NEPTUNE
MARINE CYBER SECURITY

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.

Who Are We?

Neptune is a cyber security company that works exclusively in the marine sector. Our team combines experts in shipbuilding, maintenance and operations and cyber security testing and design.

To find out how we're helping shipowners and managers control cyber risk, visit our website.

NEPTUNE
MARINE CYBER SECURITY

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.

1

IMO Risk Area: Bridge Systems

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

2

IMO Risk Area: Cargo Handling and Management Systems

Cyber risks can arise from:	Initial action steps to reduce risk:
• USB drives being inserted • Mobile devices being connected and charged • Internet connections being used to surf the web • Access to the rest of the ship's network • Lack of network segregation between IT and OT • Physical access to devices	• Ensure only company-issued USB drives are used for data transfer • Ensure company-issued USD drives are ONLY used for business purposes • Secure all ship consoles with a padlock to prevent unwanted access • Ensure no personal devices are connected to the OT network

3

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

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

NEPTUNE
MARINE CYBER SECURITY

4

IMO Risk Area: Access Control Systems

Cyber risks can arise from:	Initial action steps to reduce risk:
• Physical access to areas where computer systems are located (e.g., server rooms) • Physical access to devices and IT (e.g., unlocked server cabinets, routers left in open areas, etc.) • Keeping passwords on Post It notes • Not changing default passwords for one or more computer systems	• Ensure strong passwords are used for all computer systems and users • Adopt a “least privilege” access policy – users should only have the access they need for daily duties • Enforce personnel access restrictions for any area containing computer systems

5

IMO Risk Area: Passenger Servicing and Management Systems

Cyber risks can arise from:	Initial action steps to reduce risk:
• Lack of network segregation between IT and OT • Software of any type not being security tested • Personal internet browsing	• Ensure strong passwords are used for all computer systems and users • Ensure no personal devices are connected to the OT network • Disable browser software (e.g., Internet Explorer, Firefox, Chrome)

6

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 • Not updating network devices with the latest security patches • Insecure configuration of network devices and software • Information “leakage” from network systems and/or devices	• Ensure firewall software is up to date • Ensure firewalls are properly configured • Prevent data from crossing between networks and VLANs • Ensure strong passwords are used for wireless access points • Physically separate OT and IT networks

NEPTUNE
MARINE CYBER SECURITY

7

IMO Risk Area: Administrative and Crew Welfare Systems

Cyber risks can arise from:	Initial action steps to reduce risk:
• Lack of network segregation between these systems and OT • Software of any type not being security tested • Poor or nonexistent access management protocols • Lack of formal BYOD ("Bring Your Own Device") policies • Insecure configuration of network devices and software	• Establish a policy for Internet browsing • Monitor internet traffic for irregular activity • Ensure firewall software is up to date • Ensure firewalls are properly configured

8

IMO Risk Area: Communication Systems

Cyber risks can arise from:	Initial action steps to reduce risk:
• Not changing default access credentials • Having a publicly facing IP address • Insufficient or incorrect configuration of firewalls • Lack of network segregation between these systems and IT/OT	• Ensure strong passwords are used • Ensure antenna tuning units are not directly Internet-facing • Ensure firewall software is up to date • Ensure firewalls are properly configured • Use separate public IP addresses for IT and OT networks

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 a number of 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 Neptune today.

 | contact@neptunecyber.com | +1 514 476 6722