HFW

SHIPPING

CYBER RISKS AND PROTECTION IN SHIPPING

IT JUST GOT REAL

DIGITAL SHIP MARITIME
CIO FORUM ATHENS

ELECTRA PANAYOTOPOULOS
PARTNER, HFW

“There are two types of companies:
those who have been hacked and those who don’t yet know they’ve been hacked.”

John Chambers - Executive Chairman and former CEO of Cisco

"It takes 20 years to build a reputation and
five minutes to ruin it.
If you think about that, you'll do things differently.”

Warren Buffett

1.RISKS

2. SHIPPING

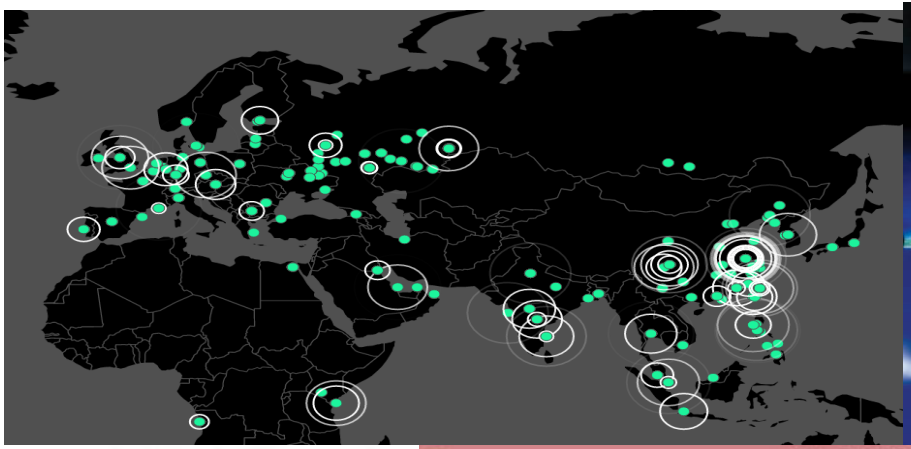
3. INSURANCE

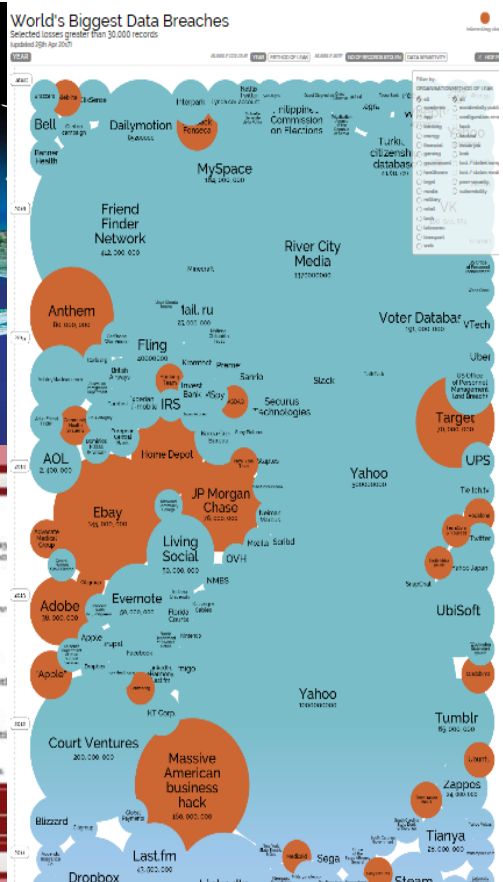
4. PROTECTION

1. RISKS

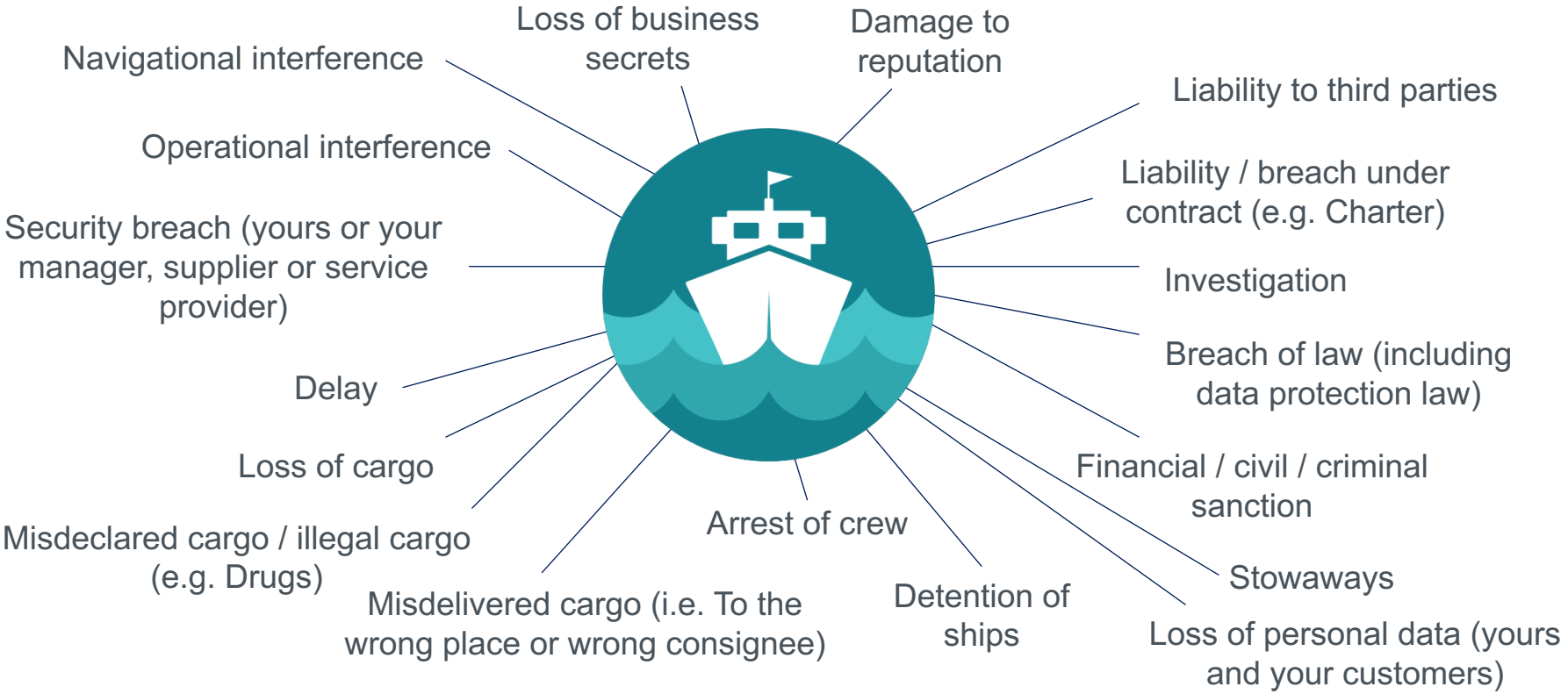
HFW

BACKGROUND





SHIP OWNERS AND OPERATORS: **RISKS**



A ‘NEW’ THREAT?

- In addition to Maersk – a large number of incidents in the past twelve months or so alone:
  - Diversion of payments – to shipyards for repairs, to shipowners for freight, crew wages and many others
  - Hacking of accounting/banking systems
  - Theft of personal and/or sensitive data
  - At best – a headache/legal bill/having to pay twice
  - At worst – major business interruption and commercial losses. Or disaster?
- Not the first time that the maritime industry had to consider the risks of its great reliance on cyber technology
- But last time (Y2K) it was over 17 years ago, the reliance has since increased and it now involves criminal intent - there is serious risk that one can be caught unawares.

SOME OTHER MARINE CYBER EVENTS

- Infiltration of digital shipping systems by Somali pirates to identify ships with high value cargo lacking adequate electronic security (2010)
- Infiltration of drug smuggling gang of computerised cargo tracking system at Antwerp to discover drugs hidden in containers (2011)
- Criminal syndicates penetrating Australian cargo systems (2012)
- Criminals extracting release codes and documents for delivery of containers from terminal facilities
- Chinese military reportedly hacking a commercial ship on contract to US military (2012)
- An online bunkering scam targeting a major fuel supplier (2013)
- Temporary denial of service disruption shutting down multiple ship to shore grains at US port facility (2014)
- Hack causing floating oil platform in African Seas to tilt, forcing temporary shutdown (2015)

2. SHIPPING

- **EssDOCS, BOLERO, CargoDocs** electronic bills of lading (E-BoL)
- Used in 73 countries by over 3,800 customers
- Across all shipping modes
- Cyber security "*is a core element...developed through years of methodical testing and industry input18". The integrity and security of the E-BoL system is critical, but so is your preparation for and response to a cyber event in your contracts, insurance and internal policies.*
- Increased use = increased risk of cyber event, such as:
  - redirection or misappropriation of goods
  - fraudulent E-BoLs issued or
  - the E-BoL system is hacked to gain access to information / documents

