IHO ENC and ECDIS cyber security instruction

Contents

Introduction

The benefits of digitalisation rely on interconnected systems which can safely transfer information to deliver operational optimisation, cost savings and safety improvements.

The maritime industry is going through a significant change, driven by the increased availability of satellite communications. Technological developments previously unachievable ten years ago are rapidly becoming possible. With increased digital interconnectivity comes the increased risk of cyber-attack, and vessels—once considered safe at sea—can no longer assume they will not be a target of cybercriminals.

The goal of the IMO maritime cyber risk management is to support safe and secure shipping operationally resilient to cyber risks.

MSC.428(98) states from 1 January 2021, all vessels must ensure their Safety Management Systems (SMS) appropriately address cyber risks.

Vessels must continuously update ENC data used in ECDIS with changes promulgated by the Hydrographic Office to remain carriage-compliant as required by SOLAS. This continual process of updating ENCs presents a permanent and persistent vulnerability, which must be managed by shipping companies in their SMS.

This guideline prepared by the IHO seeks to support Shipping companies and Mariners in mitigating their exposure to cyber risk when using ENCs in ECDIS.

The key to limiting risk is confirming the data going into the ECDIS comes from a trusted source. It is possible to reduce risk by ensuring the ENC service purchased for the vessel comes from a reputable ENC service provider, who will transfer the data in an encrypted form.

Most commercial ENC services use the IHO data protection scheme S-63 to protect the data. S-63 provides a method for ensuring vessels can authenticate data received in the ECDIS against a known and trusted list of providers. All ECDIS are tested during type approval to ensure they can load and decrypt S-63.

While all ECDIS can load and display ENC data in its native S-57 format, it offers no cyber security protection and is not advised. Several ENC service providers convert the data on shore to the proprietary data format of the ECDIS.

These are called SENC services and are specified to be protected by a security that provides equivalent or greater protections than IHO S-63.

Glossary of terms

ENC – Electronic Navigational Chart.
ECDIS – Electronic Chart Display & Information System.
SENC – System Electronic Navigational Chart
OEM – Original Equipment Manufacturer
S-63 – IHO Data Protection (encryption) Scheme for ENC against unauthorised amendment or illegal copying.

References

1. *MSC.428(98), 16 June 2017, Maritime Cyber Risk Management in Safety Management System (SMS)*
2. *MSC-FAL.1/Circ.3, 5 July 2017, Guidelines on Maritime Cyber Risk Management*
3. *Bimco, The Guidelines on Cyber Security Onboard Ships, version 4*
4. *IEC 61162-450*
5. *IEC 61162-460*

Guideline objectives

The document uses the established IMO Cyber Risk Management categories; identify, protect, detect, respond and recover.

