BIMCO

e-Navigation underway 2016

The Coordinated approach

Upsides versus Downsides -
Covering the cyber security risk

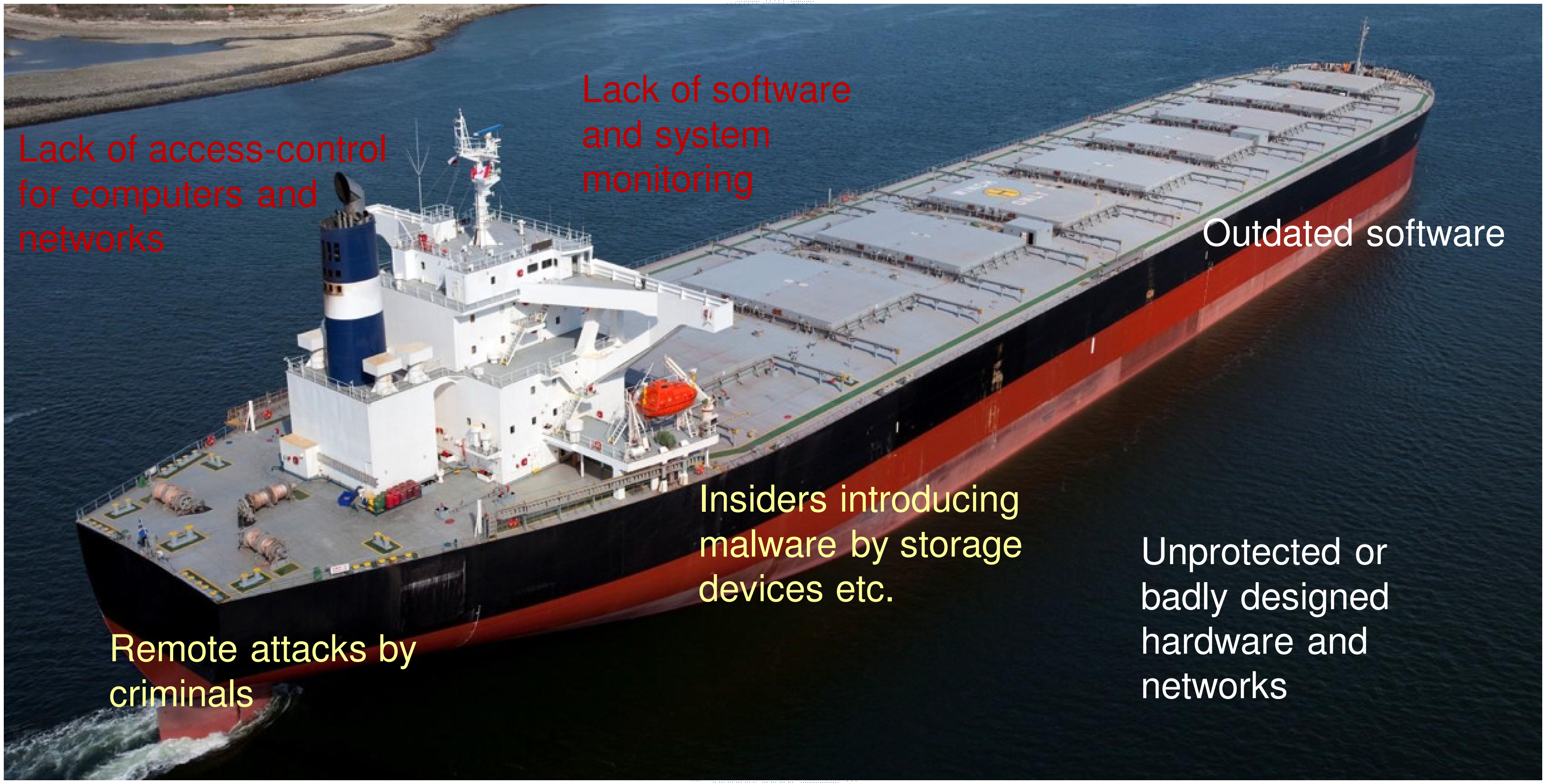
Lars Robert Pedersen, Deputy Secretary General

Cyber incident definition

Occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.

