BIMCO

Cyber Security
update

Lars Robert Pedersen

Tripartite 2019, Tokyo

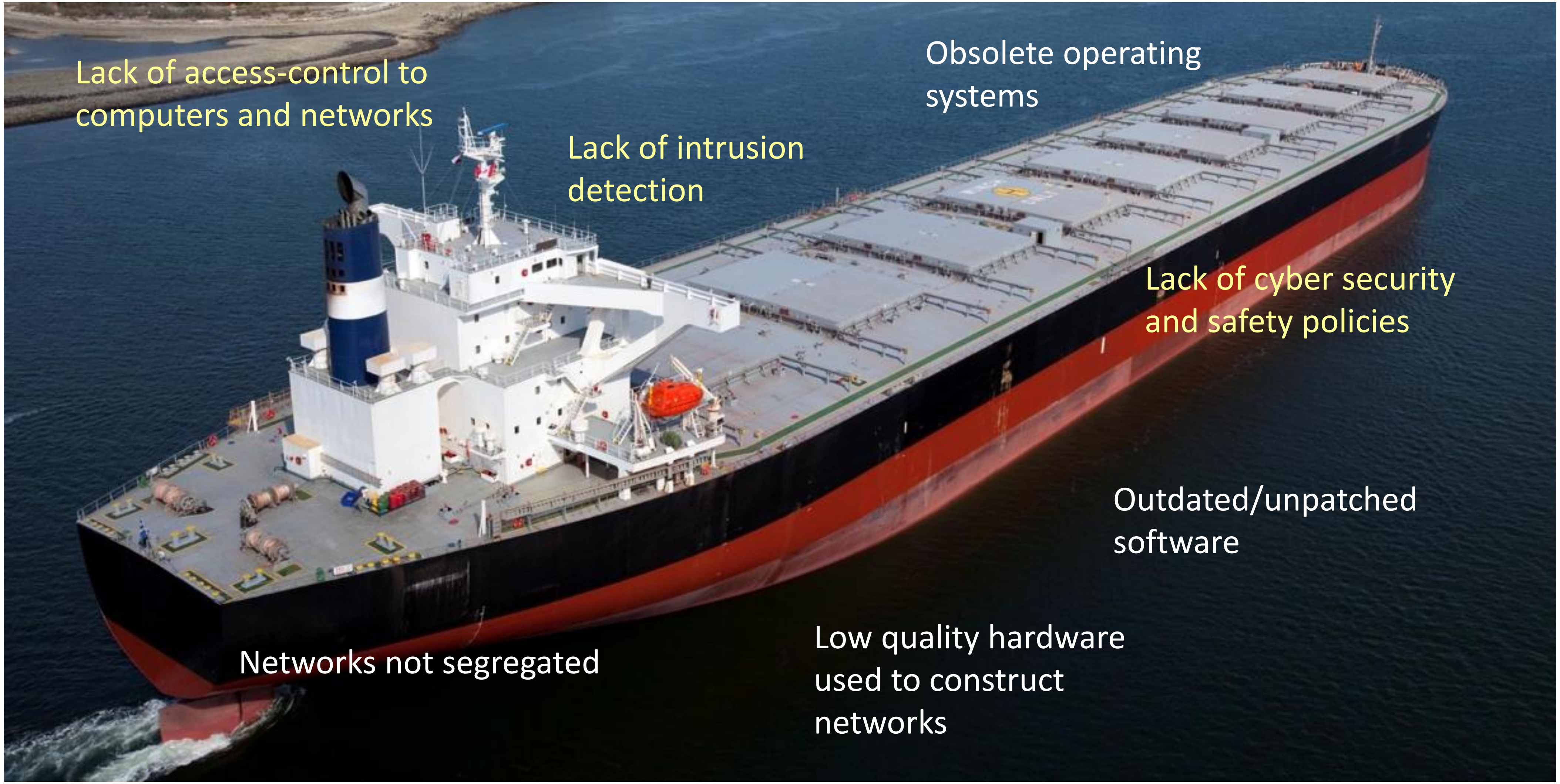
Current trends in cyber security

- FBI: Multi-factor authentication by-pass by criminals
- Patch management a risk management strategy
- Attacks targetting IoT devices
- DOJ: Bribed AT&T workers planted malware in carriers network
- Ransomware continues to hit corporations and public institutions