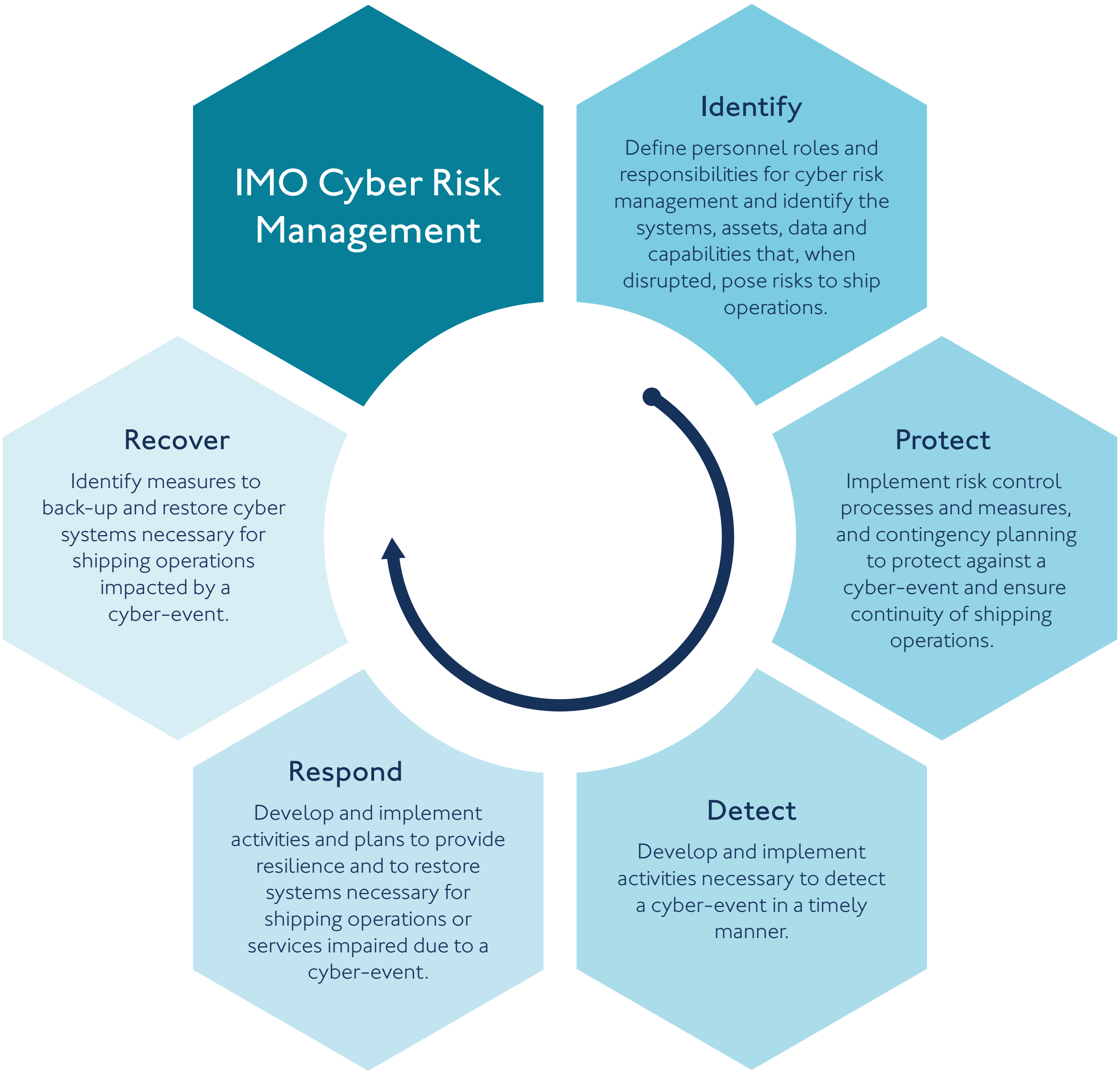

IMO Cyber Risk Management
Identify
Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.
Protect
Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
Detect
Develop and implement activities necessary to detect a cyber-event in a timely manner.
Respond
Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.
Recover
Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

Figure 1.

Scope of applicability

The two principal data transfer methods used to load ENC data and cell permits into ECDIS are covered by this guideline:

1. Removable media
2. Bridge networks

(Navigation and radio communication systems, covered by the following standards IEC 61162-460 or IEC 63154 can be used)

Transferring ENC data and cell permits via removable media

Cyber Risk Management categories	Issues/considerations
1. Identify	› ECDIS › USB/DVD › Communication PC/back-of-bridge › Lack of cyber security training and awareness › Vessel’s network › Potential threat actors › Transfer of data and permits to ECDIS via USB / DVD › Lack of Network boundaries and segmentation › ECDIS operating system › Outdated or lack of antivirus on ECDIS › Inadequate access controls
2. Protect	› Create a risk assessment matrix and quantify potential impacts based on the severity and likelihood of each cyber-attack scenario
3. Detect	› Use approved ENC distributors that secure data transfer in S-63 or an equivalent security scheme › Scan physical media or USB with antivirus for malware or ransomware after each use › Add access controls to the individual systems
4. Respond	› Develop a response plan covering relevant contingencies
5. Recover	› Preparation › Detection and analysis › Containment and eradication › Post-incident recovery

Figure 2.

