of entry into the computer systems, otherwise known as cyber vulnerabilities. The more entry points available, and the easier they are to exploit, the more likely the threat actor will be successful. Cybersecurity controls and policies are designed to reduce the number of entry points or make them harder to exploit.

Once a threat actor has managed to exploit an entry point, their goal becomes to continue taking steps and exploit further vulnerabilities until they reach their goal. This journey is commonly referred to as an attack pathway.

Human behaviour, whether by a member of the crew, visitors to the vessel or other shore-based remote users, has the potential to significantly impact the number of entry points and the ease in which they can be exploited. Any non-compliance with cybersecurity policies or other insecure behaviour, whether *intentional* or *unintentional*, increases the risk of vessel systems to cyberattacks. An analysis of cybersecurity incidents on vessel systems during 2023 and 2024 by CyberOwl shows that the majority of cybersecurity incidents can be traced back to human error *intentionally* or *unintentionally* creating cyber vulnerabilities.

The analysis demonstrates that there are some entry points that more commonly result in cybersecurity incidents than others. We have called this the **7 'deadly sins' of insecure behaviour** that result in the most common cybersecurity incidents.



7 'deadly sins' of insecure behaviour

1. Payments to unvalidated parties

Payments made to fraudulent parties pretending to be legitimate suppliers.

Examples of risky behaviour: Making payments before checking the accuracy of bank account details or complying with requests to change the bank account of the payee before checking the validity of the requestor. Ideally, checking and confirming the validity of the requestor should be done verbally over the phone.

How could this impact? Payments to fraudsters could result in financial losses. In many cases, this is impossible to recover.

2. Insecure use of removable devices

Poor control of removable devices such as USB, external hard drives or mobile phones creates the risk of spreading malware. This risk is particularly severe in cases where the removable device is passed between information technology (IT) and operational technology (OT) systems.

Examples of risky behaviour: Plugging the same removable device interchangeably into personal computers (PCs), third-party devices, company IT equipment or OT systems, e.g. the Electronic Chart Display and Information System (ECDIS), the Global Maritime Distress and Safety System (GMDSS), or other operational panels and the human-machine interfaces of OT systems, without scanning that removable device for malware.

How could this impact? Despite best efforts to secure systems, it remains common for malware to get onto PCs or company IT equipment. If this occurs undetected, a key mitigation is to limit the potential for that malware to spread across different computers, particularly OT systems that may be critical for safe navigation. Plugging the same removable device into multiple machines, without first scanning and cleaning the device, risks facilitating the spread of the malware onto other machines via the infected removable device.

3. Insecure links

Clicking on insecure links that lead to suspicious or malicious websites.

Examples of risky behaviour: Clicking on links in emails from unknown or untrusted sources. Clicking on links sent via messaging services or apps, e.g. WhatsApp or WeChat.

How could this impact? A very common technique that threat actors use is to create malicious websites that are designed to stealthily load malware onto the unsuspecting user's machines. The threat actors then send a link to these websites via emails or messages designed to tempt the reader into clicking the links that load these websites.

4. Insecure network connections

Connecting insecure equipment to critical vessel networks creates a risk of spreading malware or unintentionally giving threat actors remote access to critical equipment.

Examples of risky behaviour: Enabling the hotspot of vessel computers and tethering personal devices such as PCs, mobile phones or tablets for internet connection. Connecting crew members' or visitors' personal devices to the vessel's internet network either via an ethernet cable or WiFi, without appropriate security processes.

How could this impact? IT teams are not generally able to deploy antivirus, anti-malware or other cybersecurity systems onto crew members' or visitors' personal devices. Given this, it is common for such equipment to go unprotected. Connecting such devices onto the critical vessel networks facilitates the malware spreading onto critical equipment. Connecting cellular-enabled mobile devices creates a further risk, by potentially enabling threat actors to gain remote access to critical shipboard equipment via 3G, 4G or 5G networks.

5. Unauthorised remote access

Providing remote access to unknown or unauthorised parties.

Examples of risky behaviour: Crew responds to an unplanned or unauthorised request from a third party claiming to be a vessel or equipment manufacturer to provide a remote connection to a vessel system. Crew provides remote access to an unknown IP address. Remote connections are left open long after the intended task has been completed.