Source: National Initiative for Cybersecurity Careers and Studies (NICCS)

Risks on board ships



Lack of access-control for computers and networks

Lack of software and system monitoring

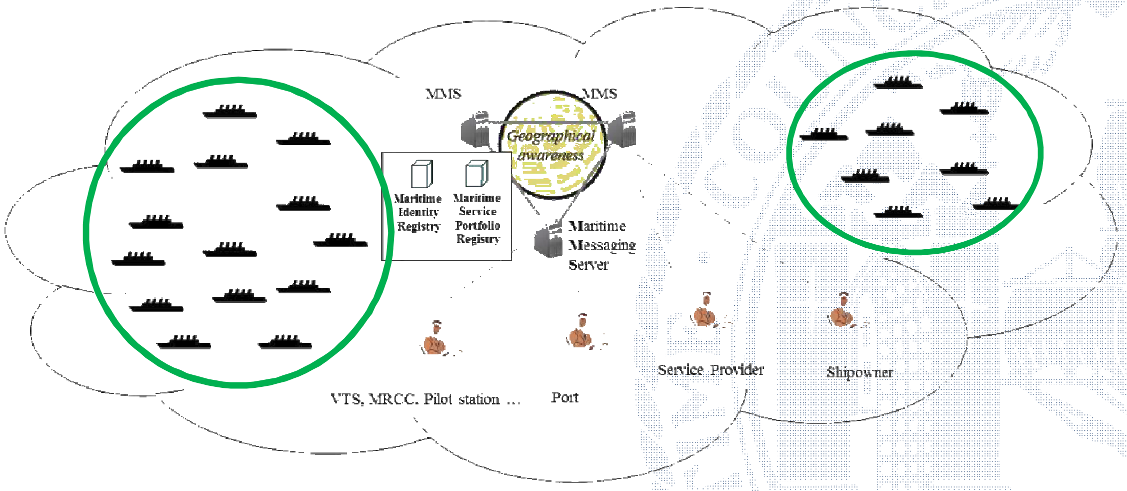
Outdated software

Insiders introducing malware by storage devices etc.

Unprotected or badly designed hardware and networks

Remote attacks by criminals

Risks for other e-Nav stakeholders


MMS
MMS
Geographical awareness
Maritime Identity Registry
Maritime Service Portfolio Registry
Maritime Messaging Server
VTS, MRCC. Pilot station ...
Port
Service Provider
Shipowner

- *Individual ships are addressed*
- Central infrastructure?
- Individual service providers?
- The Maritime indetity registry?
- The Maritime service portfolio registry?

- Risks should be addressed at the initial stage
- Risks are not dissimilar to those applicable to ships
- Likelihood of exploitation is higher for landbased installations

Ships are vulnerable to cyber attacks

- Ships chartered to 3rd party operators
  - The shipowner does not have control over the IT systems required by the charterer
- Passengers and external persons have access to the ships
- Critical data pertaining to cargo is passed through numerous land-side entities
  - Penetration of the weakest link in the chain can result in any data element being compromised
- A high reliability on IT systems related to safety
  - ECDIS and satellite receivers make a ship susceptible to either penetration or jamming

Attacking a ship will not stop world trade

- A ship is an independent unit and a cyber attack may compromise safety of that ship, the marine environment and to some extent, the business continuity of the owner
- To a large extent the crew will use the same contingency plans as for any other emergency if the ship is compromised

Attacking critical infrastructure may stop trade in a future “e-Nav world”