Identifying threats via removable media

The first stage of becoming more cyber secure is identifying the potential threat vectors for malicious code to infiltrate the vessel's networks, systems or data sources. The internal and external threats to the vessel's ECDIS need careful examination, with interdependencies on different systems and their data flows. Vessels must consider the resources involved in the management of the ECDIS, the operation/governance documents and the crew's roles and responsibilities.

USB/DVD

An ECDIS's ability to accept USB and DVD media presents a severe threat vector for threat actors to install malicious software onto the system. USBs and DVDs can auto-launch and transfer spyware and ransomware content onto the ECDIS. The threat level can heighten if the physical media's source is unknown or the vessel has not enforced strict protocol and physical barriers to the upload media.

ECDIS

The ECDIS and its underlying operating system could be a potential threat. Within the market today, many ECDIS still run on Windows XP or older operating systems, which have greater-known vulnerabilities and are more open to malicious attacks. ECDIS with newer operating systems can have regular updates, patches and service packs applied to mitigate the latest known security threats.

Communication/back-of-bridge system

Vessels commonly use a back-of-bridge system connected to an external network to receive navigational data updates and route planning. The back-of-bridge system can be a primary target for malicious actors to use as a front door for ingesting viruses for onward transit onto an ECDIS via physical media.

Vessel network

ECDIS can update via a ship's external network and physical media. Whilst threats regarding the human handling of media are not applicable, other potential threats emerge. Networks not secured via gateways, firewalls and encryption are an ideal target. If a vessel's network is breached it can have catastrophic effects on other vessel systems connected to the same network. Attackers can flood the network with excessive data traffic to degrade the service in a denial-of-service attack if the vessel does not implement monitoring and threat detection.

Potential threat actors

A vessel relies on external data and services to ensure safe navigation on the latest up-to-date data. It is also crucial to ensure crew members follow strict protocol and have no potential motives to sabotage the vessel's safety. Spear phishing emails, fake websites, redirects and cross-site scripting pose a significant security threat to the secure transfer of legitimate data onto a vessel's network or back-of-bridge before it is loaded onto an ECDIS.

Lack of cyber security training and awareness

The vessel's crew and cyber security awareness must be assessed and continuously managed. As new physical and technical attack vectors emerge and evolve, cyber security awareness will decline, and the potential cyber security risk will heighten. If there is a lack of vessel protocol, training and documentation, responding to a cyber-attack will likely take longer with catastrophic effects.

Identifying vulnerabilities

Inventory of CBSs (Computer Based Systems) and networks

Every vessel should create an inventory mapping the networks, the data flows, and the hardware and software used onboard the vessel. This inventory should be a living document. The vessel must continuously update it following any modifications to applications, operating systems and firmware.

Having an up-to-date holistic overview of the vessel's data ecosystem allows for easy analysis of the potential threats and helps highlight areas that need strengthening or risk being an easy target for attackers. Good inventories should list IP addresses, port numbers and all the necessary information that could be drawn upon to halt an attack or used in recovering from one.

When creating an inventory, the vessel must consult stakeholders from the shipping company, ship designer, System Integrator and Classification Society to help build a detailed system map.

Inventories pose a potential security threat should they get into the wrong hands. They must be physically and digitally secured and only accessed by necessary personnel.

Transferring data and permits to ECDIS via USB/DVD

For up-to-date navigation, mariners are required to load permit files and exchange sets into their ECDIS on a frequent basis. Whilst most of the exchange set information is encrypted and contains digital signature files, unsigned ancillary files still present a significant threat, which could be modified or replaced with malicious code. Furthermore, there is an IMO/IHO requirement for ECDIS to be able to load unencrypted data that presents another threat vector for threat actors to load malicious software onto the ECDIS system. With an increase in the further dissemination of open-source data which can be loaded into an ECDIS, it should be highlighted that this can pose a significant security risk as it can still interfere with the official encrypted data.