How could this impact? Threat actors can trick crew into providing them with remote access to vessel systems by pretending to be legitimate manufacturers and vendors. Once they have remote access, they can perform further malicious activity such as gaining control of systems, deploying malware or performing data theft.

6. Risky software downloads

Downloading unapproved, unwanted or risky software that may contain malware or severe vulnerabilities.

Examples of risky behaviour: Downloading software from unknown or untrusted sources. The most common risky software downloads in 2023 and 2024 included PDF editors, image editors and computer games. Crew often download PDF or image editors with the good intention of trying to edit a document required to complete vessel or port operations. However, this unintentionally introduces cyber risk.

How could this impact? Downloading unknown and unauthorised software can introduce malware or vulnerabilities to the shipboard systems. Beyond this, unwanted software can also slow shipboard systems down with unwanted functionality, such as repeatedly displaying pop-up advertising.

7. Supply chain attacks

This occurs when a shipping company inadvertently provides access to a threat actor through the computer systems of a maritime supplier.

Examples of risky behaviour: Overly trusting connections to third-party systems without validating their legitimacy. Poor control of remote access provided to third parties (see the section 5 related to 'unauthorised remote access' above). Allowing visitors to the vessel to connect PCs or USB devices to vessel systems without scanning such devices for malware beforehand.

How could this impact? When a supplier's systems are compromised, this could impact a shipping company (the supplier's customer) in multiple ways. Examples of this include the disruption of a supplier's services to the shipping company or vessel, 'piggy-backing' off a supplier's remote access to gain access to its customer's systems or simply gathering intelligence to impersonate a supplier to attempt fraud. In 2023, there were 242 claimed supply chain attacks in the United States alone. This is the highest reported number since 2017. Overall, supply chain attacks saw a year-over-year increase of 115% between 2022 and 2023.

How are shipowners and managers securing vessel systems?

The International Maritime Organization (IMO) introduced Resolution MSC.428(98) requiring shipping companies to include consideration of cyber risks within their Safety Management Systems (SMS) from 1 January 2021. Since then, shipping companies have been gradually taking measures to secure systems on board their vessels. Across shipping companies, there has been a very wide range of investments made to date, resulting in varying levels of maturities in cybersecurity controls. However, shipping companies performing best practices have, as a minimum, put in place a number of cyber risk mitigations. It is meaningful for crew members to get a general understanding of these and their role in ensuring these mitigations are in place.

Identifying and assessing the cyber risks of key IT and OT systems

Having a clear understanding of the asset inventory of all systems on board vessels is a critical starting point in any cyber risk management system. The saying goes that "you can't protect what you don't know". A good inventory incorporates details of all the hardware and software of each system on board the vessel, details of how each system is connected (to other systems and/or the internet) and the network zones they sit within. A risk assessment can then be completed, evaluating the key vulnerabilities and mitigating measures that have been put in place to protect against the vulnerabilities.

How to ensure this is in place

- Review the documentation related to asset inventory and cyber risk assessment.
- Get a high-level understanding of the list of mitigating measures that have been considered.
- Inform the IT team if you can identify any systems that have not been documented.

Developing protection measures

There is a long list of protective controls that can be implemented. The key ones include:

- Network segmentation – ensuring there is appropriate separation of critical systems so that malicious actors cannot easily hop from one system to another or malware cannot easily spread.
- Network protection – the main example of this is firewall technology to help keep intruders outside the protected vessel networks.
- Antivirus or anti-malware – these are software technologies that protect shipboard computers from malware.
- Access control – either physical access control (e.g. locks) or digital access control (e.g. login access control) to limit access to critical networks and systems, whether directly, wirelessly or remotely.
- Removable devices control – limiting the ability to connect mobile or removable devices, e.g. USB , external hard drives or mobile phones.

How to ensure this is in place

- Review the cyber risk management plan within the company's SMS.
- Get a high-level understanding of the list of protective measures that have been implemented on board the vessel.
- Inform the IT team if you suspect there are any protective measures that are not working or have not been implemented properly, e.g. expired antivirus licences, or admin access or WiFi access where there shouldn't be.
- Inform the IT team if you identify any anomalies in the computer systems.
- Educate crew on the importance of security controls and ensure they do not attempt to circumvent any restrictions as a short-cut to following the correct procedures.

