Maritime cyber security

Jakob P. Larsen, Head of Maritime Security

jpl@bimco.org

2019 ReCAAP ISC Piracy and Sea Robbery Conference

Agenda

- The regulatory framework
- Shipping industry guidance
- Cyber incident examples from real life

Regulatory framework for cyber security

- Ambiguity from IMO:
  - "…recommend a risk management approach to cyber risks that is resilient and evolves as a natural extension of existing safety and security management practices."
  - "ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021."

BIMCO, ICS and United States' approach

BIMCO

- Physical access to restricted areas should be managed under the ISPS Code (Ship Security Assessment and Ship Security Plan)
- Other cyber risks should be managed under the ISM Code in the Safety Management System

- This will facilitate
  - Up to date procedures,
  - Avoiding duplication,
  - Best possible level of cyber security,
  - Reduced cost to ship owners (avoiding frequent updates to SSP).

Industry guidance for cyber security on board ships

- Cyber security and safety management
- Threat identification
- Vulnerability identification
- Risk assessment
- Protection and detection measures
- Contingency plans
- How to respond and recover

THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS

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

v3

Virus in ECDIS delays ship’s departure

- Technical problem
- No paper charts on board
- Maker’s technician called in
- Virus discovered, isolated and ECDIS computers restored
- Deleays cost hundreds of thousands USD

Crash of integrated navigation bridge

- Ship experienced failure of nearly all systems at sea, in dense traffic and reduced visibility
- Ship had to navigate for two days using paper chart and a stand-alone radar to reach port
- Maker’s technician had performed software updates of navigation software running on ship’s computer
- Outdated operatingn system was unable to run the updated software, and crashed

Worm attack on maritime IT and OT

- Onboard power management system connected to the internet
- Company IT department discovered a dormant worm that could have activated when ship was connected to the internet
- Worm believed to originate from maker’s service technician
- Worm spread via USB to all servers and associated equipment
- Worm was undiscovered for 875 days

Main application server infected by ransomware

- Ransomware infection on the main application server of a ship caused complete disruption of the IT infrastructure
- Ransomware encrypted all essential files and data was lost
- Poor password policy enabled attackers to log on via remote management services
- The undocumented user was deactivated and stronger password policy was introduced

Comments and questions