Vessels still use CDs and DVDs to update their ECDIS with the latest weekly data. Distributors and shipping companies often write these before sending them via a courier. Threat actors can transfer malicious data onto the disk or switch the disk during transit.

Whatever the update method, if removable media devices are used, they should be checked for malware using up-to-date antivirus software and validated by digital signatures and watermarks before connecting to the system.

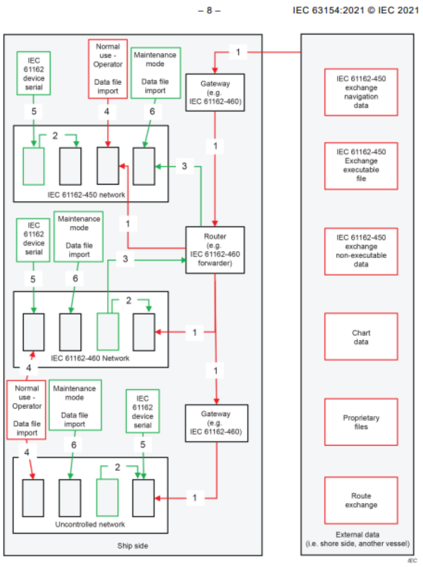

– 8 –
IEC 63154:2021 © IEC 2021
IEC 61162 device serial
Normal use - Operator Data file import
Maintenance mode Data file import
Gateway (e.g. IEC 61162-460)
1
5
4
6
2
3
IEC 61162-450 network
IEC 61162 device serial
Maintenance mode Data file import
Router (e.g. IEC 61162-460 forwarder)
IEC 61162-460 Network
Normal use - Operator Data file import
Maintenance mode Data file import
IEC 61162 device serial
Gateway (e.g. IEC 61162-460)
Uncontrolled network
Ship side
IEC 61162-450 exchange navigation data
IEC 61162-450 Exchange executable file
IEC 61162-450 exchange non-executable data
Chart data
Proprietary files
Route exchange
External data (i.e. shore side, another vessel)
IEC

Figure 3.

ECDIS operating system

Many ECDIS are running on Windows XP or other legacy systems with well-known security and vulnerability issues. Vessels should ensure their ECDIS have patches installed regularly in a maintenance mode to address security vulnerabilities and other bugs or improve operating systems or applications. Vessels should ensure they back up files and systems to recover them if attacked or if they experience database corruption.

The vessel's ECDIS user policy should adopt a principle of Least Functionality, which provides only essential capabilities and prohibits/restricts the use of non-essential functions, ports, protocols and services that are disabled or otherwise prohibited. The ECDIS should be used for primary navigational use only, and all other data validation and preparation should be carried out on a secure back-of-bridge system/network.

Outdated or lack of antivirus on ECDIS

ECDIS and back-of-bridge systems should be protected against malicious code such as viruses, worms, trojan horses, spyware, etc. A virus can easily evade and hide within the ECDIS whilst self-replicating, spreading and acting maliciously, performing actions that affect the system's navigational performance.

Antivirus, antimalware and antispam software will create a shield to block known threat vectors into the system and remove any viruses already detected within the system hardware.

Common means for virus infiltration into or via a back-of-bridge setup are electronic mail, electronic mail attachments, websites, removable media, PDF documents, web services, network connections and already infected networks.

If ECDIS cannot run or have installed antivirus and antimalware software, a vessel must implement malware protection through operational procedures, physical safeguards, or according to the manufacturer's recommendations.

Inadequate access controls

The ECDIS, back-of-bridge system and network on the vessel should provide physical and digital measures to limit the ability to interact with the system itself. Access controls and user groups should be implemented to restrict access to system resources or gain knowledge of essential control system components and functions.

Access to the vessel's onboard networks and access points should only be allowed to authorised personnel, under supervision or according to documented procedures, e.g., for maintenance. Other networks should be used for non-navigational requirements such as printing documents or accessing external uncontrolled networks like the internet.

