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 targeting 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
- Networks not segregated
- Obsolete operating systems
- Lack of cyber security and safety policies
- Outdated/unpatched software
- 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
• 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
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
Thank you!

Contact BIMCO at
www.bimco.org

Guidelines can be downloaded for free at our website