Case study: MSC [one of the largest container shipping companies] strengthens access control for vessel WiFi

Mediterranean Shipping Company (MSC) has put in place strict controls over access to WiFi on board vessels and access to vessel computer systems. Each individual is provided with a personal account that is verified by the shore IT team. Crew members receive login details via the dedicated company application. Visitors who are not crew can obtain temporary login details with restricted access, but only if approved by the Master and the shore IT team.

This preventative measure balances providing crew and visitors with the flexibility of WiFi connectivity, but ensures that the level of access to critical systems is limited.

Developing detection and monitoring measures

Even with significant investments in protective measures, it is not possible to completely prevent a cyber attack. This is because threat actors are constantly updating their methods and tactics, and systems are continuously being upgraded, potentially giving rise to new vulnerabilities. Given this, an effective cyber risk management system should have a system in place for detecting and continuously monitoring cyber risks.

Effective monitoring systems should be designed to identify known threats, anomalous activity and breaches in cyber policy compliance. Alarms should be generated where these are discovered so that qualified experts can triage, investigate and take mitigating actions to avoid any losses or damages.

How to ensure this is in place

- Ask the IT team what systems are in place to detect and monitor cyber risks to onboard systems.
- Understand the procedures for informing the crew about identified risks, as required.
- Gain clarity on whether there is 24x7 support for cyber emergency response.
- Inform the IT team if you identify any anomalies in the computer systems.

Preparing response and contingency plans

An incident response plan is developed to cover relevant contingencies and specify how to react to cybersecurity incidents. The plan often contains a predetermined set of procedures or instructions to detect, respond to and limit the consequences of cyber incidents. An increasing number of shipowners have also put in place backup systems that periodically back up the data from shipboard systems to computers located in different locations. This limits the impact of any cyberattacks resulting in the blocking of access to systems or data.

How to ensure this is in place

- Review the cyber incident response plan that should form part of the company's SMS.
- Understand your role during a cyber incident.
- Set up drills to ensure these procedures are well understood, should a cyber emergency arise.
- Gain clarity on who to contact in the case of an emergency.

Case study: Güngen Maritime & Trading A/S [medium-sized tanker owner] puts in place contingency and backup digital systems

Güngen has implemented a contingency backup system that periodically backs up data from vessel systems to data storage facilities located in a completely different environment to the company's shoreside and shipboard computers. The backup system creates a daily copy of data from shipboard computers.

This contingency measure means that even if the vessel suffers a ransomware attack, the shipowner can reformat its onboard computers and easily restore applications and data, with a maximum of only 1 day of data loss. Employees are given instructions on a simple procedure with step-by-step guidance on how to retrieve entire applications and data from the backup system.