Transferring ENC data and cell permits via a network

Cyber Risk Management categories	Issues/considerations
Identify	› Lack of cyber security training and awareness › Vessel's network › Potential threat actors › Lack of network boundaries and segmentation. › ECDIS operating system. › Outdated or lack of antivirus on ECDIS › Inadequate access control › Unverified applications running on other back-of-bridge or systems connected to the network
Protect	› Use an authorised ENC distributor where data contains certificates. › Ensure antivirus is up to date on back-of-bridge or systems connected to the ECDIS network › Use a 460 Network Gateway › Pre-validation of data within the distributor's system › Develop an incident response plan, checklists and drills for a possible attack, including a backup arrangement of ECDIS
Detect (one in isolation may not indicate a cyber-attack)	› Check the sender's URL and network addresses/ whitelist › Monitor ECDIS behaviour for abnormalities › Monitor system performance and speed › Regularly check alerts and notifications from antivirus › Question if your system likely to be infected based on network connectivity and the amount of use › Add access controls to individual systems
Respond	› Ensure you have informed the vessel master of a possible cyber issue as soon as it occurs › Log the incident as soon as possible › Ensure the safety of the crew and vessel › Enact a contingency plan covering relevant contingencies, and ensure the vessel strictly follows a response plan for cyber-attack › If possible, add an extra watch on the vessel while the vessel undergoes a response plan › Check redundancy systems – backup ECDIS, back-of-bridge, paper chart etc › Collect evidence of the attack (screenshots or videos) to aid response plans and better respond to future incidents › Contact the shipping company to inform them of onward communication with coastguards and discuss what assistance they can provide

	› Inform shipping companies and distributors, describing symptoms, severity, operations on the bridge and operational contexts › Inform coastal authorities VTS etc so nearby they can alert nearby traffic to the dangers › As a last resort, disconnect network cables and Wi-Fi › Communications of demand – In a ransomware scenario, listen to demands and stall before deciding how to proceed › Ensure communication with the entire crew
Recover	› Safety first: navigate to a port where a professional can access the system › If required, allow a professional to complete an uninstall/reinstall of ECDIS software › Communicate with the system integrator responsible for the installation regarding the security vulnerability › Ensure a professional returns the ECDIS to a safe state and not the vessel's normal state › Containment and eradication – Analyse causes and ensure a professional removes any threats from the ECDIS and network components › Evaluate what went well and requires improvement › Ensure you record the incident and the experience in case of future incidents

Figure 4.

Identifying threats to your network

Lack of network boundaries and segmentation

Networks that connect to the ECDIS need to be managed and have security zones established by your system integrator and shipping company to ensure viruses and malicious data packets do not penetrate the ECDIS or other vessel systems.

Well-defined security policies and capabilities need to be established to only allow explicit traffic across the different zones of the network to the ECDIS. Ensure your system integrator has installed 460-Gateways, Firewalls, Routers and isolated (air-gaped) networks to manage the vessel's connection with an external network.

Using Intrusion Prevention Systems (IPS) - Network traffic can be monitored. Using 460-Gateways, Forwarders and DMZs (demilitarized zones) it is more difficult for an attacker to perpetrate an attack throughout the entire network and reach the ECDIS. Segmentation can help reduce the potential attack surface, prevent attackers from achieving lateral movement through systems and improve network performance.

