Cyber Risks and Marine Insurance: Seaworthiness, Causation, and Lessons from Maritime Piracy

M. Bob Kao

PhD Candidate

Queen Mary University of London


"TWO THUMBS UP!"
SANDRA BULLOCK
JASON PATRIC
SPEED 2
CRUISE CONTROL

Cyber Risk in Shipping Industry

- Maritime cyber risk 'refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.' (IMO)

- Terminology: Cyber risk or cyber crime, not cyber attack

Types of Maritime Cybercrimes

- Types of cybercrimes
  - Untargeted
    - social engineering, phishing, water holing, ransomware, and scanning
  - Targeted
    - spear-phishing, deploying of botnets, and subverting the supply chain
    - Information Technology vs Operational Technology

Possible Ramifications

- business disruption
- financial loss
- damage to reputation
- damage to goods and environment
- incident response cost
- fines and/or legal issue
- loss of life

Examples of Potential Attacks

- Hacking of Global Positioning System (GPS) demonstrated by researchers at University of Texas at Austin
- Jamming of GPS demonstrated by the UK and Irish General Lighthouse Authority
- Hacking of Automatic Identification System (AIS) demonstrated by cybersecurity firm Trend Micro
- Hacking of Electronic Chart Display and Information System (ECDIS) demonstrated by NCC Group

Responses by Shipping Industry

- Joint Hull Committee and the law firm of Stephenson Harwood released a *Cyber Attack* report in September 2015

- BIMCO released *The Guidelines on Cyber Security Onboard Ships* in February 2016

- IMO Maritime Safety Committee passed the *Interim Guidelines on Maritime Cyber Risk Management* in June 2016

Implied Warranty of Seaworthiness

- Marine Insurance Act 1906 section 39(4): 'A ship is deemed to be seaworthy when she is reasonably fit in all respects to encounter the ordinary perils of the seas of the adventure insured'.

- *McFadden v Blue Star Line*, quoting *Carver on Carriage by Sea*: 'A vessel must have that degree of fitness which an ordinary careful and prudent owner would require his vessel to have at the commencement of her voyage having regard to all the probable circumstances of it'.

Aspects of Seaworthiness

- physicial state of the vessel and the equipment on board
- training and number of the crew
- appropriate documentation

Seaworthiness in Context of Cyber Security – Hull & Equipment

- Integrity of the hull is unlikely to need special attention to be made seaworthy against cyber threats
- Equipment that need to be guarded can be broadly categorised as communication systems, bridge systems, propulsion and machinery management and power control systems, access control systems, cargo management systems, passenger servicing and management systems, passenger-facing networks, core infrastructure systems, and administrative and crew welfare systems.
- Owners must secure the equipment
  - How is 'ordinary careful and prudent owner' defined in this context?
  - Are cyber threats 'ordinary perils of the seas'?

Seaworthiness in Context of Cyber Security – Master & Crew

- For the ship to be seaworthy, there must be crew members trained to specifically address cybercrimes, and there must be a sufficient number of people to tackle the issue should cyber threats become reality.

- Owners must ensure crew is trained
  - Who should be trained?
  - Can ‘crew’ include personnel not physically on the ship?

Seaworthiness in Context of Cyber Security – Documentation

- For the ship to be seaworthy, appropriate documentation related to cyber risks must be on board ships, including *BIMCO Guidelines*, IMO Guidelines, and other voluntary guidelines that aid the response to cyber threats mentioned earlier.

Causation

- Causation is codified in Marine Insurance Act section 55(1): 'Subject to the provisions of this Act, and unless the policy otherwise provides, the insurer is liable for any loss proximately caused by a peril insured against, but, subject as aforesaid, he is not liable for any loss which is not proximately caused by a peril insured against.

- Multiple causes

Multiple Causes in Cybercrime Scenario

The ship's GPS is attacked and the crew is tricked into thinking the vessel is at a different location than it is actually located. The vessel then ventures into pirate-infested waters and is subsequently attacked by the pirates for its cargo. In such a scenario, what is the proximate cause of the loss?

Lessons from Maritime Piracy

- Nature of piracy problem today
- Similarities and differences to cybercrimes
- Responses to piracy
- Do these responses translate to the cybercrime context?

Conclusions

- Shipping industry is beginning to take cyber threats seriously but the pace is slow.
- However, the lack of substantial real life cases makes some issues that may arise, including seaworthiness and the owner's responsibility, uncertain right now.
- In the absence of guidance from the judiciary, insurers and assureds should inject predictability by agreeing on some of these issues in the policies.
- Lessons can be drawn from responses to piracy but differences need to be noted.