MARITIME CYBER RISK MANAGEMENT

A QUICK START GUIDE

In June 2017 the International Maritime Organization (IMO) laid out its "Guidelines on Maritime Cyber Risk Management".

Shipowners and managers now have until 1st January 2021 to build cyber risk management into their ship safety initiatives, or risk having their ships detained.

To help you get started, this document provides an overview of the risk areas highlighted by the IMO. We've included some of the top risks to look out for, as well as initial steps you can take to address them.

Hedgehog Security is a cyber security company that has been working in the maritime sector for over 10 years, advising vessels owners as well as port operators on maintaining a high level of cyber security.

With exceptional experience in working with Operational Technology deployed onboard and within ports, as well as the standard Information Technology and IoT devices, Hedgehog Security is well placed to be your principal advisor on Maritime Cyber Security and the associated Risk Management.

MARITIME CYBER RISK MANAGEMENT

The IMO's 8 Areas of Cyber Risk

The IMO has highlighted eight areas of cyber risk for maritime vessels. Depending on the size and function of your vessels, there may be further areas of risk to be addressed.

Note that cyber risks don't only arise from attacks—they also arise from mistakes. The action steps given here are intended to minimize the likelihood of both intentional and accidental compromise of your systems.

IMO Risk Area: Bridge Systems

Cyber risks can arise from:	Initial action steps to reduce risk:
• USB drives being inserted	• Secure all ship consoles with a padlock to avoid unwanted access
• Mobile devices being connected and charged	• Disable browser software from bridge systems
• Internet connections being used to surf the web	• Ensure that no personal devices are connected to the OT network
• Lack of network segregation between IT and OT devices	
• Physical access to devices	

IMO Risk Area: Cargo Handling & Management Systems

Cyber risks can arise from:	Initial action steps to reduce risk:
• USB drives being connected	• Ensure only company issued USB drives are used for data transfer
• Mobile devices being connected and charged	• Ensure company issued USB drivers are only user for business purposes
• Internet connections being used to access the internet	• Secure all shops consoles with a padlock to prevent unwanted access
• Physical access to devices	• Ensure no personal devices are connected to the OT network

IMO Risk Area: Propulsion & Machinery Management & Power Control Systems

Cyber risks can arise from:	Initial action steps to reduce risk:
• Lack of network segregation between IT and OT networks / devices	• Physically separate IT and OT networks
• Lack of security testing for individual components connected to the network and/or the internet	• Get up to date cyber security certificates from suppliers for all internet to network connected devices, or run regular independent cyber security assessments
• Unauthorised devices connecting to the network	• Ensure network sockets are disabled if not in use.

Hedgehog Security Ltd.
12/1 City Mill Lane, Gibraltar, GX11 1AA

Visit our website @ hedgehogsecurity.gi and hedgehogsecurity.co.uk
Call us on +350 200 31337 or +44 3333 444 256

MARITIME CYBER RISK MANAGEMENT

IMO Risk Area: Access Control Systems

Cyber risks can arise from:	Initial action steps to reduce risk:
• Physical access to area where computer systems are located, for example in server closets	• Ensure long passwords are used for all computer systems and user accounts
• Physical access to devices and IT. For example, unlocked server cabinets, routers in open areas etc.	• Adopt a “least privilege” access policy. Users should only have the access they need for daily duties.
• Keeping passwords written down	• Enforce personal access restrictions for any area containing computer systems
• Not changing default passwords for one or more computer system	

IMO Risk Area: Passenger Servicing & Management Systems

Cyber risks can arise from:	Initial action steps to reduce risk:
• Lack of network segregation between IT and OT networks / devices	• Ensure long passwords are used for all computer systems and users
• Software of any type not being security tested	• Ensure no personal devices are connected to the OT network or the IT network
• Personal internet browsing	• Disable browser software

IMO Risk Area: Passenger Facing Public Networks

Cyber risks can arise from:	Initial action steps to reduce risk:
• Lack of network segregation between IT and OT networks / devices	• Ensure firewall software is up to date
• Not updating network devices with the latest security patches	• Ensure firewalls are properly configured
• Insecure configuration of network devices and software	• Prevent data crossing between networks
• Information leakage from networked systems and devices	• Ensure long passwords are used for all computer systems and users
	• Physically separate OT and IT networks
	• Certification against the IASME Maritime Cyber Baseline Standard

IMO Risk Area: Administrative & Crew Welfare Systems

Cyber risks can arise from:	Initial action steps to reduce risk:
• Lack of network segregation between systems and OT networks and devices	• Establish a policy for internet browsing
• Software of any type not being security tested	• Monitor internet activity for irregular activity
• Poor or non-existent access control protocols	• Ensure firewall software is up to date
• Lack of form Bring your own Device policies	• Ensure firewalls are properly configured
• Insecure configuration of network devices and software	• Certification against the IASME Maritime Cyber Baseline Standard

Hedgehog Security Ltd.
12/1 City Mill Lane, Gibraltar, GX11 1AA

Visit our website @ hedgehogsecurity.gi and hedgehogsecurity.co.uk
Call us on +350 200 31337 or +44 3333 444 256

MARITIME CYBER RISK MANAGEMENT

IMO Risk Area: Communication Systems

Cyber risks can arise from:	Initial action steps to reduce risk:
Not changing default access credentials	Ensure long passwords are used
Having a publicly facing IP address	Ensure antenna tuning users are not directly internet connected
Insufficient or incorrect configuration of firewalls	Ensure firewall software is up to date
Lack of network segregation between IT and OT networks / devices	Ensure firewalls are properly configured
	Use separate public IP addresses for IT and OT networks
	Certification against the IASME Maritime Cyber Baseline Standard

Next Steps

Over the last decade, ships and other maritime vessels have become highly connected and dependent on computer systems. Right now, the computer systems on many vessels are vulnerable to compromise, which has already led to several highly expensive cyber incidents.

The action steps given here are intended as a quick start guide to help you prepare for the new IMO regulations. Depending on the complexity of your vessels, more steps may be needed to adequately protect against cyber-attacks.

For no-nonsense advice and support to get your vessels cyber-ready, contact Hedgehog Security today and talk to our Maritime Cyber Security team.

Hedgehog Security Ltd.
12/1 City Mill Lane, Gibraltar, GX11 1AA

Visit our website @ hedgehogsecurity.gi and hedgehogsecurity.co.uk
Call us on +350 200 31337 or +44 3333 444 256