

Cyber Security and eNavigation

Lars Robert Pedersen – Deputy secretary general, BIMCO

Copenhagen, 31 January 2017

Products

- contracts & clauses
- IDEA2
- Shipping KPIs

Training

- eLearning
- classroom courses
- webinars

Regulation

- international
- regional

Information and advice

| | |
|--------------|-------------------|
| Ships | Commercial |
|--------------|-------------------|

- environment
- safety
- security
- navigation

- chartering support
- market analysis
- credit risk
- debt recovery
- ports and cargo databases
- publications

Today's presentation:



- Is cyber a problem?
- Revision of the Guidelines on Cyber Security on Board Ships
- What should be done next?

IHS MARKIT

Cyber security survey

In association with BIMCO

2016



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?



21%

Yes



57%

No

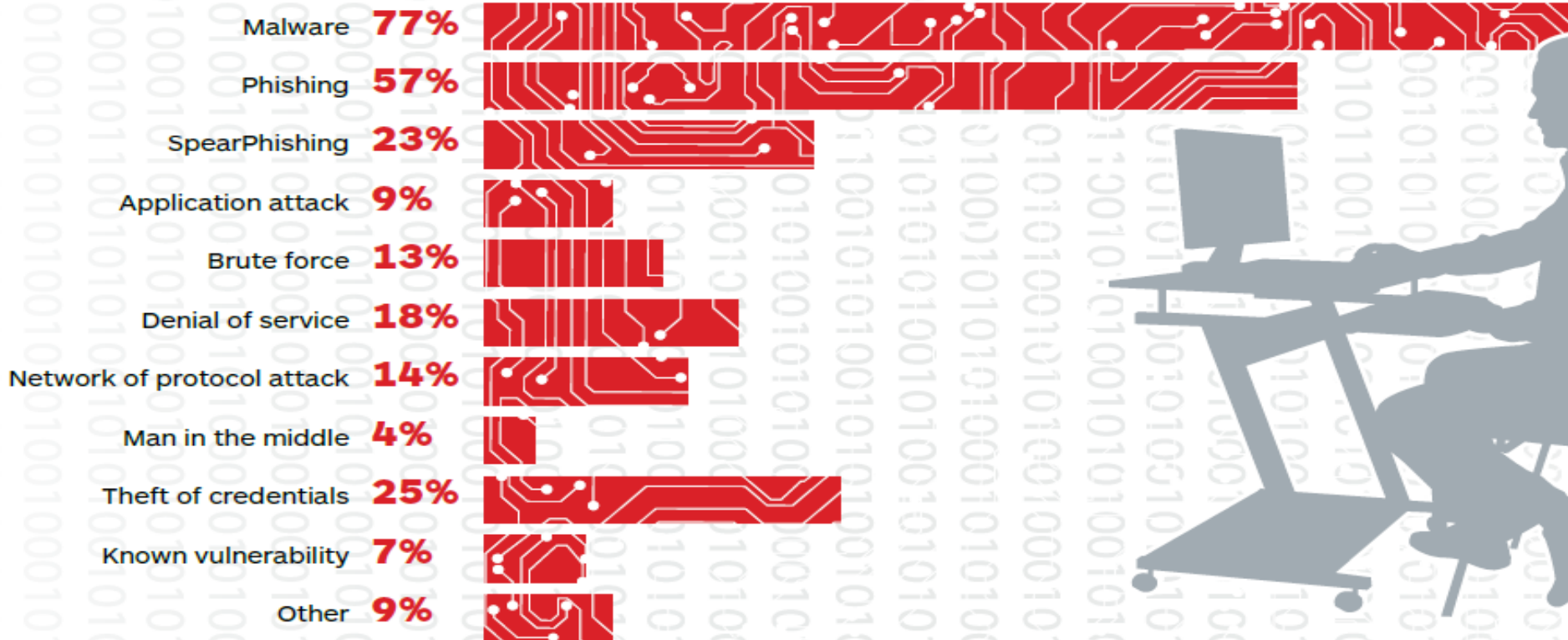


22%

No responses

Survey - Continued

What was the nature of the attack?



