Cyber Security – Maritime Industry

INTRODUCTION TO BIMCO

Taking Maritime Cyber Security Seriously

Ways to protect your ship

Vulnerabilities onboard ships
INTRODUCTION TO BIMCO
Our strength in numbers

- 3 locations – Shanghai, Singapore, Copenhagen
- 50+ staff – 13 nationalities
- 57% of the world’s tonnage
- 2,000 members in over 120 countries
- 10,000 helpdesk enquiries per year
- 30,000 followers on social media
- 3 million page views on BIMCO website per year
- 1 billion TDW and growing
Taking Maritime Cyber Security Seriously
Today’s presentation:
Taking Maritime Cyber Security Seriously.

- Knowledge and awareness
- Cyber vulnerabilities on ships - No one is excluded.
- The Guidelines on Cyber Security on Board Ships
- Ways to protect your ship
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
ISO/IEC 27032:2012
Information technology -- Security techniques -- Guidelines for cybersecurity

The NIST Cyber Security Framework
How to Reduce the Security Risk of your Institution

Be Cyber Aware At Sea - The Film

Why Aspida
Aspida is a unique risk management organization that provides fast and efficient solutions to complex situations and high risk environments.

#1 DEC 2016
PHISH & SHIPS

#2 JAN 2017
PHISH & SHIPS

#3 FEB 2017
PHISH & SHIPS

#4 MAR 2017
PHISH & SHIPS

Recommended Practice
DNV-GL, RP-0401, 2016-07
Cyber security resilience management for ships and mobile offshore units in operation

Our approach is based on Security, not IT.
We are very experienced in complex and high risk Maritime and Security projects.
We use a holistic approach to provide a 360° cover. by partnering with, developing secure SCRs and working in social engineering.
## Motivation and Objectives

<table>
<thead>
<tr>
<th>Group</th>
<th>Motivation</th>
<th>Objective</th>
</tr>
</thead>
</table>
| Activists (including disgruntled employees) | • Reputational damage  
• Disruption of operations | • Destruction of data  
• Publication of sensitive data  
• Media attention  
• Denial of access to the service or system targeted |
| Criminals                    | • Financial gain  
• Commercial espionage  
• Industrial espionage | • Selling stolen data  
• Ransoming stolen data  
• Ransoming system operability  
• Arranging fraudulent transportation of cargo  
• Gathering intelligence for more sophisticated crime, exact cargo location, off vessel transportation and handling plans etc. |
| Opportunists                 | • The challenge                           | • Getting through cyber security defences  
• Financial gain |
| States                       |                                           | • Gaining knowledge  
• Disruption to economies and critical national infrastructure |
| State sponsored organisations |                                           |                                                                           |
| Terrorists                   |                                           |                                                                           |
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.
What was the extent of the attack?

- 48% Loss of corporate data
- 21% Financial loss
- 67% IT system functionality
- 4% Shipborne systems functionality
What was the nature of the attack?

- Malware: 77%
- Phishing: 57%
- SpearPhishing: 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%
Vulnerabilities onboard ships
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
The cyber attack
The impact

On June 27th A. P. Moller – Maersk, amongst many global companies, were hit by the malware NotPetya.

49,000 laptops infected
ALL print capability inaccessible
1200 applications were inaccessible
1000 applications were destroyed
FILE shares unavailable

76 port terminals closed around the world
Cost to the business USD $300m
Ways to protect your ship
The Guidelines on Cyber Security onboard Ships
Ways to protect your ship
What to do to minimize the risk of Cyber attacks in the practical level
Summarize

- DISMANTLING NEWBUILDCON SUPERMAN
- cyber awareness programme
- TERM SHEET ANTI-CORRUPTION eBILLS OF LADING
Cyber Security
Can you afford not to do it?