Human behaviour remain central to mitigation

Sharing of information important to keep up with developments

Vulnerabilities onboard ships



Lack of access-control to computers and networks

Lack of intrusion detection

Obsolete operating systems

Lack of cyber security and safety policies

Outdated/unpatched software

Networks not segregated

Low quality hardware used to construct networks

Three things that needed to be done

The cyber risk must be managed by the shipowner

Ships should be built in a cyber resilient way

Equipment software should be designed with cyber risks in mind

International Maritime Organization 2019

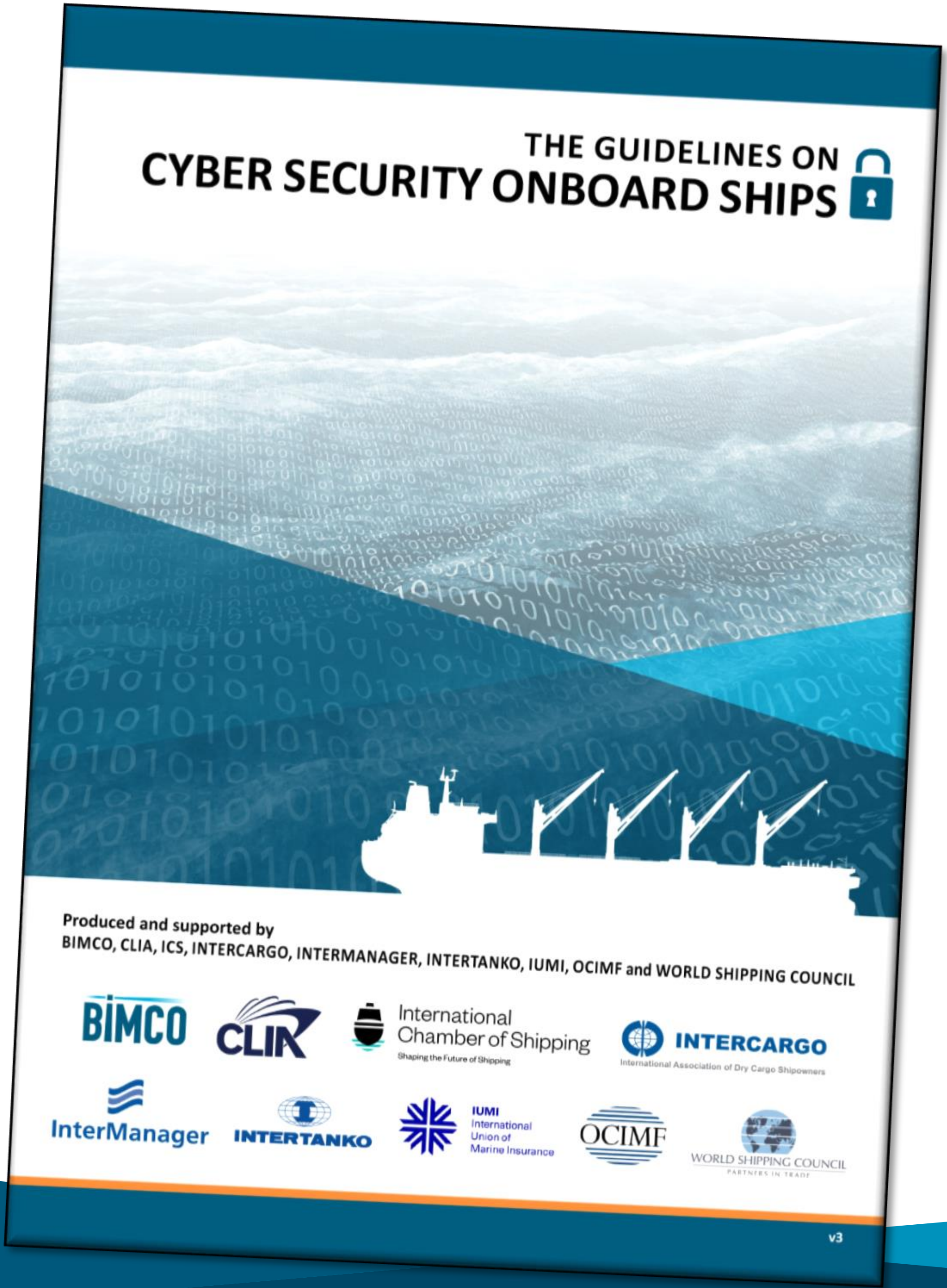
- agreed that aspects of cyber risk management, including physical security aspects of cyber security, should be addressed in Ship Security Plans under the ISPS Code
- confirmed that resolution MSC.428(98) set out the Organization's requirements for Administrations to ensure that cyber risks were appropriately addressed in existing SMS
- encouraged Administrations to engage with other national and regional authorities to explain the IMO's requirements for cyber risk management by companies

Different risk exposures

Except when it comes to the crew

NEW

- More focus on Operational Technical systems
- How to address cyber risk in the SMS
- Relationship between ship manager, agent, vendors and shipowner
- Disconnecting the ship when having a cyber incident
- 7 cyber incidents added

