Proteus
Risk Solutions

Cyber Security at Sea

Capt. Walter Justers, AFNI

Cyber attacks

Cyber risk

Risk of financial loss or damage or disruption from failure of information technology systems.

Maritime cyber risk (IMO Interim Guidelines on Cyber Risk Management)

The extent to which a technology asset is threatened by 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.

Cyber attacks

Means to perpetrate cyber attacks

- Phishing e-mails : Corrupted mails seemingly from reliable sources containing infected links or attachments in order to break through security, steal credentials or introduce malware e.g. from banks or persons applying for a job.
- Social engineering : Influencing people e.g. through social media to disclose confidential information (by manipulation or by extortion).
- DDoS (Distributed Denial of Service) attacks

Direct results of a cyber attack

- Data breach : Hackers stealing sensitive data
- Cyber-jacking or cyber-extortion : Hackers ransoming stolen data or blocking the entire computer system and/or website by data encryption and demanding ransom to unlock it (ransomware or ransomweb)

Cyber attacks

Potential consequences of a cyber attack

- Business interruption
- Ransom payments
- Wire transfer fraud
- Loss of reputation and bad publicity
- Third party claims
- Fines for breach of data protection & privacy laws

Vulnerabilities in shipping

General

- Cyber security awareness in the maritime industry is still low
- Risk is presently considered low but getting more significant due to fast development of technology leading to increased automation and connectivity
- Automation so far not accompanied by corresponding security protection

⇒ Challenges ahead!

How can ships be affected by cyber attacks?

Navigation systems

All navigation systems are **not** encrypted and hence are vulnerable to attacks :

- GPS
- ECDIS
- AIS
- Radar
- Gyro
- VDR

Proteus
Risk Solutions

Vulnerabilities in shipping

How can ships be affected by cyber attacks?

Machinery

- Remote condition monitoring of electronically controlled engines (propulsion, power generation, steering systems, etc.) ⇒ Can shut down systems in case of operation beyond set parameters
- Remote control for troubleshooting

Cargo and ballast control systems

- Remote control of valves, pumps, compressors, etc.
- Reefers and other high value cargo stowed in containers being fitted with GPS tracking systems

Proteus Risk Solutions

Vulnerabilities in shipping

How can ships be affected by cyber attacks?

Communication systems

- ➢ Ship’s administration system
- ➢ Crew welfare system
- ➢ Public network for passengers

⇒ Communication via GMDSS considered low risk

⇒ Unprotected port Wi-Fi systems and 4G are high risk

Other

- ➢ Paperless trading (e-Bs/L, e-Manifest)
- ➢ Cruise vessels : passenger data and payment systems

Proteus Risk Solutions

Reported cyber attacks in the maritime sector

- Wire Transfer Fraud by BEC
- The Phantom Menace
- The Enrico Ievoli hijacking
- Cargo tracking system of the port of Antwerp being hacked by drug smugglers between 2011 and 2013
- Pirates stealing high value goods by hacking into the servers of a shipping company
- Tilting over an oil rig off the coast of West Africa
- A ship reported having its GPS signal interrupted by a GPS jammer attached to a stolen prestige car in a container
- Chinese military computer specialists hacked into Transcom systems on board of commercial vessels in order to get access to confidential information.

Proteus
Risk Solutions

International initiatives and legislation

EU

- EU Network and Information Security (NIS) Directive
- GDPR (General Data Protection Regulation) entering into force on 25/05/18

USA

- Cybersecurity Information Sharing Act (CISA) 2015 (in force since 18/12/15)
- National Cybersecurity Protection Act 2014 (in force since 18/12/14)
- US Coast Guard **requires** all MTSA regulated persons to report cyber incidents that may result in transportation security incidents to the National Response Center and the DHS National Cybersecurity and Communications Integration Center
- Trump administration tasked Cyber Review Team to scrutinise US cyber vulnerabilities and defences, in particular so far as critical infrastructure or services are concerned including maritime transport sector

International initiatives and legislation

International initiatives

- Industry Round Table (BIMCO, ICS, Intertanko, Intercargo and CLIA) Guidelines on Cyber Security on board Ships
- IMO Interim Guidelines on Maritime Cyber Risk Management adopted by MSC 96 in May 2016 and are largely based on Industry Round Table Guidelines
- Be Cyber Aware At Sea campaign (www.becyberawareatsea.com)
- Cybersail (https://cybersail.org)
- CSO Alliance (www.csoalliance.com)
- IACS Classification Societies providing assistance to protect security of shipboard cyber-enabled systems
- P&I clubs loss prevention
- OCIMF vetting inspections

Loss prevention

General

- Cyber security : Technologies, processes and practices designed to protect computer programmes and networks against attack or unauthorised access.
- Risk still largely being underestimated across the maritime industry.
- Main stages in the development of a cyber risk management programme :
  - Risk assessment
  - Risk management
  - Emergency response planning
  - Risk transfer

Loss prevention

Risk assessment

- Evaluate the risks in general and those specific to the company in order to better understand the relevant threats and vulnerabilities (external and internal)
- Risk evaluation can be done by self-assessment or with the assistance of cyber security experts
- Ship security risk assessment can be based on principles of the ISPS Code
- Assessment should not only cover the company and its assets but also the regular business partners

Points to consider :

- Present level of compliance with international security management standards such as ISO/IEC 27001
- Past cyber security incidents the company and other shipping companies have experienced as well as the likelihood and potential impact on key shipboard operations
- Assess vulnerability of network connected systems on board (safety critical systems)

Loss prevention

Risk assessment

Suggestions by the Industry Round Table Guidelines :