Conducting regular training and exercising the response plans

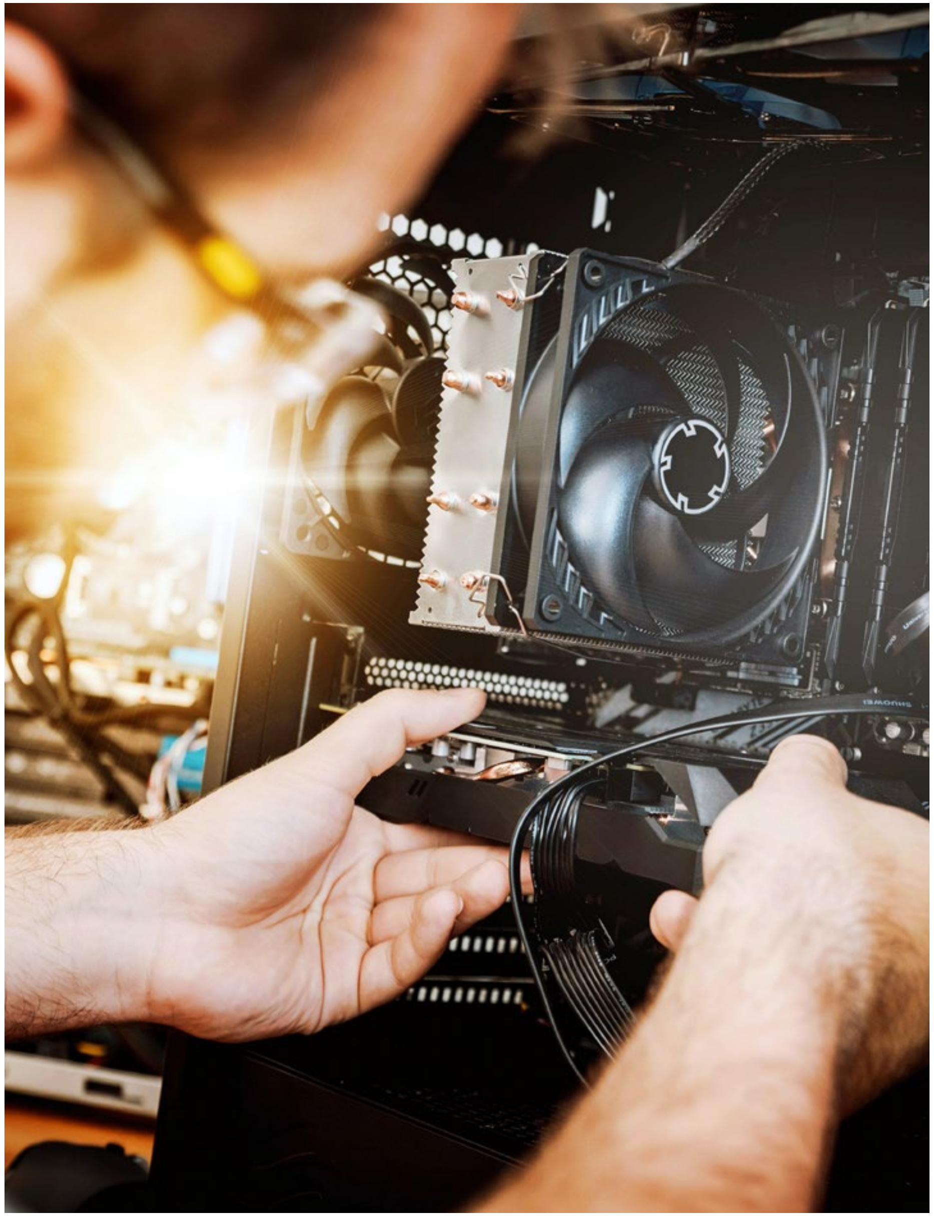
The International Convention for the Safety of Life at Sea (SOLAS) and the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) requires seafarers to familiarise themselves with and be able to effectively coordinate their activities in an emergency situation. Under the International Safety Management (ISM) Code, this now includes cyber risks and incidents. Shipowners should have in place an awareness programme for all onboard personnel, according to their role. Best practice shipowners have also included regular cyber emergency drills and exercises for their shore-based staff.

How to ensure this is in place

- Review all available cyber awareness training materials and understand your role in maintaining the cyber risk management plan.
- Ensure crew properly engage with drills and have a good understanding of the cyber emergency response plans.
- Gain clarity on who to contact in the case of an emergency.

Case study: Ionic Shipping (Management) Inc. [medium-sized tanker and bulker owner] puts in place a cyber training programme for crew

Ionic puts in place a staff induction process for new crew joining the company. Individuals receive training on cyber awareness and also their personal cybersecurity responsibilities when they are both sailing and on shore leave. In addition, all users receive regular refresher training sessions to maintain an updated understanding of risks, best practices and new regulations. The shipowner also conducts periodic crew-specific cybersecurity drills and simulations to ensure the crew understand how to respond during a cyber incident.

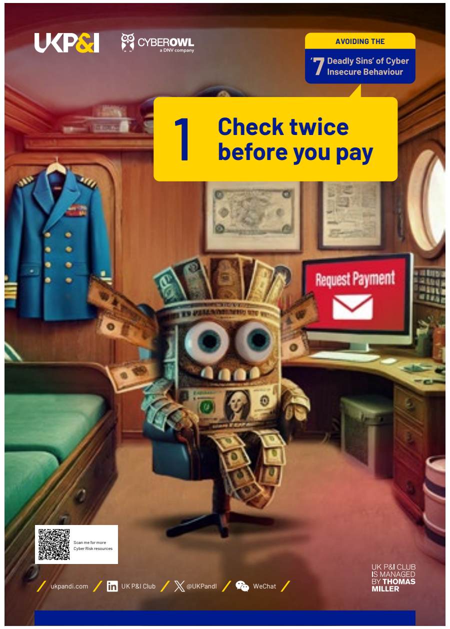


How can you help reduce the risk?