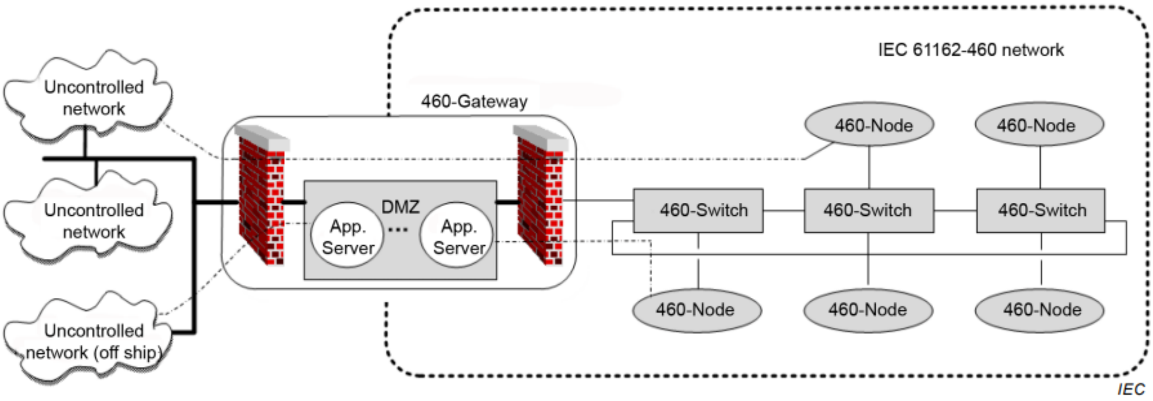


Figure 5.

Use of unverified applications running on other back-of-bridge systems connected to the network

The vessel should ensure the use of third parties or applications not documented or on the CBS inventory is prohibited where possible. The crew's personal devices must connect to a separate network of the vessels to reduce the risk of an attack on the critical underlying network of the vessel. Attackers may attempt to access onboard systems through the weakest vulnerability loopholes, which is often a third-party application with known security vulnerabilities.

Protect

Use an authorised ENC distributor where data contains certificates

When receiving data via a network, it is important to use a data provider who adds signatures to their data. Data with a signature prevents a malicious actor from modifying an original file via its transfer into the vessel's ECDIS. If the ECDIS can not validate the signature file, it will prevent it from being loaded into the ECDIS, significantly reducing the chance of a malicious attack on your systems. Some data producers make their ENCs available unencrypted. However, it may be prudent to source these ENCs via a data server where signatures are provided alongside the data.

Using an ENC distributor to provide ENCs over a network can also reduce the cyber security risk due to their ability to pre-validate the data sent. Distributor systems can scan content for malicious files or suspicious content that could present a risk to your networked ECDIS. Having a distributor in the data transfer flowline to the ECDIS adds another layer of resilience and provides a point of contact for any questions or concerns with the data sent.

Develop a contingency plan

Develop an incident response plan should a cyber attack on the vessel's network or ECDIS occur. This response plan should contain checklists of practical actions the crew can take to detect, respond and limit the consequences of cyber incidents. The plan can help inform the crew of how to implement breakpoints of compromised equipment, prioritise response options, detect signs of what to look for when being attacked and how to operate during an attack without using infected networks or hardware.

Detect

Check URL and network addresses of data sender/whitelist

If your ECDIS connects via a network, ensure you whitelist the connection URL so your ECDIS trusts only that network path. Where possible, the network should be configured so that only trusted data sources can access the network. Ensure network addresses are constantly reviewed and validated with your data provider should a new or modification to an existing network address be required.

Monitor ECDIS behaviour for abnormalities

You can look for several symptoms to help detect an attack on a networked ECDIS; these include:

- Any screen flickering abnormalities or unresponsive user interfaces
- Unexplained system reboots
- Unstable PC temperature
- Abnormal system noise from fans and hard drives
- Inconsistent ECDIS timing with the GPS; an attacker could spoof your position using GPS timing or be sending the ECDIS incorrect packets of positional data from your GPS
- Abnormal system performance
- Abnormal system speed: if you experience a noticeable degradation in speed and system performance, you could be under a cyber-attack; your ECDIS may be running malicious software in the background

If you notice one or more of these symptoms above, you should stop what you are doing, notify the master/crew of the vessel take caution and ascertain if you are under attack before deciding to continue operation.

Check alerts and notifications from antivirus regularly

Ensure your system integrator or shipping company keeps your antivirus software up to date. If the vessel's approved ECDIS cannot run an antivirus, ensure the back-of-bridge system or any other systems connected to the same network as the ECDIS utilise it.

Vessels should run antivirus checks on the network frequently; this improves your chances of detecting and removing malicious files before they spread and take effect.