NYPE 1946 clause 15

- *"breakdown or damages to hull, machinery or equipment… or by any other cause preventing the full working of the vessel, the payment of hire shall cease for the time thereby lost"*
- "Any other cause" actually means any other cause like the ones in the preceding list – so, depending on the way in which a cyber event manifests itself, and the way in which it prevents the full working of the vessel, a cyber event may be an off-hire event
- Charterers being advised to include specific reference to cyber events and a clear definition of what "cyber events" means

CHARTERPARTIES – **PAYMENT OF HIRE**

CHARTERPARTIES – **LAYTIME AND DEMURRAGE**

- Attack on ship -v- attack on shore
- Interruptions and exclusions

Common law obligation

- Vessel, crew, equipment, sound and able to withstand ordinary perils of the sea
- Ship suitable to carry the cargo
- Includes systems, manning and documents – not just physical condition

Hague/Hague Visby Rules

- Articles III(1) and IV(1)
- Claims under charter and contract of carriage

ISM Code

SIRE

Rightship

CHARTERPARTIES – **UNSAFE PORT**

3. INSURANCE

- **s. 39 of the MIA 1906:**

  (1) In a voyage policy there is an implied warranty that at the commencement of the voyage the ship shall be seaworthy for the purpose of the particular adventure insured.

  ...

  (5) In a time policy there is no implied warranty that the ship shall be seaworthy at any stage of the adventure, but where, with the privity of the assured, the ship is sent to sea in an unseaworthy state, the insurer is not liable for any loss attributable to unseaworthiness.

- Is a ship “seaworthy” if the Vessel’s or the Company’s network is not protected against attack or if the Vessel’s GPS and AIS can be easily ‘hacked’ and there is no means in place to know when this has happened?

- **Hull & Machinery – insure your property**
  - Institute Cyber Attack Exclusion Clause (Cl.380)

    "in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means of inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system"

- Products to cover the "**Coverage Gap**" and the expensive investigation stage which other policies may not cover

- Requirements of the cover

P&I

- TW 13/6/14: "P&I cover is sufficiently wide to potentially cover liabilities arising from collisions groundings or other marine risks if these were the result of hacking of a computer system or navigational equipment but would not cover commercial risks, which might be the most threatening and costly aspect of a cyber attack.

- BUT: “Where any claim arises directly or indirectly from [failure to comply with ...], Members will be expected to demonstrate to the satisfaction of the Association that they have taken such steps as an uninsured person acting reasonably in similar circumstances would have take to avoid such a claim. Where an individual Member has not so acted, recovery in respect of any claim will be subject to the Association’s sole discretion”.

Terrorism exclusion, as part of “**War Risks**”

- **War Risks**
  - "*any terrorist or any person acting maliciously, or from a political, religious or ideological motive"* within "Risks Covered"
  - But, must ensure that the insurer's requirements are complied with, with "due diligence"
  - Also, wording similar to the Cyber Risks Exclusion Clause in some policies, for claims above a certain amount

- Real time detection and protection of the ship's and premises' network for emails and Internet Security?
- And who will pay for first party response including public relations, forensics, breach management?

- Professional Indemnity cover?

INSURANCE – **SPECIFIC CHALLENGES**

- Preparation for both Insured and Insurer is critical
- Strength of policy wording: what is intended to be covered?
- Multiplicity of “cyber insurers” in the market

Problems include:

- lack of consistency in wordings
- absence of standard/market definitions of "loss", "damage“, “network” etc
- rapidly changing threats
- uncertainty of contract parties' realistic pre-loss expectations
- shallow pool of experienced (underwriting and) claims personnel
- limited judicial precedent in UK and outside US
- jurisdictional arbitrage: how and where will disputes be resolved?

4. PROTECTION

HFW

CYBER RISKS PROTECTION
TOP 10 TIPS FOR BUSINESSES

Proactive

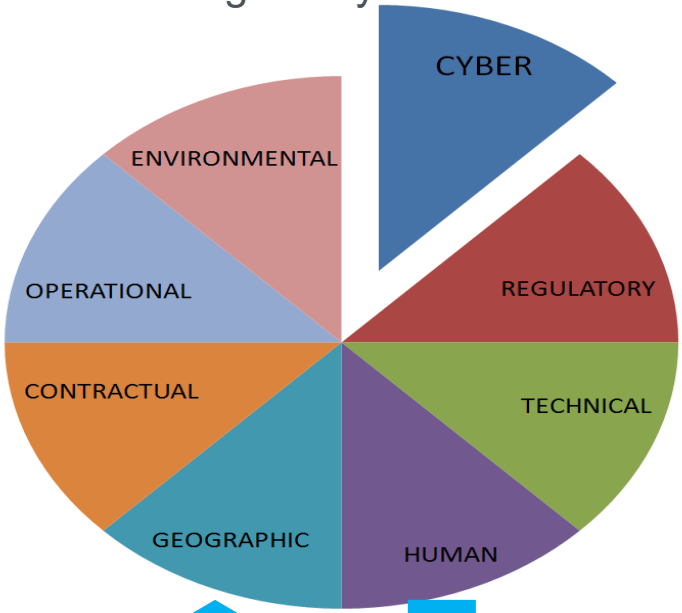
1. Risk assessment
2. Incident management strategy
3. Employee education and awareness
4. Regulatory and compliance
5. Network and IT security