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

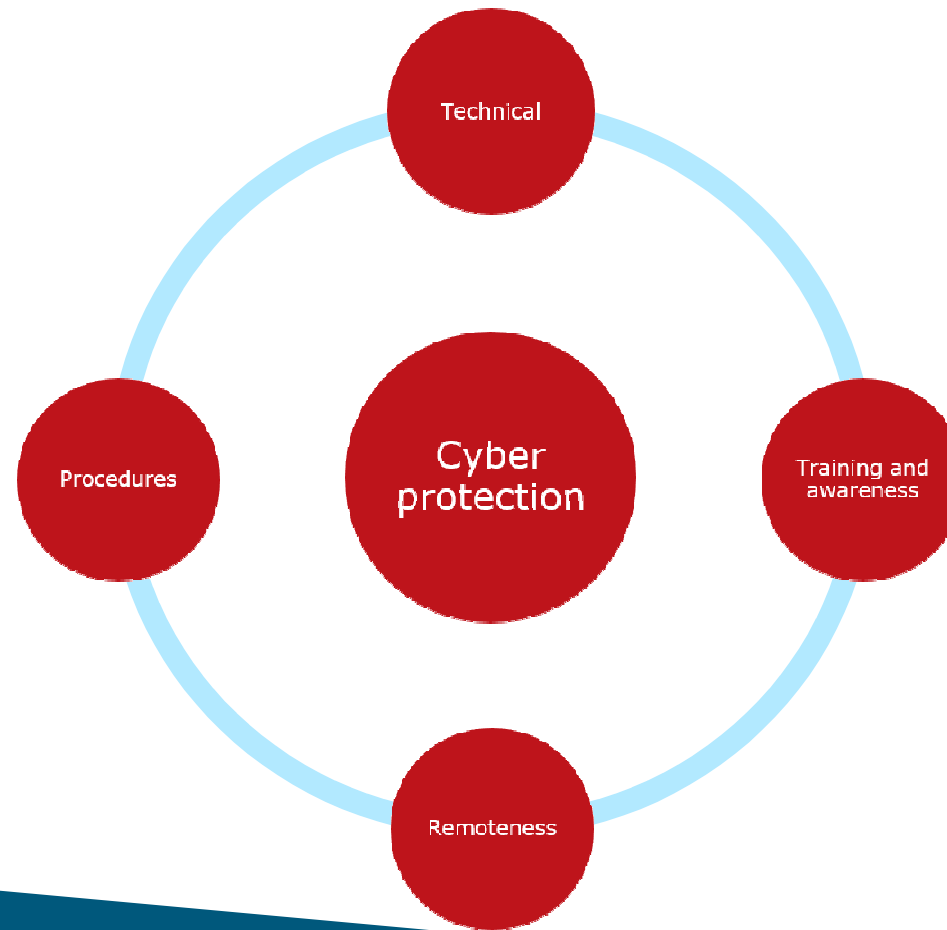
Understanding the Cyber Threat to Ships



| Group | Motivation | Objective |
|---|--|--|
| Activists (including disgruntled employees) | <ul style="list-style-type: none"> • Reputational damage • Disruption of operations | <ul style="list-style-type: none"> • Destruction of data • Publication of sensitive data • Media attention |
| Criminals | <ul style="list-style-type: none"> • Financial gain • Commercial espionage • Industrial espionage | <ul style="list-style-type: none"> • Selling stolen data • Ransoming stolen data • Ransoming system operability • Arranging fraudulent transportation of cargo |
| Opportunists | <ul style="list-style-type: none"> • The challenge | <ul style="list-style-type: none"> • Getting through cyber security defences • Financial gain |
| State sponsored organisations Terrorists | <ul style="list-style-type: none"> • Political gain • Espionage | <ul style="list-style-type: none"> • Gaining knowledge • Disruption to economies and critical national infrastructure. |

And of course the persons onboard the ships!

Ways to protect your ship



THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS


BIMCO



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



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
- 
- A decorative graphic at the bottom of the slide, consisting of overlapping blue shapes that create a wave-like effect.

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 manufacturers 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





BIMCO

Thank you!

Contact BIMCO at
www.bimco.org