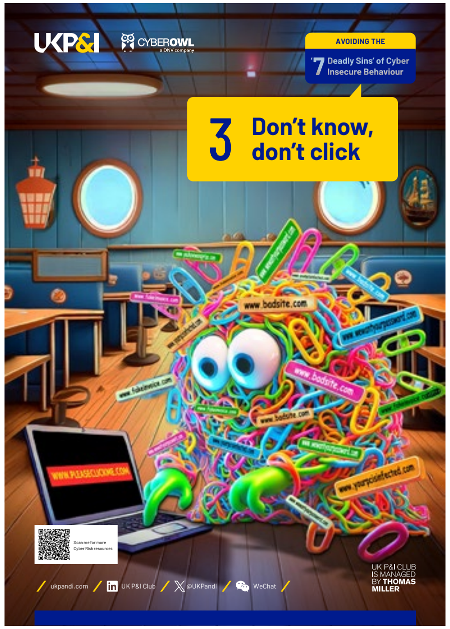
The vast majority of successful cyberattacks on shipboard systems occur when threat actors exploit 'back doors that are left open'. Humans are the weakest link in any network, but they are also the best defence. Ensuring that basic cyber hygiene is maintained can therefore go a long way towards keeping shipboard systems cyber safe. The crew have an important role to play in this.

In order to ensure good hygiene, there are rules for each of the 7 deadly sins that crew can follow to significantly reduce cyber risk to shipboard systems. These are summarised in this section. We have also designed posters that can serve as reminders of these 7 rules.

1. **Check twice before you pay**. Ensure that you are paying a legitimate payee and the bank account details are accurate by contacting the requestor direct, ideally verbally on the phone, before transferring any funds.
2. **Scan first, use second**. Scan a removable device for malware or virus before using it. This includes USB, mobile and portable devices (including external hard drives).
3. **Don't know, don't click**. Avoid clicking links from untrusted sources. If you're unsure about the sender of an email, links on a website or links in a document, don't click the link. Contact the Captain and/or your IT support team for further assistance.
4. **Don't try to fix it yourself**. Avoid changing any system configurations to work around security controls and policies. If there is an unexpected computing technical issue, ensure that you can still safely navigate the vessel, but avoid trying to fix the technical issue without the help of an expert.
5. **Confirm who is connecting**. Double check the legitimacy of anyone requesting remote connections. Pay particular attention if they request a change in process or IP address to enable connections, even if they appear to be a supplier you recognise. Check with the Captain and/or IT team before enabling remote connections, if you are unsure.
6. **Don't trust, don't download**. Avoid downloading any software that is not approved or is from untrusted sources.
7. **Report anything abnormal**. Do not ignore abnormal computer activity and assume it is system failure. Report such abnormal computer activity to the Captain and/or IT team.


UKP&I
CYBEROWL a DNV company
AVOIDING THE
7 Deadly Sins' of Cyber Insecure Behaviour
1 Check twice before you pay
Request Payment
Scan me for more Cyber Risk resources
ukpandi.com / UK P&I Club / @UKPandI / WeChat /
UK P&I CLUB IS MANAGED BY THOMAS MILLER

UKP&I
CYBEROWL a DNV company
AVOIDING THE
7 Deadly Sins' of Cyber Insecure Behaviour
2 Scan first, use second
Antivirus Scan Ready
Scan me for more Cyber Risk resources
ukpandi.com / UK P&I Club / @UKPandI / WeChat /
UK P&I CLUB IS MANAGED BY THOMAS MILLER


UKP&I
CYBEROWL a DNV company
AVOIDING THE
7 Deadly Sins' of Cyber Insecure Behaviour
3 Don't know, don't click
www.bodsite.com
WWW.PLEASECLICKME.COM
Scan me for more Cyber Risk resources
ukpandi.com / UK P&I Club / @UKPandI / WeChat /
UK P&I CLUB IS MANAGED BY THOMAS MILLER

UKP&I
CYBEROWL a DNV company
AVOIDING THE
7 Deadly Sins' of Cyber Insecure Behaviour
4 Don't try to fix it yourself
ERROR!
Scan me for more Cyber Risk resources
ukpandi.com / UK P&I Club / @UKPandI / WeChat /
UK P&I CLUB IS MANAGED BY THOMAS MILLER