Reactive

1. Detect
2. Assess
3. Contain
4. Investigate
5. Remedy

MANAGING RISK

Sources of financial and regulatory risk



Responding to sources of risk

- ACCEPT
- AVOID
- REDUCE
- TRANSFER

Executing responses

- Build into pricing
- Eliminating certain sources
  - New/different technology
  - New systems
- Contractual
  - Subcontracting
  - Drafting
- Insurance

MONITORING, REVIEWING AND REPORTING

- **Guidelines on Cyber Security Onboard Ships** by BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO
  - Launched on 4 January 2016 and updated in July 2017
  - Voluntary (for the moment)
  - "A tool in assessing and managing cyber risks onboard vessels"
  - *"Guidance to shipowners and operators on how to assess their operations for cyber risks and put in place the necessary procedures and actions to maintain the security of systems onboard their vessels"*
  - *"develop an understanding and awareness of key aspects of cyber security and provide a risk-based approach to identifying and responding to cyber threats"*
- BE CYBER AWARE AT SEA - https://www.becyberawareatsea.com/

HFW

CONCLUSION
THREE KEY POINTS

1) To mitigate risk of attack

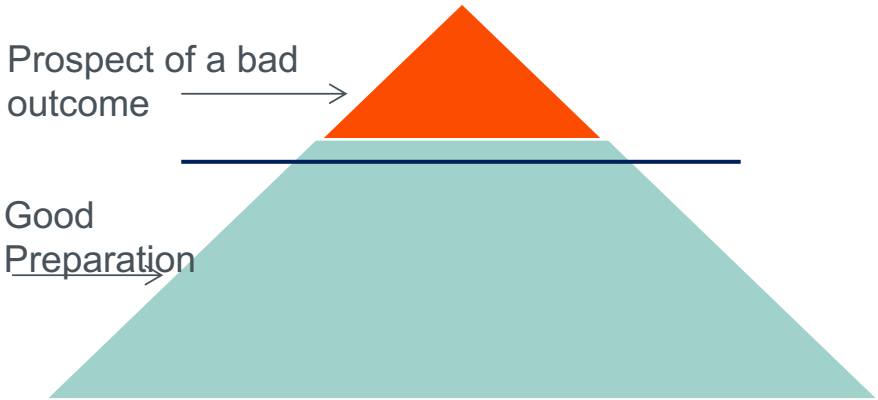
- Cyber Security Plan
- Best Practice
- Training

2) Cyber security insurance

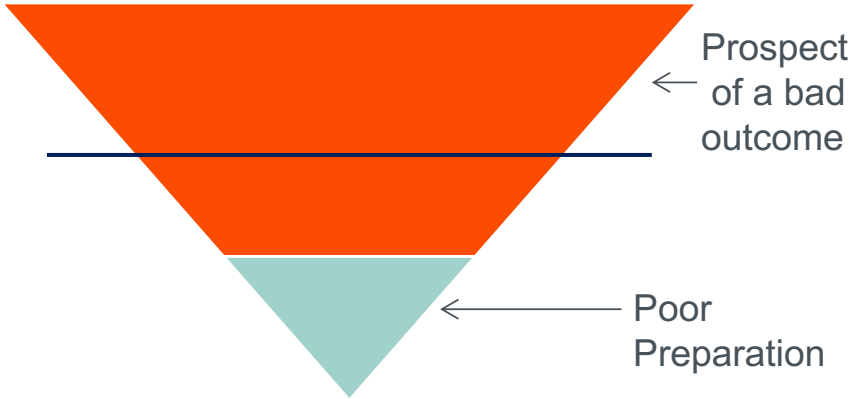
3) In the event of an attack

- Report it to your board
- Comply with regulatory obligations
- Instruct your lawyers
- (crisis management, assess liabilities, ensure legal privilege)

Preparation – Pre-Breach Event



Poor Preparation – Breach Response



Beirut Brussels Dubai Geneva Hong Kong Houston Kuwait London Melbourne Paris Perth Piraeus Riyadh São Paulo Shanghai Singapore Sydney