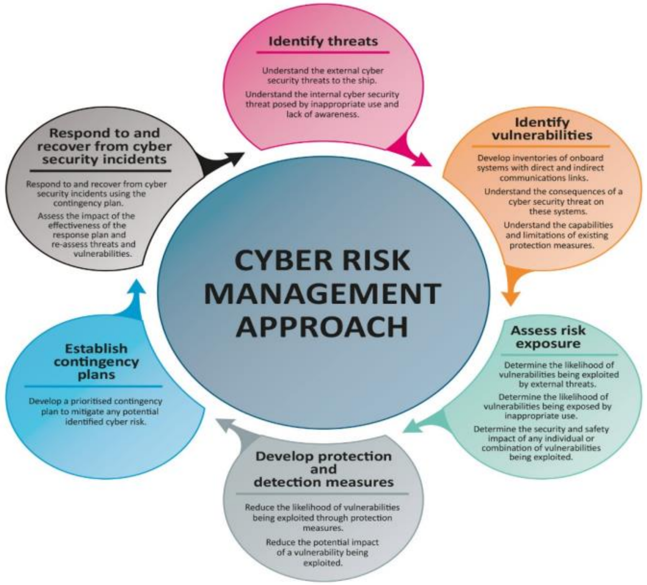


THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS

Produced and supported by
BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL

v3

Accepted by shipowners, classification societies and the International Maritime Organisation



CYBER RISK MANAGEMENT APPROACH

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 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 protection 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

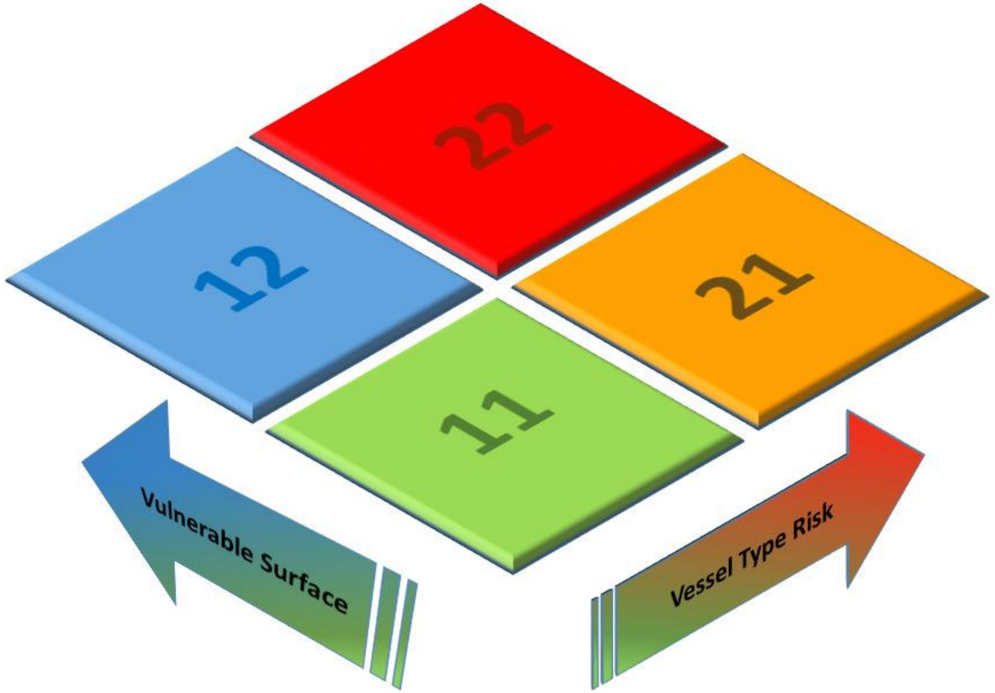
Develop a prioritised contingency plan to mitigate any potential identified cyber risk.

Respond to and recover from cyber security incidents

Respond to and recover from cyber security incidents using the contingency plan.

Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.

International Association of Classification Societies (IACS) interim recommendations



Recommendation 1 'Software Maintenance'
Recommendation 4 ‘Manual Backup’
Recommendation 3 'Contingency Post Failure'
Recommendation 4 'Network Architecture'
Recommendation 5 'Data Assurance'
Recommendation 6 'Physical Security'
Recommendation 7 'Network Security'
Recommendation 8 'Vessel System Design (and handover)'
Recommendation 9 'Programmable System Equipment Inventory'
Recommendation 10 'Integration'
Recommendation 11 'Remote Update / Access'
Recommendation 12 'Communication and Interfaces'