UKP&I
CYBEROWL a DNV company
AVOIDING THE
7 Deadly Sins' of Cyber Insecure Behaviour
5 Confirm who is connecting
Scan me for more Cyber Risk resources
ukpandi.com / UK P&I Club / @UKPandI / WeChat /
UK P&I CLUB IS MANAGED BY THOMAS MILLER

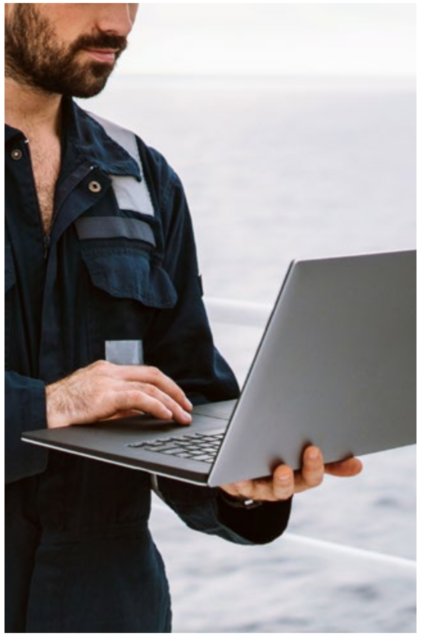
UKP&I
CYBEROWL a DNV company
AVOIDING THE
7 Deadly Sins' of Cyber Insecure Behaviour
6 Don't trust, don't download
DOWNLOAD
Scan me for more Cyber Risk resources
ukpandi.com / UK P&I Club / @UKPandI / WeChat /
UK P&I CLUB IS MANAGED BY THOMAS MILLER

UKP&I
CYBEROWL a DNV company
AVOIDING THE
7 Deadly Sins' of Cyber Insecure Behaviour
7 Report anything abnormal
???
Scan me for more Cyber Risk resources
ukpandi.com / UK P&I Club / @UKPandI / WeChat /
UK P&I CLUB IS MANAGED BY THOMAS MILLER

→ To download or order copies of posters or stickers click here.

Industry standards and regulations

As cyber risks continue to develop, the industry has been developing a set of rules and guides to help shipowners put in place an effective cyber risk management plan. It is important for crew to have general awareness of these regulations, as they provide guidance on cyber safety that impacts day-to-day vessel operations. The key regulations are highlighted in this section.



General regulations and guidelines, based on size of vessel

IMO resolution and guidelines

The IMO is an agency of the United Nations responsible for measures to improve the safety and security of shipping. The IMO defines the ISM Code, which requires vessels to have a Safety Management System (SMS) in place, and this is enforced by Flag States. IMO Resolution MSC.428(98) requires shipping companies to include consideration of cyber risks within their SMS. The ISM Code generally applies to all commercial vessels over 500GT.

Details of how cyber risks should be assessed and managed are not specified in the resolution itself, but the IMO has provided some initial guidance in MSC-FAL.1/Circ.3, which has been supplemented with a guidance document – The Guidelines on Cyber Security Onboard Ships – produced and supported by the International Chamber of Shipping, International Union of Marine Insurance, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, World Shipping Council and Superyacht Builders Association. Now in its 5th edition, the Guidelines on Cyber Security Onboard Ships is frequently referenced by auditors as a starting point for expected standards.

Class Notations

There are many different Classification Societies, of which 12 are members of the International Association of Classification Societies (IACS). These organisations provide classification, statutory certification and services as a Recognised Organisation acting on behalf of a Flag State. Classification Societies issue Notations, which are a record of the key features of a vessel. These features are generally audited each year to ensure the vessel remains compliant. Most Classification Societies have developed rules and Notation standards for cybersecurity, but these are not yet widely enforced or used (see next section on the IACS).

Regulations based on age of vessel

The IACS has introduced two new Unified Requirements for cyber resilience (UR E26 and UR E27) that are now being adopted by all member Classification Societies. This unification will help ensure common levels of cybersecurity across vessels with Notations from different members. Importantly, the IACS has also said that obtaining a cybersecurity Notation will be mandatory for all new vessels where the contract for building the vessel is signed after 1 July 2024. Crew will therefore be likely to encounter Classification Society audits of cybersecurity on new vessels from some time in 2026 when these vessels enter service.

