



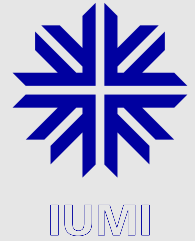
# Cyber Risks and Marine Insurance

Lars Lange, IUMI Secretary General

SIMI Marine Insurance Forum,  
27 Nov 2017, Renaissance Shanghai Pudong Hotel

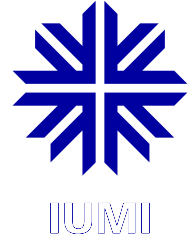


# Agenda



- 1. What's the risk?**
2. Is this covered?
3. What do ship-owners do?
4. Are classification societies aware?
5. What is IMO's approach?
6. And where does this lead to?

# 1. What's the risk?



## Ship

- Ships fully connected to the shore
- Electronic systems like ECDIS updated online
- Navigation and route planning online-based
- Crew using wireless connections
- Cargo management automated

## Cargo

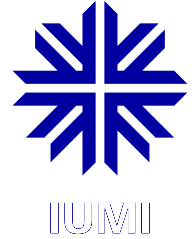
- Warehouse management computer based
- Port terminals automated and fully online

## Offshore

- Vulnerable electronic systems and high exposures



# 1. What's the risk?



... and it's a moving target

- Digitalization is ongoing - **technical expertise**
- autonomous shipping – **higher vulnerability**
- Smart port logistics / intelligent containers – **new open doors**
- Blockchain technology, IoT, internet based placing platforms – **big data**

**Systemic risk?**

**NotPetya** as an example – estimated costs of 250-300 bn. USD alone for Maersk



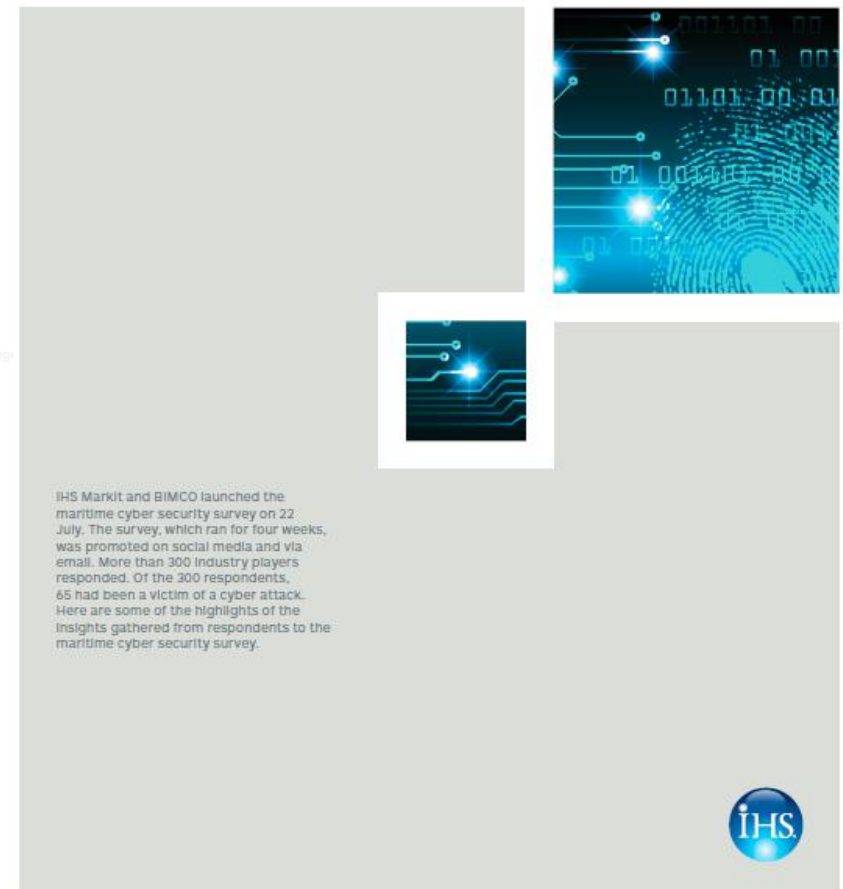
By Maersk Line - A container dressed in blue  
Source: commons.wikimedia.org



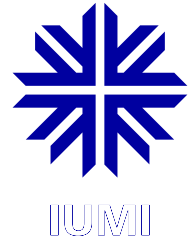
# 1. What's the risk?



