Cyber risk management on board ships

Aron Sorensen, Head of Maritime Technology and Regulation

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.

BIMCO

Guidelines widely accepted by shipowners, classification societies, and IMO

Operational technology (OT) includes devices, sensors, software and associated networking that monitor and control onboard systems.

Cyber attack has the potential to stop the operation of the ship

Different risk exposures

From senior management to onboard personnel

Ship shore interface

Visitors and plug in devices		
Technicians Pilots	Port officials Terminal representatives	Agents Vendors

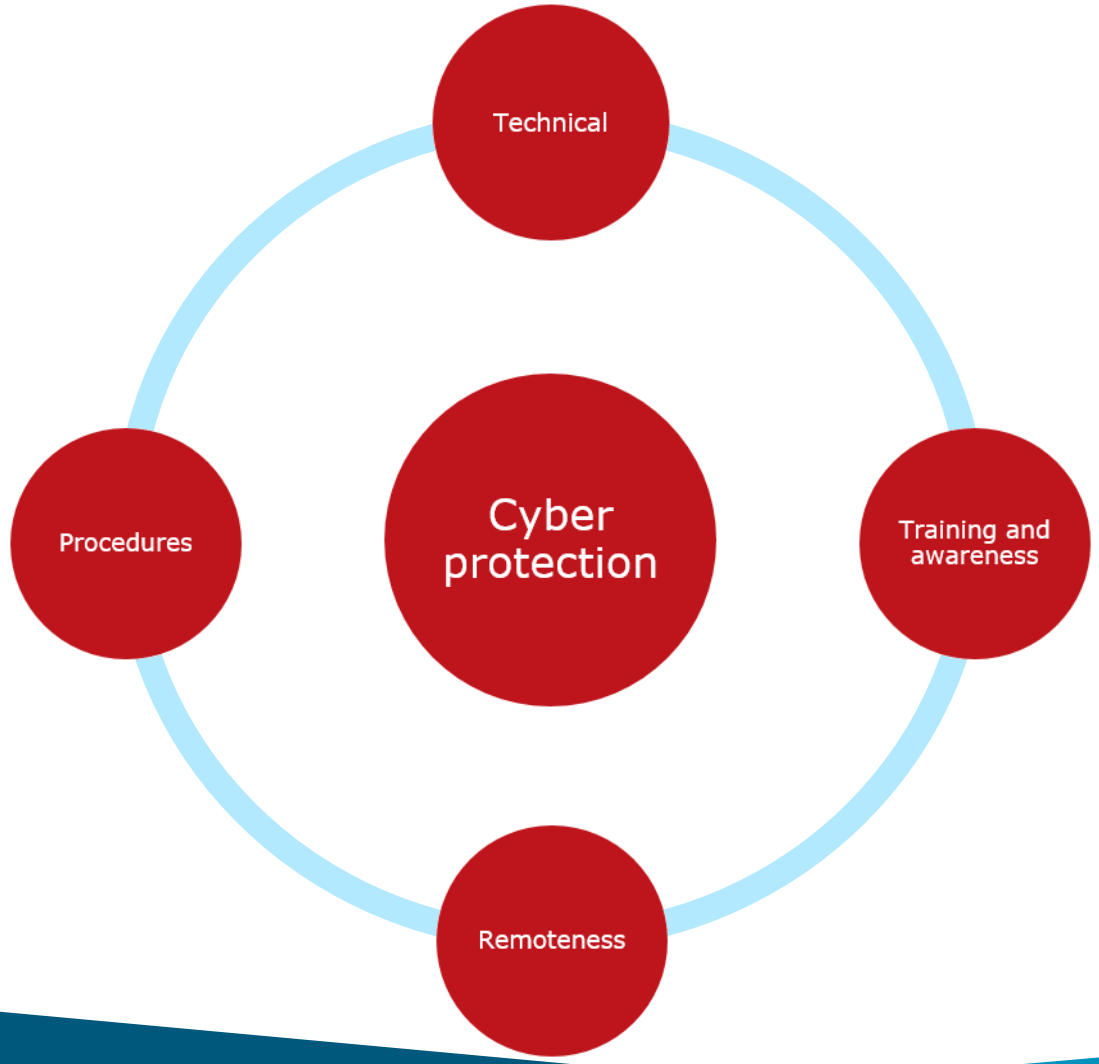
Balancing cyber risk

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

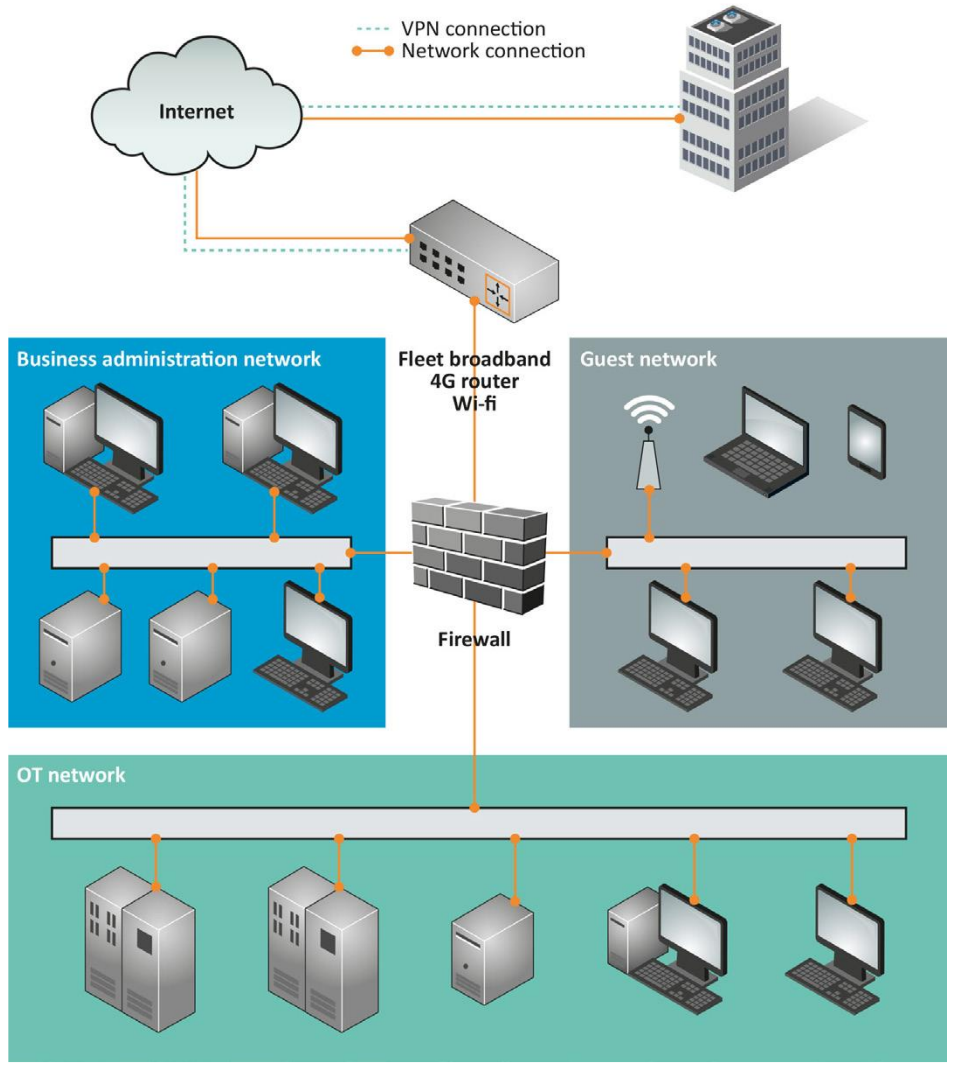
Ways to protect



Technical

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

- <u>Software</u> 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)

Implementation of IMO's descision

- The SMS 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 SSP may include specific sensitive information regarding IT and OT systems
- Recovery plans and arrangements for data back-up 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

Thank you!

Contact BIMCO at

www.bimco.org