Regulations based on cargo and route of vessel

Commercial cargo associations

These organisations exist to give independent assurance to the charterer or customer of a vessel that their cargo will be safely conveyed to its destination. These organisations are increasingly taking an interest in the cybersecurity of the vessel and are likely to ask questions during a survey. OCIMF and RightShip have published guidance for their surveyors which includes asking specific questions on cyber risk management plans and details of required supporting evidence.

dcsa

INTERCARGO

INTERTANKO

OCIMF

RIGHTSHIP

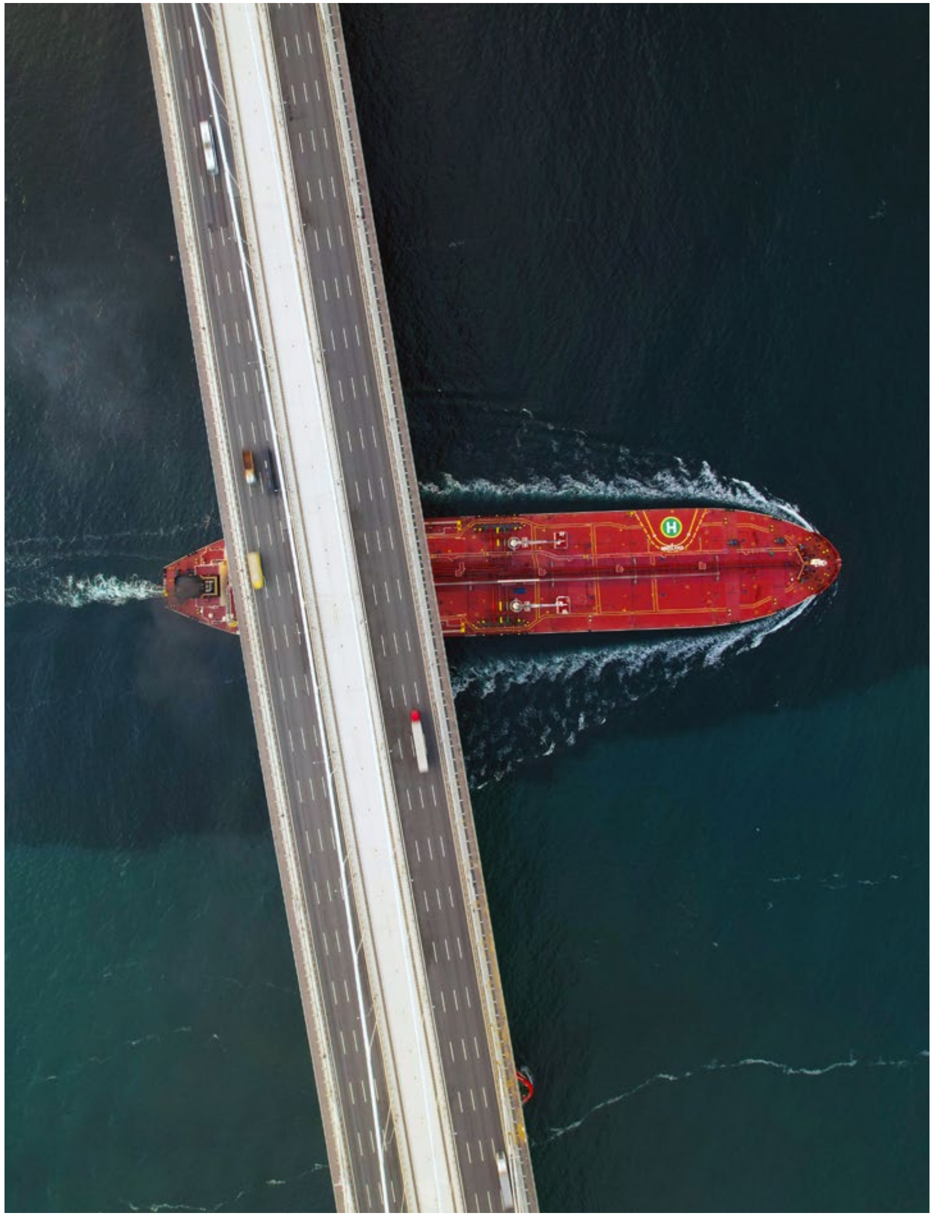
Port State Control

Nations may require vessels to meet certain requirements before allowing them to call at ports. The United States Coastguard (USCG) is the most advanced with setting out requirements relating to cybersecurity[9]. Vessels calling at US ports can expect to be asked about their cybersecurity controls and practices.

