

# Cyber risk management on board ships

Aron Sorensen, Head of Maritime Technology and Regulation

www.BIMCO.org



# What is cyber risk management?

• Cyber risk management means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level; taking into consideration the costs and benefits of actions taken by stakeholders.



# Different risk exposures









# onboard personnel

#### **Identify threats**

Understand the external cyber security threats to the ship.

Understand the internal cyber security threat posed by inappropriate use and lack of awareness.

Cyber

security

approach

**Develop protection** 

and detection measures

Reduce the likelihood of vulnerabilities being exploited through protection measures. Reduce the potential impact of a vulnerability being exploited.

# Respond to and recover from cyber security incidents

Respond to and recover from cyber security incidents that are realised using the response plan.

Assess the impact of the effectiveness of the response plan and reassess threats and vulnerabilities.

# Establish contingency plans

Develop a response plan to reduce the impact of threats that are realised on the safety and security of the ship.

#### 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 protecion 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.

#### risk ure





# Visitors and plug in devices

Technicians
Pilots

Port officials

Terminal representatives

Agents

Vendors





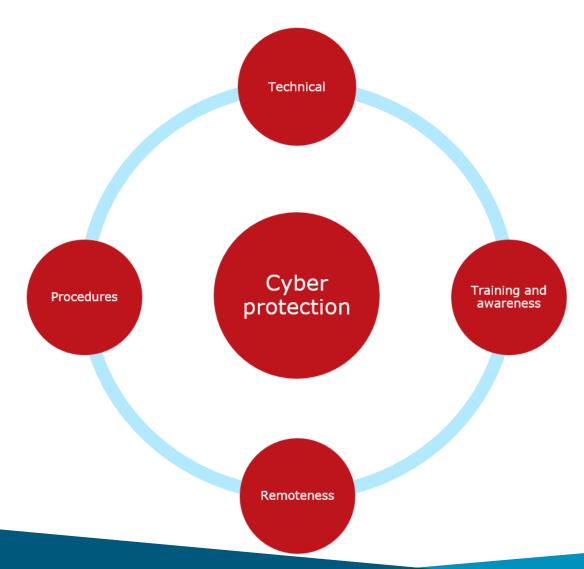
Shipowners, ports, and agents are being hit by cyber incidents every day

Too stringent mitigation of cyber risks can obstruct your normal ways of doing business

In a business
environment you
cannot protect
yourself a 100 per cent
from cyber risks

# Ways to protect

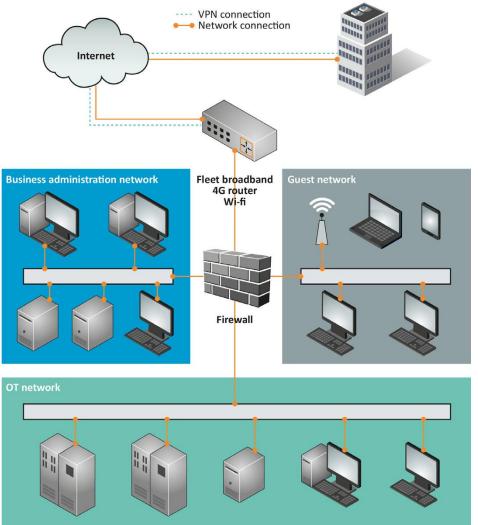




## **Technical**

- Cyber resilient <u>Hardware</u>
  - Ships needs to be built to cyber standards eg. Networks, PLCs (IACS cyber panel)
- Software with cyber thinking





# **Training and awareness**

- Easy guidance on low hanging fruits
- KVH Videotel security training programme produced in association BIMCO
- Consideration to include in a BIMCO standard contracts



## **IMO** decision



- The ISM Code is the natural regulatory framework for cyber risk assessments
  - it already include assessment of identified risks to ships, personnel and the environment
- Existing contingency plans may be used
  - Even if the ship is cyber compromised
- Ensure that cyber risks are appropriately addressed in Safety Management Systems
  - No later than the first annual verification of the Document of Compliance after 1 January 2021 (audit and PSC from 2022)







- The <u>SMS</u> is an open system and should contain information on how cyber risk management is implemented
- Concentrate on contingency and how to respond to a cyber incident

- The <u>SSP</u> may include specific sensitive information regarding IT and OT systems
- Recovery plans and arrangements for data backup should be kept here for confidentiality

### **Conclusions**



- Continue to build awareness industry to learn from incidents
- Implementation of the industry cyber guidelines
- Commercial cyber security considerations BIMCO contracts
- Ships should be built with cyber secure networks/components, and use contemporary software (IACS cyber panel)
- Equipment and systems should be maintained in a cyber secure way
- Implementation in the SMS and ISPS

