[ENCWG7-4.5]

IHO ENC & ECDIS Cyber Security Guideline

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 period of 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 which once considered themselves safe when at sea can no longer assume that they will not be a target of cyber criminals.

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

MSC.428(98), states from 1st Jan 2021 all vessels must ensure that cyber risks are appropriately addressed in their Safety Management Systems (SMS).

ENC data used in ECDIS must be continually updated 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 limiting their exposure to cyber risk when using ENCs in ECDIS.

Key to limiting risk is ensuring the data that goes into the ECDIS comes from a trusted source. It is possible to reduce risk by ensuring the ENC service that is purchased for the vessel come from a reputable ENC service provider, who will transfer the data to the vessel 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 the data received in the ECDIS can be authenticated 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 are capable of loading and displaying ENC data in its native S-57 format, this offers no cyber security protection and is not advised.

There are a number of ENC service providers that 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 that IHO S-63.

Glossary of terms

ENC

ECDIS

References

MSC.428(98), 16 June 2017, Maritime Cyber Risk Management in Safety Management System (SMS)

MSC-FAL.1/Circ.3, 5 July 2017, Guidelines on Maritime Cyber Risk Management

Bimco, The Guidelines on Cyber Security Onboard Ships, version 4

IEC 61162-450

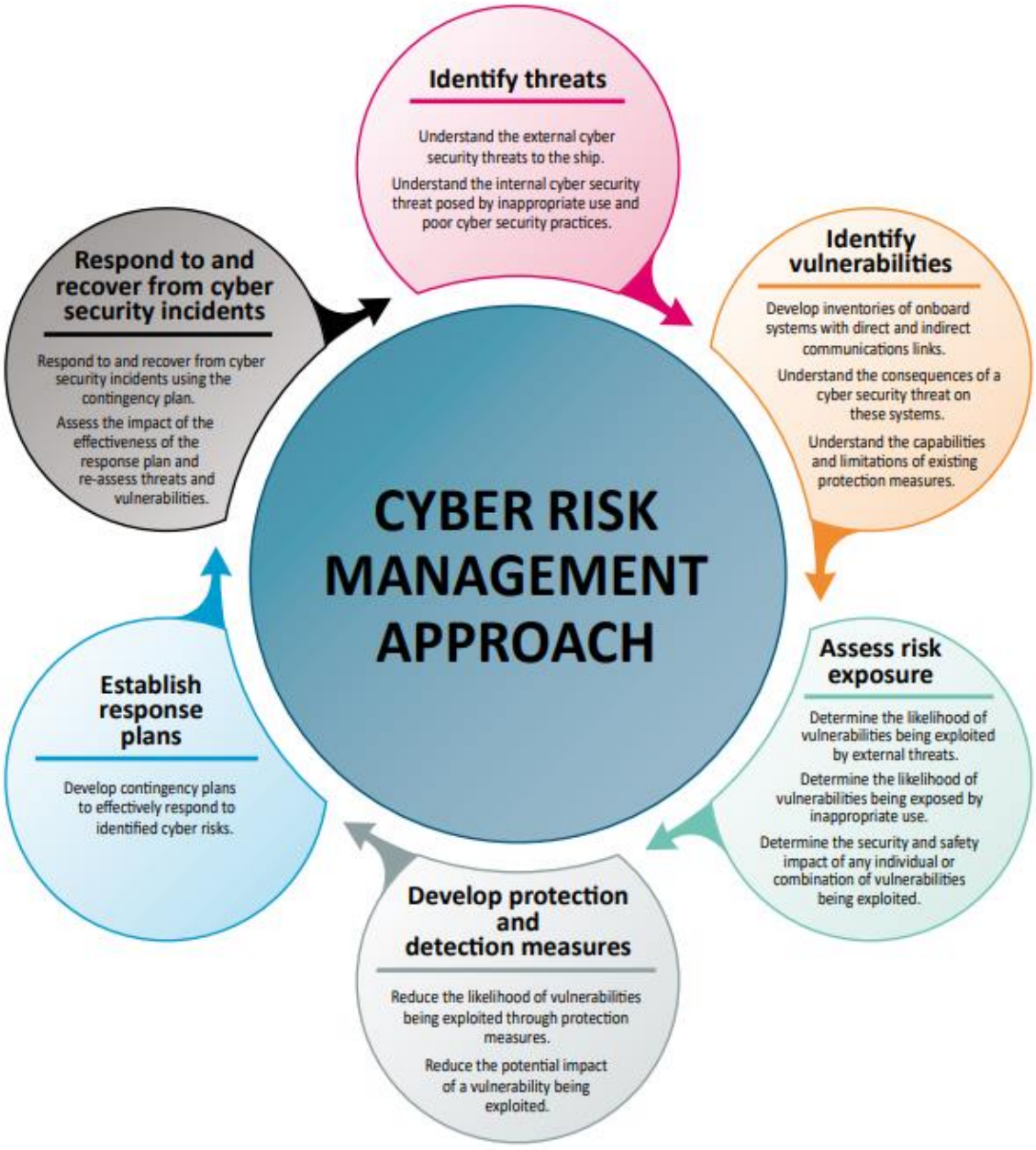
IEC 61162-460

Guideline Objectives
The following table uses the established Cyber Risk Management categories to mitigate the risk associated to managing the loading of ENC data and associated cell permits into ECDIS.

This document focuses on two principal data transfer methods to ECDIS, the first uses removable media the second using a network.

1. Transfer of ENC data and cell permits via removable media or network.

Cyber Risk Management Categories	Issues / Considerations
Identify threats	• ECDIS • USB / DVD • Communication PC / Back of Bridge • Lack of cyber security training and awareness. • Vessel's network • Potential Threat actors
Identify Vulnerabilities	• Transfer of data and permits to ECDIS via USB / DVD. • Network boundaries and segmentation. • ECDIS operating system. • Outdated or lack of Anti-Virus on ECDIS. • Inadequate access controls.
Assess risk Exposure	• Create a risk assessment matrix and quantify potential impacts based on the severity and likelihood of each cyber-attack scenario.
Develop protection and detection measures	• 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 every time it's used. • Add access controls to the individual systems.