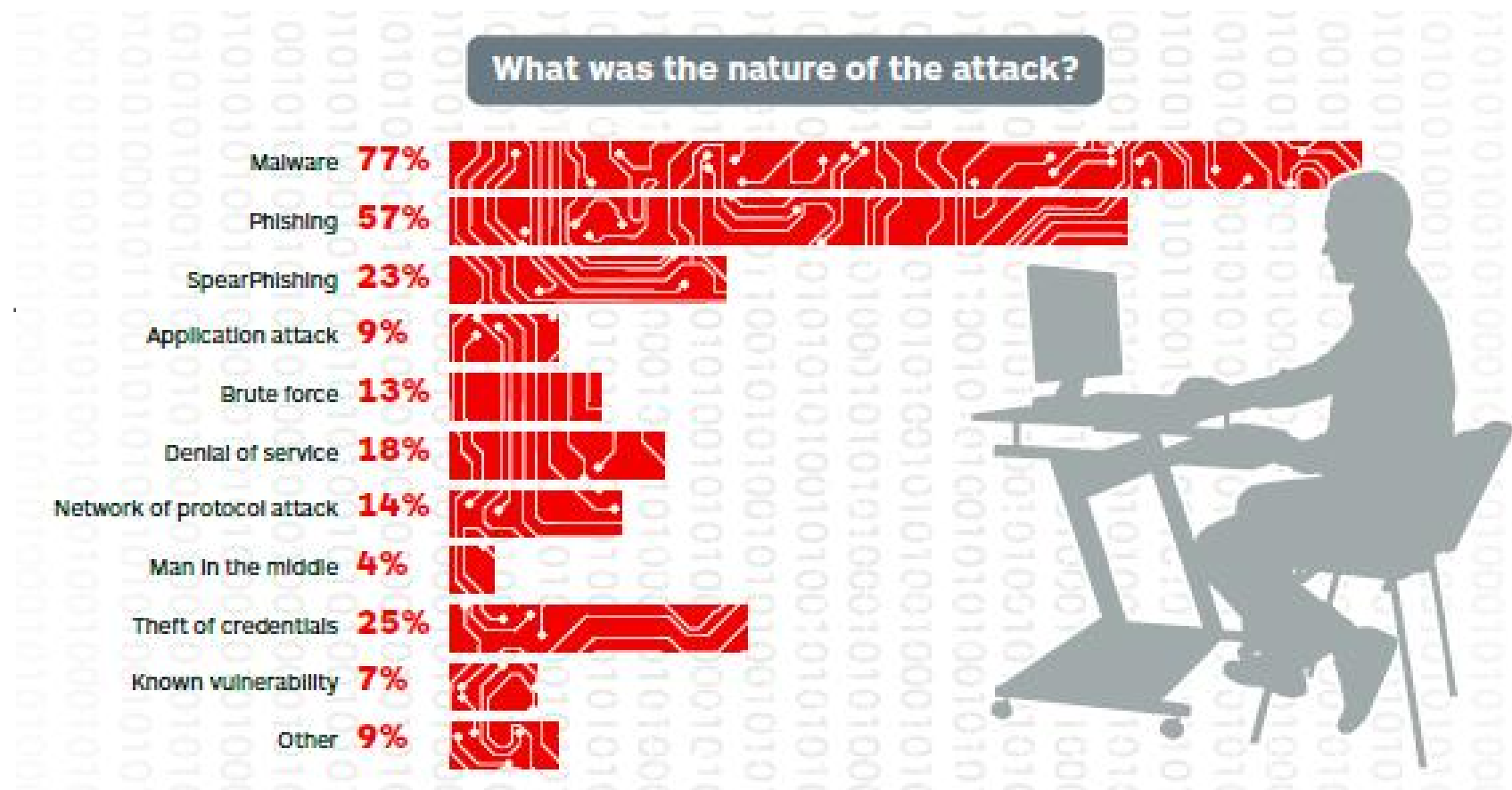
## BIMCO / IHS Markit „Cyber Security Survey“



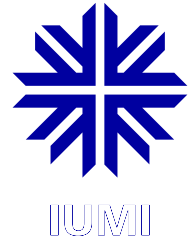
# 1. What's the risk?