Check network connectivity and the amount of use

Ensure your system integrator or shipping company keeps your antivirus software up to date. If the vessel type approved ECDIS cannot run an antivirus, then ensure the back-of-bridge system or any other systems connected to the same network as the ECDIS.

Antivirus checks should be run frequently on the ship's network, to a schedule and reviewed to heighten the chances of detecting and removing malicious files before they spread and take effect.

How likely is your system to be infected based on network connectivity and amount of use?

When detecting a network-based cyber-attack, it is prudent to constantly evaluate the network's use and how much data the ECDIS has ingested. If frequent transfer of multiple files has occurred, there is a heightened risk of a cyber-attack. After heavy network use for a prolonged period, it would be wise to run a virus check or seek a professional system check by a system integrator or technician to run a health check on your system.

Respond

When responding to a cyber-attack ensure the master of the vessel and all crew members are informed, and the incident is logged in the vessel's SMS. Enact the contingency plan and ensure all crew members are safe from immediate threats. Where the vessel's ECDIS could be compromised and mislead the navigator, you could add an extra watch to ensure the vessel stays clear of potential dangers and other traffic.

When it is safe to do so, and where possible, use the redundant navigation system such as a secondary ECDIS or paper chart to base navigational decisions on. Whilst under a cyber-attack try to obtain evidence of the observed behaviours and abnormality via system screenshots or via phones.

It may be prudent to have a different update regime for the redundant navigation system and not synchronise the same data across multiple navigational units simultaneously. This practice will help mitigate a compromised main ECDIS from affecting other redundant backup systems and will become particularly relevant as mariners move to event-driven updates via satellite communications.

Whilst under attack, contact the coastal authority for the area, your shipping company and the distributor of the vessel's data. By informing all parties, the coastal authority can forewarn vessels in the area via radio warnings and may be able to aid and protect the vessel and ensure it stays safe. Whilst trying to resolve the threat, record all operations carried out and any observations documented. If all attempts to overcome the attack on the network have failed, then it might be applicable to disconnect all systems from the compromised network. Throughout the attack, ensure all vessel crew are informed of developments and decisions made.

Recover

When it is safe to do so, and you are confident your network has been attacked, you must safely navigate to the port for your systems to be cleaned of the cyber threat/virus.

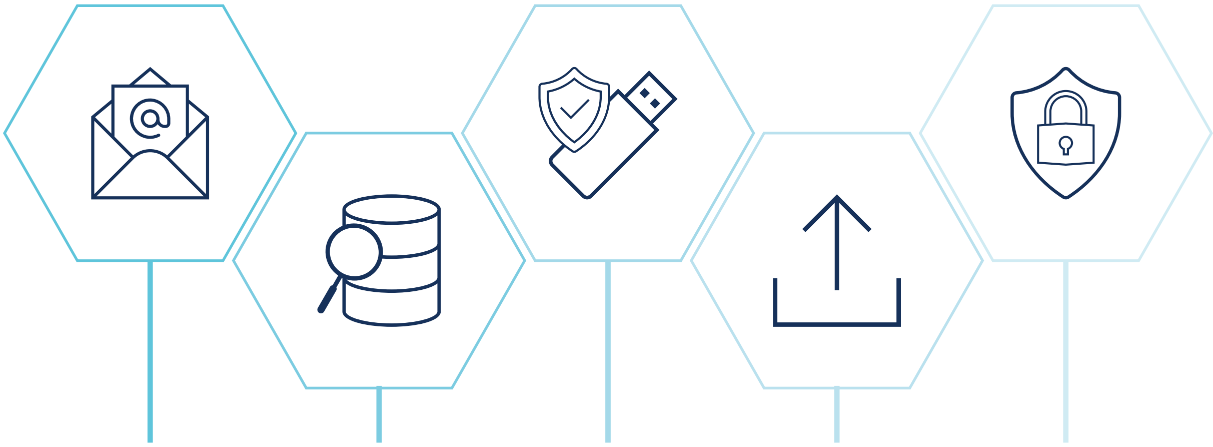
When travelling to the nearest port, you must enact your contingency plan and use backup ECDIS or hardware you know has not been compromised. Once in port, the vessel must contact the ECDIS OEM, the system integrator and vessel technicians to analyse the network and connected systems to remove the malicious files and address the underlying vulnerability.