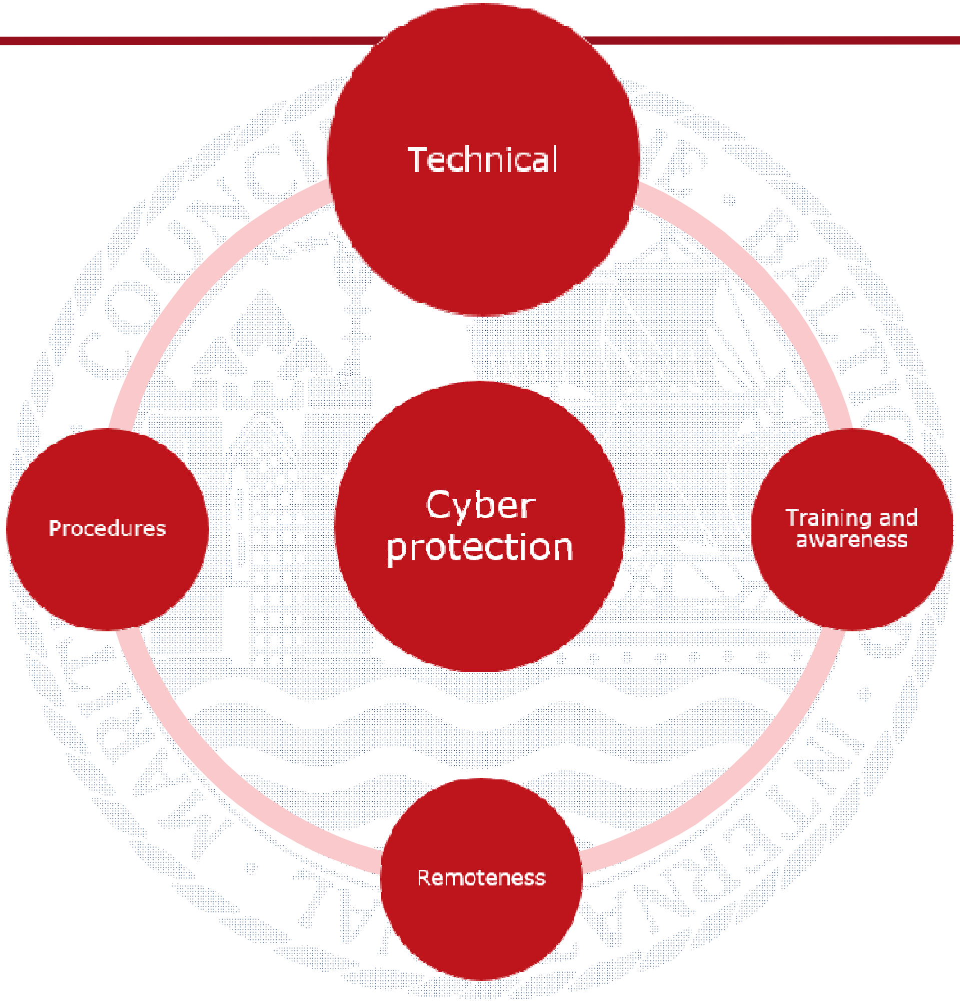
BIMCO

- The Central Identity Registry is critical
- E-Navigation rely specifically on trust in the identity of participants.
- BIMCO pointed out last year that the trust issue is critical to the success of e-Navigation
- The benefits from e-Navigation will never be realised if the confidentiality, integrity and availability of the participants are not maintained
- Cyber security must thus be central to the development of e-Navigation

Agility needed

- Cyber attacks techniques develop constantly so mitigating measurers will also have to change constantly
- IMO regulation would be too slow
- Type approval of software is not the full answer, as it is a static process

- We see industry best management practice as the way to operationally cope with cyber security