If a Port State Control inspection identifies a deficiency, the vessel may well be detained until the issue is resolved or may be subject to other penalties.

Other survey requirements

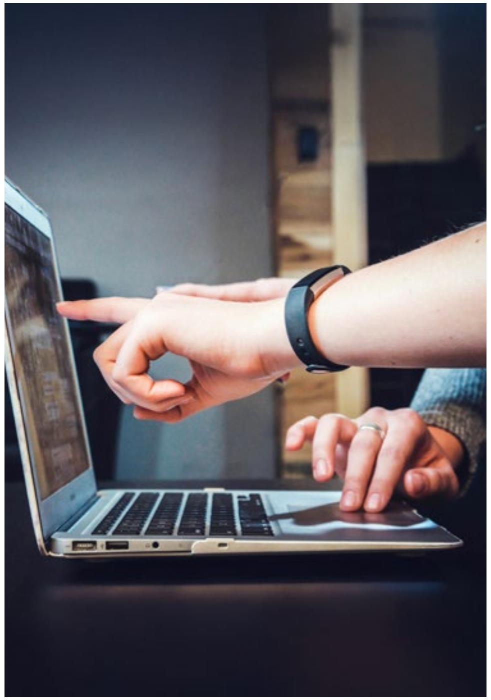
Various other commercial or legal requirements for cybersecurity may apply to a vessel. For instance, a vessel that is deemed to be part of a nation's critical infrastructure may be subject to the Network Information Security Directive (NIS-D) requirements in the EU. Alternatively, if a vessel's insurance covers cyber risk, then the insurance company may want to conduct an audit.



[9] Coast Guard Maritime Industry Cybersecurity Resource Website

How the crew can ensure compliance

In the majority of shipping companies today, the responsibility for complying with maritime cybersecurity regulations is still mainly seen as resting on the shoulders of the IT team. However, the crew have a critical role to play in cyber compliance.



Maintaining hygiene in daily operations

Crew members can help ensure compliance with cyber regulations in daily vessel operations by following these guidelines:

- Be familiar with the cybersecurity policies, processes and procedures in the company's SMS.
- Strictly adhere to the established policies. Where exceptional temporary workarounds are required, make sure you inform the IT team.
- Complete cybersecurity awareness training and participate in cyber emergency response drills to make sure you know what to do during a cyber emergency.
- Report any suspicious activities or potential security breaches immediately.
- Know where to find documentation relating to the vessel cyber risk management plan.

Preparing for an audit / inspection

Audits and inspections can be both stressful and time-consuming for the crew. However, if cyber hygiene is maintained continuously during daily operations, it makes audits and inspections easier. Taking the following steps as preparation for an audit can prevent unnecessary stress and disruption, and ensure the audit process runs smoothly.

- Refresh your memory on the latest cyber risk assessment and the cyber risk management plan, generally incorporated within the company's SMS.
- Familiarise yourself with the vessel cybersecurity policies.
- Identify areas where the policies have not been followed, and be prepared to explain why those exceptions were made and the alternative mitigations that were put in place.
- Gather the following documents for potential inspection:
  - Any available cybersecurity certificates, including type approvals and cybersecurity Notations
  - A copy of the cyber risk management plan
  - A copy of the asset and network inventory of all onboard vessel systems
  - Records of completed cyber training, drills and exercises.

About us

UK P&I Club

UK P&I Club is a leading provider of P&I insurance and other services to the international shipping community. The UK P&I Club insures over 250 million tonnes of owned and chartered shipping through its international offices and claims network. 'A-' rated by Standard & Poor's, the UK P&I Club is renowned for its specialist skills and expertise that ensure 'best in class' underwriting, claims handling and loss prevention services. (www.ukpandi.com)

CyberOwl

CyberOwl is the global leader in cybersecurity for the maritime and offshore sectors. We help maritime operators operate cybersecurity monitoring and response, simplify evidence gathering for proving adherence to cyber regulation and manage operational technology risks pragmatically. This is delivered through technology specifically designed for shipping and 24x7 support from our maritime cybersecurity specialists in our bases in the UK, Greece and Singapore.

CYBEROWL
a DNV company

https://cyberowl.io

&In your corner.

UK P&I