Where applicable, it might be required to completely uninstall operating software and applications connected to the network to ensure no vulnerabilities or attack vectors remain.

Whilst the systems and ECDIS are restored, the OEM or system integrator should return it to its original state. Where vulnerabilities or threats are discovered by poor vessel practice, you must share these with the crew and address them before onward navigation.

Once the incident is resolved, evaluate what went well and where you can improve the contingency plans. Ensure you record the incident in the vessel's SMS and document all experiences for future incidents.

Email policy



Email arrives

- Whitelist
- Follow policy
- Verify sender
- Scan email

Visit source data

- Blacklist
- Whitelist
- Verify URL
- Secure certificates

Download to USB

- Scan USB devices
- Scan upload
- Use a dedicated USB

Install on ECDIS

- Use a secure/ verified USB
- Follow policy
- Use secure ports
- Scan software
- Use antimalware
- Asset management
- Lock OS

Prevention

- IDS/IDP
- Use A I-based firewalls
- Follow incident response policy
- Prepare, drill and train

Checklist for the creation of a response plan for an ECDIS using USB or removable media

Action	Assignee			Signed	Approved	Date last issued
	System Integrator	Ship Company	Vessel			
Use an approved ENC chart distributor that uses either the IHO data protection scheme S-63 or a type-approved SENC delivery method to secure the data						
Ensure the crew have adequate access to cyber security training						
Change onboard default equipment and software passwords monthly or if compromised						
Install virus-checking software onboard						
Ensure virus-checking software remains up-to-date with the latest software releases						
Be vigilant of spam emails and attached files						
Scan removable USB devices before transferring digital files from a communication PC to the ECDIS						
Only use the dedicated USB device to download and transfer ENC data and permits to ECDIS						
Clearly label the USB device to mark it as dedicated to transferring ENC data and permits						
Do not use the dedicated USB device for anything else than data download/import to ECDIS						
Do not store digital files on this device						
Do not leave the dedicated USB device unattended						
Reformat the dedicated USB device after use						
Before transferring data to the ECDIS via USB pun permits and ENC data through antivirus and antimalware tools						
Do no not allow crew's personal devices to be connected to ECDIS						

Keep ECDIS updated to latest IHO standards						
Keep ECDIS updated for the latest software releases as recommended by the ECDIS manufacturer						

Checklist for the creation of a response plan for a networked ECDIS

Action	Assignee			Signed	Approved	Date last issued
	System Integrator	Ship Company	Vessel			
Create an inventory of the hardware, software networks and connections of the vessels systems to expose any vulnerabilities.						
Change network passwords/ authentication credentials onboard every month or if compromised						
Ensure your Shipping Company or system integrator installs firewalls and virus checking software onboard across the networks						
Ensure your Shipping Company or System Integrator checks software is kept up to date with the latest software releases						
Ensure your Shipping Company or System Integrator installs networks that are segmented, and air gaped where possible from one another						
Ensure your Shipping Company or system integrator has the vessels ECDIS only connected to external networks via a 460-Gateay or 460 Wireless Gateway and is utilising DMZs in front of your ECDIS network to minimise threat vector						
Ensure your Shipping Company or system integrator has configured your network so all other systems running on the same ECDIS network are connected via 460 switches and forwarders						
Install intrusion prevention systems and monitor network traffic for abnormalities						
Ensure networks and ports are designated for certain essential activity only						
Ensure access to network ports are digitally or physically secured to certain personnel only						
Use a separate isolated network for personal use to external network (internet)						
Regularly backup network paths and configurations in a secure location						

Whitelist allowable network paths to the ECDIS						
Ensure network connections are automatically closed after being idle for an amount of time						
If ECDIS is connected to the communication PC via a firewall, make sure the hardware is running the latest software version from your provider						
Map remote accesses and data flows						