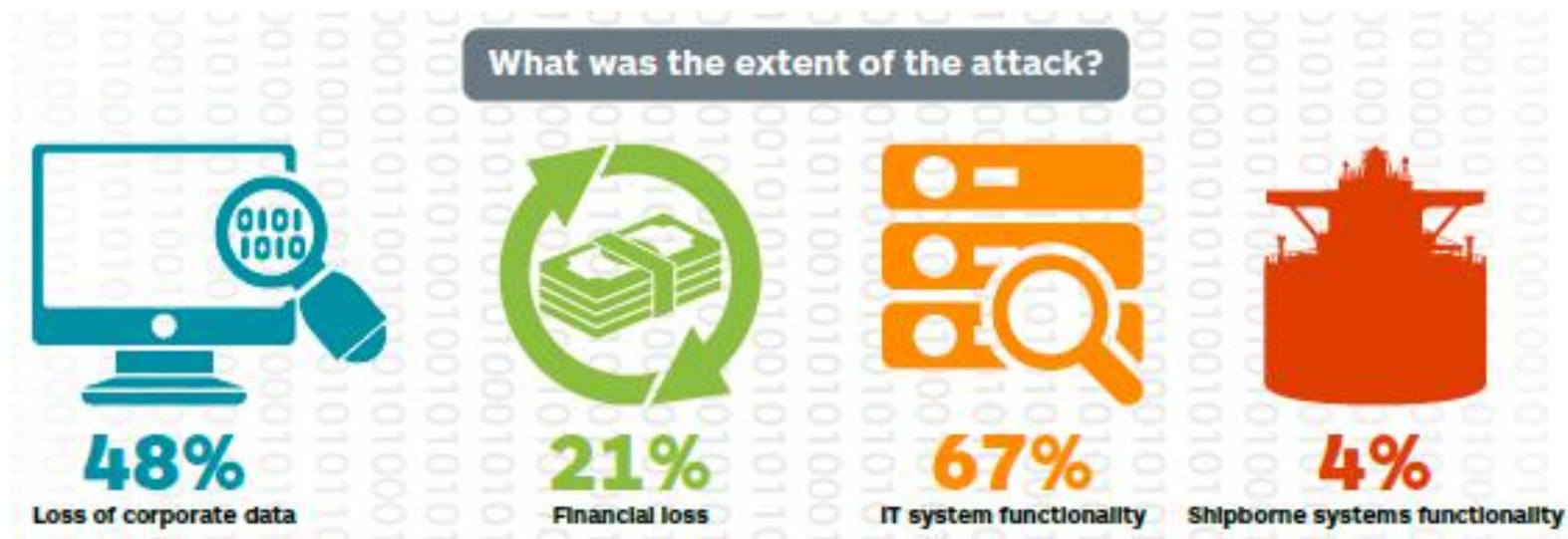
## BIMCO / IHS Markit „Cyber Security Survey“



# 1. What's the risk?



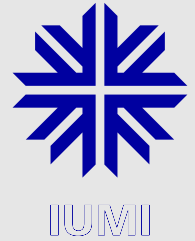
## BIMCO / IHS Markit „Cyber Security Survey“



... and did you tell your insurers?



# Agenda



1. What's the risk?
- 2. Is this covered?**
3. What do ship-owners do?
4. Are classification societies aware?
5. What is IMO's approach?
6. And where does this lead to?



## 2. Is this covered?



depends on individual clauses, cover and line of business:

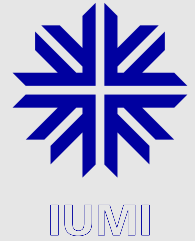
- E.g. CL 380 for cyber attacks
- Silent cover?
- Forwarder's liability

«Perils of the Sea»: Shouldn't insurers aim to grant coverage?

- Understand the risk
- Assess and mitigate the risk
- Give recommendations to clients
- make it insurable

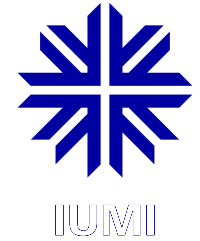


# Agenda



1. What's the risk?
2. Is this covered?
- 3. What do ship-owners do?**
4. Are classification societies aware?
5. What is IMO's approach?
6. And where does this lead to?

