Cyber Security and eNavigation

Lars Robert Pedersen – Deputy secretary general, BIMCO

Copenhagen, 31 January 2017
<table>
<thead>
<tr>
<th>Products</th>
<th>Training</th>
<th>Regulation</th>
<th>Information and advice</th>
</tr>
</thead>
<tbody>
<tr>
<td>contracts &amp; clauses</td>
<td>eLearning</td>
<td>international</td>
<td>environment</td>
</tr>
<tr>
<td>IDEA2</td>
<td>classroom courses</td>
<td>regional</td>
<td>safety</td>
</tr>
<tr>
<td>Shipping KPIs</td>
<td>webinars</td>
<td></td>
<td>security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>navigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>chartering support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>market analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>credit risk</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debt recovery</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ports and cargo databases</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>publications</td>
</tr>
</tbody>
</table>
Today’s presentation:

- Is cyber a problem?
- Revision of the Guidelines on Cyber Security on Board Ships
- What should be done next?
IHS Markit and BIMCO launched the maritime cyber security survey on 22 July. The survey, which ran for four weeks, was promoted on social media and via email. More than 300 industry players responded. Of the 300 respondents, 65 had been a victim of a cyber attack. Here are some of the highlights of the insights gathered from respondents to the maritime cyber security survey.
Have you been a victim of cyber attack?

- Yes: 21%
- No: 57%
- No responses: 22%
Survey - Continued

What was the nature of the attack?

- Malware: 77%
- Phishing: 57%
- Spear Phishing: 23%
- Application attack: 9%
- Brute force: 13%
- Denial of service: 18%
- Network of protocol attack: 14%
- Man in the middle: 4%
- Theft of credentials: 25%
- Known vulnerability: 7%
- Other: 9%
Survey - Continued

What was the extent of the attack?

- 48% Loss of corporate data
- 21% Financial loss
- 67% IT system functionality
- 4% Shipborne systems functionality
Cyber Attack

- A ship is an independent unit and a cyber attack may compromise the safety of that ship, the marine environment and to some extent, the business continuity and reputation 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.
# Understanding the Cyber Threat to Ships

<table>
<thead>
<tr>
<th>Group</th>
<th>Motivation</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activists (including disgruntled employees)</td>
<td>• Reputational damage</td>
<td>• Destruction of data</td>
</tr>
<tr>
<td></td>
<td>• Disruption of operations</td>
<td>• Publication of sensitive data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Media attention</td>
</tr>
<tr>
<td>Criminals</td>
<td>• Financial gain</td>
<td>• Selling stolen data</td>
</tr>
<tr>
<td></td>
<td>• Commercial espionage</td>
<td>• Ransoming stolen data</td>
</tr>
<tr>
<td></td>
<td>• Industrial espionage</td>
<td>• Ransoming system operability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Arranging fraudulent transportation of cargo</td>
</tr>
<tr>
<td>Opportunists</td>
<td>• The challenge</td>
<td>• Getting through cyber security defences</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Financial gain</td>
</tr>
<tr>
<td>State sponsored organisations Terrorists</td>
<td>• Political gain</td>
<td>• Gaining knowledge</td>
</tr>
<tr>
<td></td>
<td>• Espionage</td>
<td>• Disruption to economies and critical national infrastructure.</td>
</tr>
</tbody>
</table>

And of course the persons onboard the ships!
Ways to protect your ship

Cyber protection

- Technical
- Procedures
- Training and awareness
- Remoteness
THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS

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

Under revision
Guideline revision plan

• Accepted by shipowners, classification societies, and the International Maritime Organization, so only minor amendments
• Annex 3 regarding onboard networks to be clarified
• The layered approach more details to be added
• Additional guidance on the ship shore interface
• Remote software maintenance guidance
• Insurance issues
What is next?

- Awareness needed in the industry – learn from incidents
- e-Navigation may add vulnerabilities and solutions should consider cyber security
- Ships should be built with cyber secure networks/components, and use contemporary software
- Supply chain cyber security considerations is coming – risk assessment of business partners
Equipment manufacturers – what is next?

- Equipment manufactures should have a QA system for software lifecycle activities
  - Equipment and systems should be designed to facilitate patching of vulnerabilities
  - Cyber security starts with the manufacturing of on board equipment
  - Remote software maintenance should be prepared so it can be done in a safe and secure way
Thank you!

Contact BIMCO at
www.bimco.org