Establish response plans	• Develop a response plan covering relevant contingencies.
Respond to and recover from cyber security incidents	• Preparation • Detection and analysis • Containment and eradication • Post incident recovery.


Identify threats
Understand the external cyber security threats to the ship.
Understand the internal cyber security threat posed by inappropriate use and poor cyber security practices.
Identify vulnerabilities
Develop inventories of onboard systems with direct and indirect communications links.
Understand the consequences of a cyber security threat on these systems.
Understand the capabilities and limitations of existing protection measures.
Assess risk exposure
Determine the likelihood of vulnerabilities being exploited by external threats.
Determine the likelihood of vulnerabilities being exposed by inappropriate use.
Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.
Develop protection and detection measures
Reduce the likelihood of vulnerabilities being exploited through protection measures.
Reduce the potential impact of a vulnerability being exploited.
Establish response plans
Develop contingency plans to effectively respond to identified cyber risks.
Respond to and recover from cyber security incidents
Respond to and recover from cyber security incidents using the contingency plan.
Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.
CYBER RISK MANAGEMENT APPROACH

Action	Signed	Approved
Ensure crew have adequate access to cyber security training		
Change default equipment passwords onboard regularly		
Install virus checking software onboard		
Ensure ECDIS has latest IHO certificate loaded		
Ensure virus checking software is kept up to date with the latest software releases		
If removable USB devices are to be used to transfer the digital files from a communication PC to the ECDIS the should be scanned for viruses scan removeable media		
Do no not allow crew's personal devices to be connected to ECDIS		
Use only dedicated removable media (USB stick) to download ENC data and permits		
Add a sticker / label to the item to clearly mark it as dedicated to the transfer of ENC data.		
Do no use this item for anything else than data download / import to ECDIS.		
Do not store digital files on this device.		
Reformat USB after use		
Do not leave removable media unattended.		
After using the USB, store it in safe place where only authorized personnel have access		
Use the USB only one-way (from back-of-bridge communication PC to ECDIS).		
Do not save any ECDIS data on USB		
Be vigilant of spam emails and attached files.		
Run permits and ENC data through Anti-virus and anti-malware tools		
Keep ECDIS updated to latest IHO		

standards		
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.