- Penetration tests simulating attacks on IT/OT systems
- Detailed report to be prepared on the vulnerability of the shipboard IT/OT systems including the likelihood and potential impact of a cyber security breach taking into account the existing controls. The report should also state recommended technical and procedural corrective actions to reduce the risk to an acceptable level
- Reported recommendations to be discussed with manufacturers and service providers in order to establish a remediation plan

Loss prevention

Risk management

- Minimise exposure by reducing both the likelihood as well as the potential consequences of a cyber security breach
- Cyber security measures should be decided at management level and must be in compliance with the relevant flag state and classification requirements
- Measures consist of several layers of defence, the main ones being
  - Implementing technical/design safeguards
  - Adopting industry best practice in respect of computer systems

Technical controls

- Securing IT and OT systems
- Avoiding outdated or unnecessary programmes
- Back-ups
- Secure network engineering on board
- Physical protection of critical hardware/cable runs
- Protection of sensitive information by encryption
- Strong passwords

Loss prevention

Risk management

Procedural controls

- Cyber security awareness and computer best practice training for personnel and crew
- Access control
- Personnel/crew vetting
- Prohibition to use unencrypted or un-scanned physical media
- Prohibition to download and run executable files
- Prohibition to install foreign software on company/ship hardware
- Prohibition to post operational data of the ship on social media
- **Apply good seamanship!**

Proteus
Risk Solutions

Loss prevention

Risk management

Computer best practices

- Beware of phishing scams
- Beware of wire transfer fraud
- Beware of social media
- Avoid using open port networks for exchanging essential or confidential data

Loss prevention

Contingency plans

Plan should lay down procedures to follow is case of cyber security breaches and incidents both ashore and on board :

- How to identify/detect them
- How to respond to them (if successful)
  - Minimise the impact on operability (extent/time)
  - Restore capability
- Reporting
- Investigation and law enforcement

Plans can be developed with the assistance of specialised cyber risk insurers and their cyber security experts or classification societies.

Plans should be regularly reviewed and updated based on

- Development of new relevant legislation
- Evolution in style and pattern of cyber attacks
- Enhanced shipboard automation
- Lessons learnt from experience including drills

Proteus Risk Solutions

Legal issues

Potential seaworthiness issues :

- Hague-Visby Rules duty of the carrier to exercise due diligence to make the vessel seaworthy : What would a skilled and prudent shipowner have done to deal with the risk? What are the currently applicable standards of care and industry best practices?
- General Average : YAR Rule D defence

Potential breach of ISPS Code ⇒ Fines

Off-hire : In case of breakdown of machinery or equipment preventing the full working of the vessel due to a cyber attack the vessel will be off-hire for the time thereby lost.

Risk transfer

Cyber risk insurance to protect business including the advisory and rapid response team provided by insurers can be part of a company's contingency plan.

Issues :

- Specific cyber risk policies generally exclude property damage and personal injury
- Asset protection policies (H&M/War) generally exclude cyber attack

Institute Cyber Attack Exclusion Clause (Cl. 380) or similar included in virtually all marine insurance policies.

As yet, there are little specific marine cyber insurance products covering ships. However :

- Marine underwriters informed CSO Alliance they may in future remove Clause 380 from the policy provided owners commit to proper reporting of cyber incidents allowing underwriters to assess/quantify the risk
- Some London underwriters are willing to remove Clause 380 subject to satisfactory evaluation based on JH2015/005 (JHC Cyber Risk Assessment Guidance)

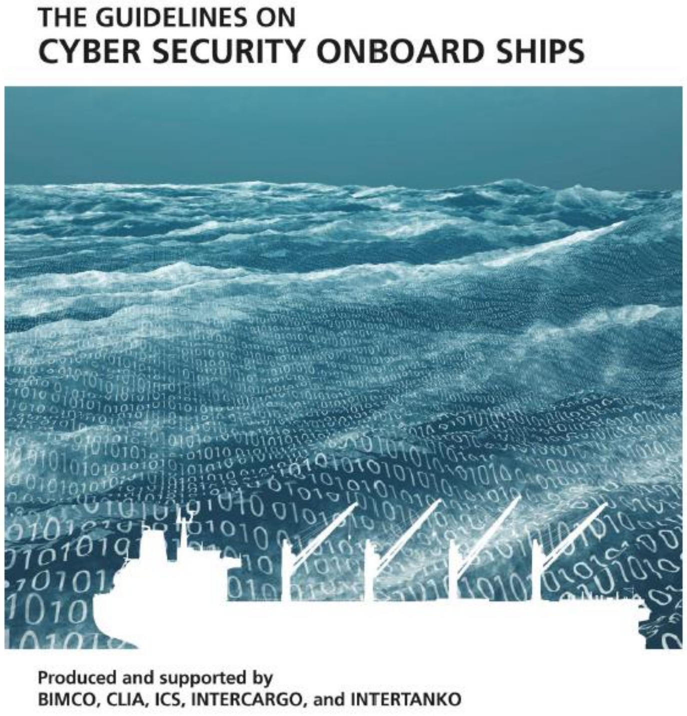
Proteus Risk Solutions

Risk transfer

P&I insurance does not exclude cyber attacks as such, however :

- Exclusion of war and terrorism
- Potential exclusion of foreseeable losses which could have been prevented by the adoption of standard industry practice

International Group Bio-Chemical Risks cover will pick up certain liabilities flowing from cyber attacks up to US$ 30M if terrorism exclusion applies under standard P&I insurance.



THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS

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

UK CHAMBER OF SHIPPING
A MASTER'S GUIDE TO
CYBER SECURITY

Proteus
Risk Solutions