Technical

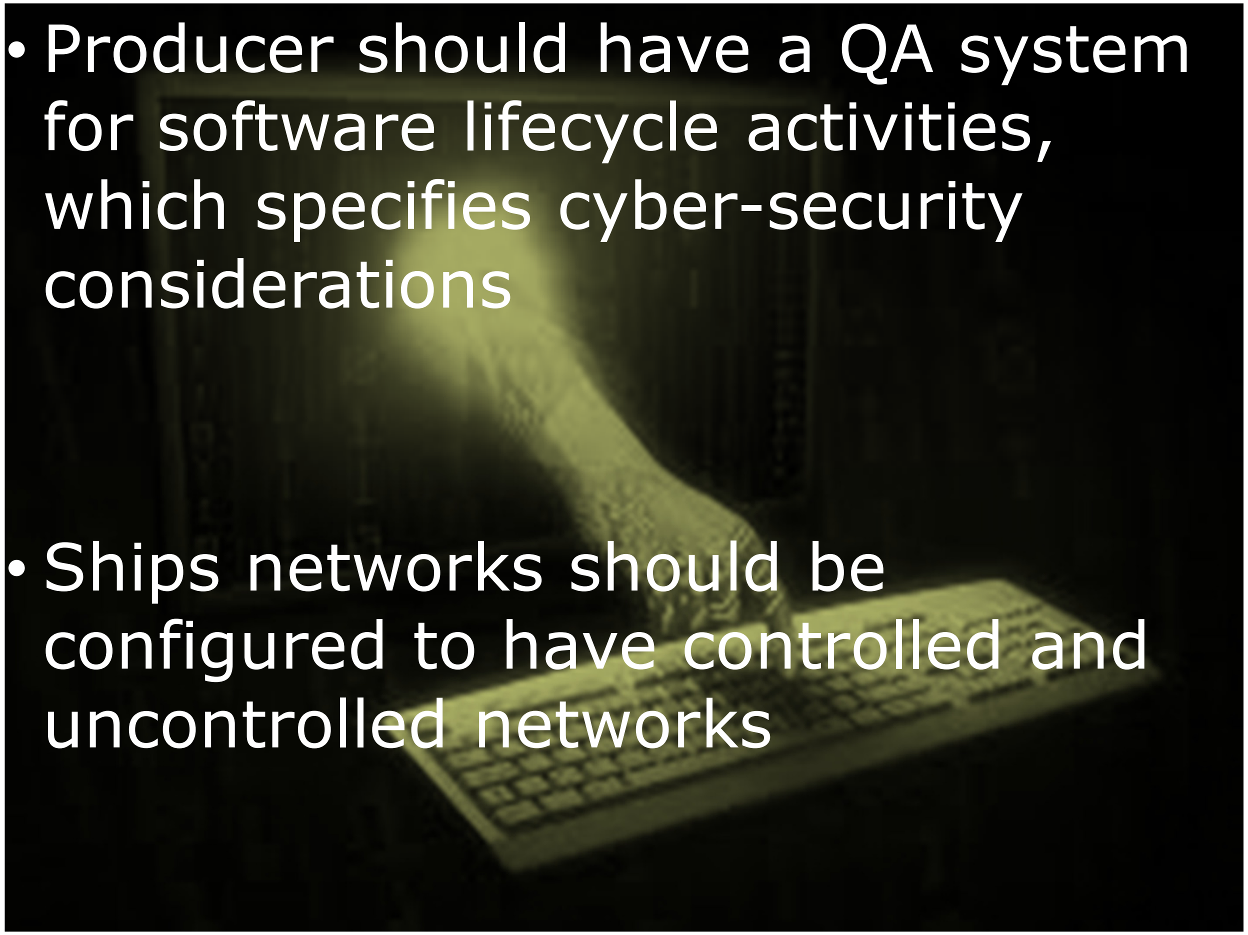
Cyber protection

Procedures

Training and awareness

Remoteness

It starts during construction



- Producer should have a QA system for software lifecycle activities, which specifies cyber-security considerations
- Ships networks should be configured to have controlled and uncontrolled networks

Risk based approach needed

- Some organisations, ships and systems may be more at risk than others, depending on the type and value of data stored
- To manage risks, personnel should understand the probability for an event to occur and the resulting impact