Revised recommendations February 2020 to be submitted to IMO

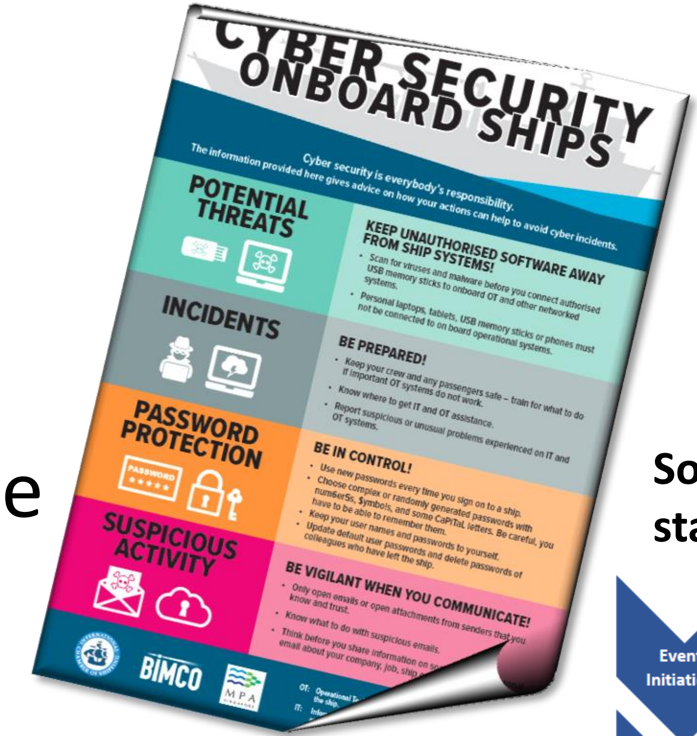
Information sharing platform

- Can we set up an information sharing facility in shipping?
  - Who should host?
  - Who should participate?

- Can an international platform be trusted for sharing data?
  - Role of flag states?
  - Trust between states?

What is next?

- Ship owners prepare the SMS and train personnel
- New ships to be built in accordance with IACS recommendations
- Equipment and systems should enable contemporary software and this should be maintained



CYBER SECURITY ONBOARD SHIPS

Cyber security is everybody's responsibility.
The information provided here gives advice on how your actions can help to avoid cyber incidents.

POTENTIAL THREATS

KEEP UNAUTHORISED SOFTWARE AWAY FROM SHIP SYSTEMS!
- Scan for viruses and malware before you connect authorised USB memory sticks to onboard OT and other networked systems.
- Personal laptops, tablets, USB memory sticks or phones must not be connected to on board operational systems.

INCIDENTS

BE PREPARED!
- Keep your crew and any passengers safe – train for what to do if important OT systems do not work.
- Know where to get IT and OT assistance.
- Report suspicious or unusual problems experienced on IT and OT systems.

PASSWORD PROTECTION

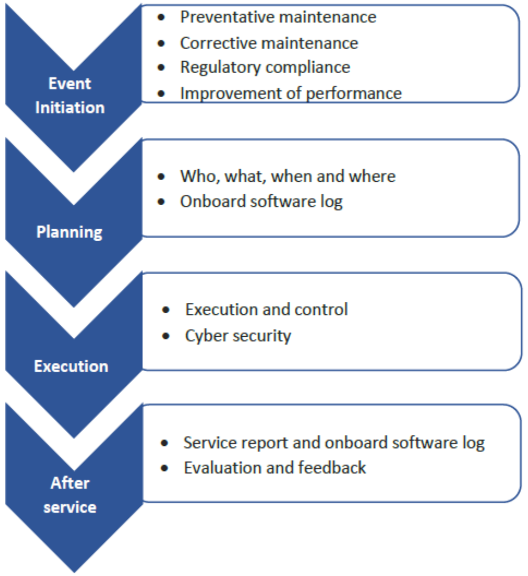
BE IN CONTROL!
- Use new passwords every time you sign on to a ship.
- Choose complex or randomly generated passwords with num6er5s, $ymbo!s, and some CaPiTaL letters. Be careful, you have to be able to remember them.
- Keep your user names and passwords to yourself.
- Update default user passwords and delete passwords of colleagues who have left the ship.

SUSPICIOUS ACTIVITY

BE VIGILANT WHEN YOU COMMUNICATE!
- Only open emails or open attachments from senders that you know and trust.
- Know what to do with suspicious emails.
- Think before you share information on so
email about your company, job, ship

OT: Operational Te
the ship.
IT: Info

Software maintenece standard



- Preventative maintenance
- Corrective maintenance
- Regulatory compliance
- Improvement of performance

- Who, what, when and where
- Onboard software log

- Execution and control
- Cyber security

- Service report and onboard software log
- Evaluation and feedback

Thank you!

Contact BIMCO at

www.bimco.org

Guidelines can be downloaded for free at our website