### 3. What do ship-owners do?



- Guidelines published in July 2017 (2<sup>nd</sup> edition)
- IUMI is co-author, insurance chapter is added
- Very concrete guidance for the crew:



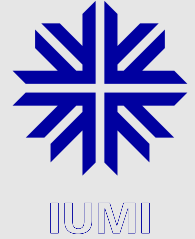
**THE GUIDELINES ON  
CYBER SECURITY ONBOARD SHIPS**

The cover image of the guidelines shows a stylized, abstract landscape with blue and white waves or clouds. In the foreground, there is a silhouette of a ship's hull and superstructure. The background is filled with a pattern of binary code (0s and 1s) in a light blue color.

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

**BIMCO** **CLIR** **INTERCARGO** **INTERTANKO** **OCIMF** **IUMI**  
International Union of Marine Insurance

# Agenda



1. What's the risk?
2. Is this covered?
3. What do ship-owners do?
- 4. Are classification societies aware?**
5. What is IMO's approach?
6. And where does this lead to?

## 4. Are classification societies aware?



Numerous **classification societies** working on it individually - DNV.GL, ABS etc.

### IACS:

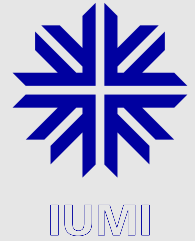
- Founded “Cyber Panel” in Dec 2015
- Founded “JWG on Cyber Systems” in Nov 2016
  - Industry representatives included
  - Flag states included (including IMO WG chair)
- Intended output: Recommendations; Unified Requirements (UR) and / or Unified Interpretations (UI) are further down the line



**IUMI:** supports and is member of the IACS JWG

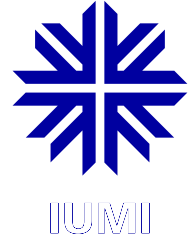


# Agenda



1. What's the risk?
2. Is this covered?
3. What do ship-owners do?
4. Are classification societies aware?
- 5. What is IMO's approach?**
6. And where does this lead to?

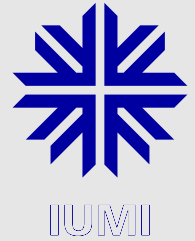
## 5. What is IMO's approach?



- Maritime Safety Committee (MSC) 96 in May 2016: Interim Guidelines on Maritime Cyber Risk Management (MSC.1/Circ.1526)
- MSC 98 in June 2017:
  - cyber risk management onboard ships should become part of the ISM Code and form part of the ship's mandatory Safety Management System by 2021 – audits!
  - Interim Guideline transferred to permanent Guideline
- IMO best place to deal with cyber?
- IUMI welcomes IMO's framework and prefers industry solutions for detail – e.g. "BIMCO Guideline"

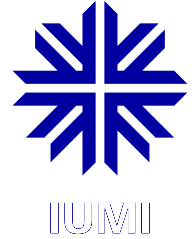


# Agenda



1. What's the risk?
2. Is this covered?
3. What do ship-owners do?
4. Are classification societies aware?
5. What is IMO's approach?
- 6. And where does this lead to?**

## 6. And where does this lead to?

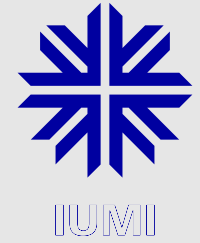


### Opportunity or threat?

- Digitalization and interconnectedness will continue
- Vulnerability in the industry will hence even more increase
- Strong demand for insurance coverage and additional services
- Insurers should build up expertise and present themselves as cyber experts to their clients
- IUMI will play its role in this



# Agenda



**... and last but not least**



# Connect to IUMI



- **IUMI Asia Forum**

Singapore, 24/25 April 2018

[www.iumi.com](http://www.iumi.com)



## IUMI 2018 ASIA FORUM

In association with GIA Singapore

- **IUMI Conference 2018**

Cape Town / ZA, 16-19 September 2018

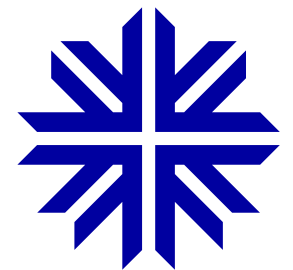
[www.iumi2018.com](http://www.iumi2018.com)





# That's it!

Lars Lange  
Secretary General  
International Union of Marine Insurance e.V.  
Große Elbstraße 36  
D-22767 Hamburg  
[lars.lange@iumi.com](mailto:lars.lange@iumi.com)



IUMI