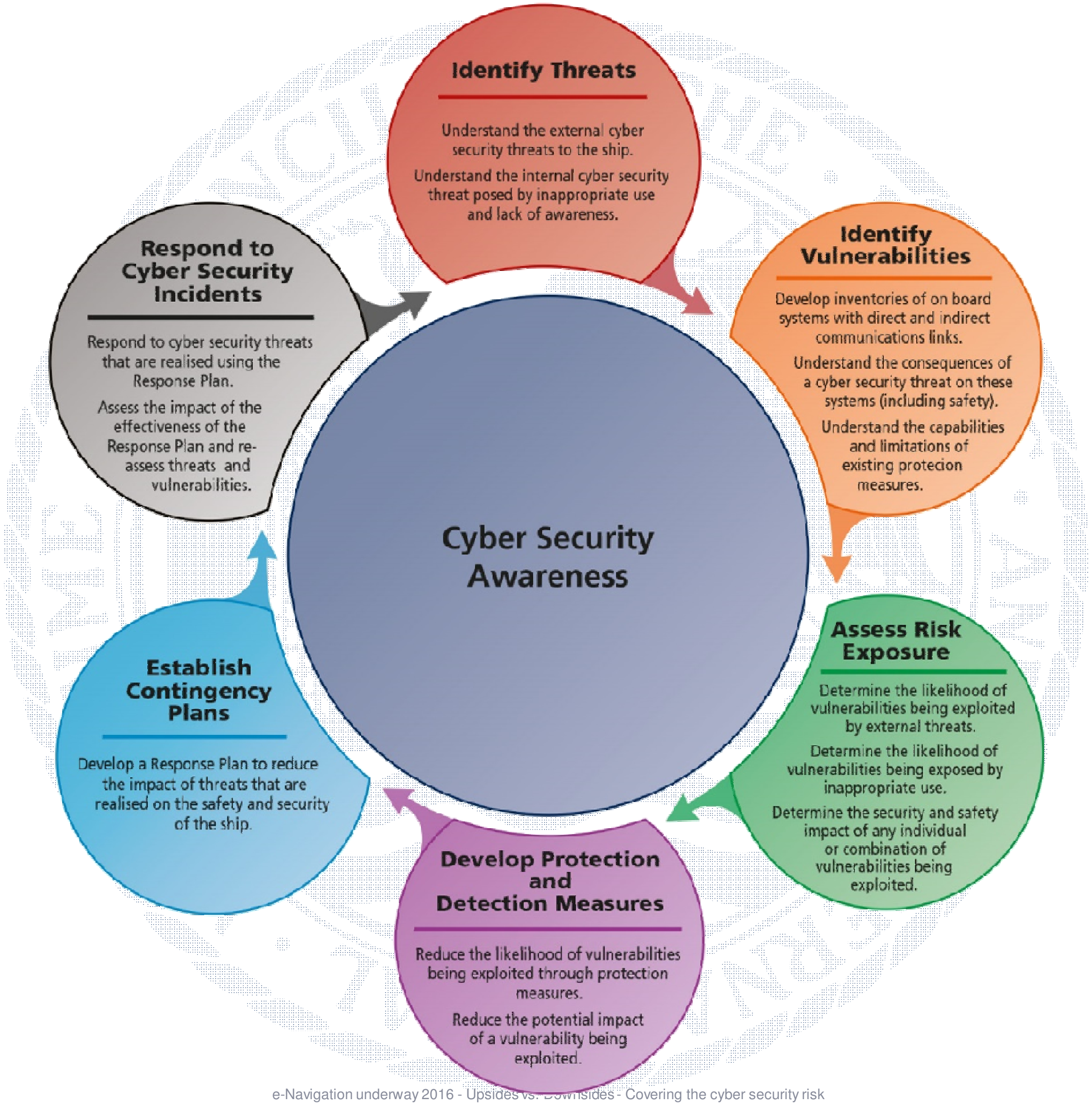
The Industry Guidelines on Cyber Security on board Ships

The guidance includes how to:

- minimize the risk of a cyber-attack through user access management
- protect on board systems
- develop contingency plans and
- manage incidents if they do occur

THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS

Produced and supported by
BIMCO, CLIA, ICS, INTERCARGO, and INTERTANKO



Cyber Security Awareness

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.

Identify Vulnerabilities

Develop inventories of on board systems with direct and indirect communications links.

Understand the consequences of a cyber security threat on these systems (including safety).

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.

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 Contingency Plans

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

Respond to Cyber Security Incidents

Respond to cyber security threats that are realised using the Response Plan.

Assess the impact of the effectiveness of the Response Plan and re-assess threats and vulnerabilities.

IMO proces

- BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO will submit the Industry Guidelines on Cyber Security on board Ships to the next session of the FAL and MSC for consideration
- US and Ca submission to FAL on IMO guidelines
- Possible US and Ca submission to MSC on IMO guidelines

- Question is, should IMO develop guidelines?, or leave the initiative to industry at this stage

Initiatives underway

- the finalisation of industry guidelines on cybersecurity on board ships intended to be applied by shipowners, managers and seafarers in order to mitigate maritime cybersecurity risks;
- the work in a joint BIMCO and CIRM working group to developed a standard on Software Maintenance of Shipboard Equipment;
- the decision taken in December 2015 by IACS, to create a Cyber Systems Panel to lend support and resources to address what has become a key industry issue. Upgrading the existing IACS Expert Group on Cyber Systems to a full Panel will significantly enhance the ability of classification societies to address cyber system safety concerns; and
- the decision, also taken in December 2015, by a number of industry associations, representing shipowners, ship operators, shipbuilders, insurers and classification societies to establish a cross industry Joint Working Group on Cyber Systems.

Conclusions

- Awareness is needed in the industry
- Industry Guidance will be submitted to IMO
- Cyber crime is constantly developing and we need to keep up
- Cyber security considerations should start at the software production stage and cyber robustness considerations should be made when the ship is constructed
- Cyber security should be an integral component of all e-Navigation initiatives

BIMCO