




Understanding the maritime supply chain cyber threat

17<sup>th</sup> May 2018

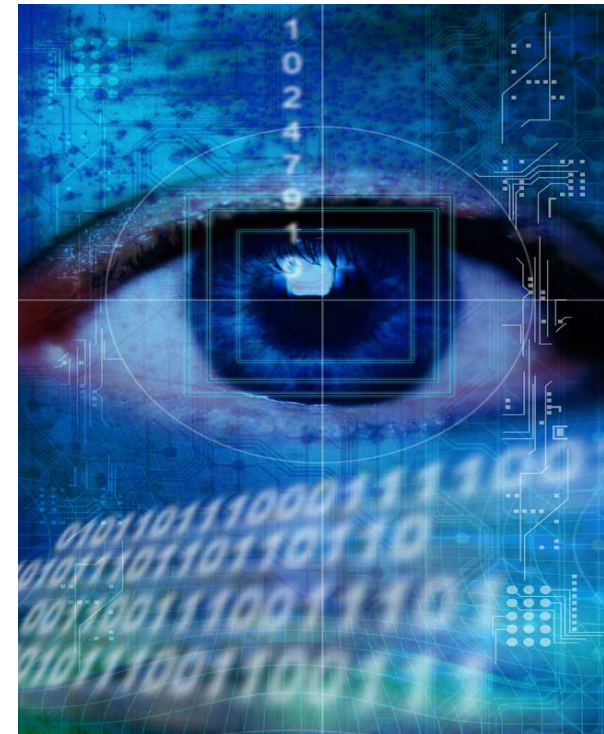
- 
- TT Club
  - Introduction
  - BIMCO/ Fairplay 2016 Survey
  - Industry standards & guidance
  - What are the threats to the supply chain?
  - Notable incidents to date
  - Repercussions
  - Loss Prevention

- 
- MSC 428/98 / NIS Directive / GDPR
  - What is a cyber incident?
  - Who is making the attacks?
  - Are you a target?

- BIMCO / Fairplay Survey in 2016
- 21% of respondents from maritime sector admitted to being victim
- Seaintel in early 2017 revealed that 44% of the top 50 carriers have weak or inadequate cyber security policies and processes

- 
- 1<sup>st</sup> June 2016
  - IMO released new regulation guidelines on cyber risk management
  - 7<sup>th</sup> June 2017
  - Resolution MSC.428(98) requires administrations ‘to take the necessary steps to incorporate cyber threat considerations appropriately through safety management systems.....’ By 1 January 2021
  - EU GDPR effective 25 May 2018
  - NIS Directive

- Illegitimate breach by hackers to access IT systems or data
- In the maritime domain this could result in:
  - Interference with RF domains
  - GNSS & AIS Jamming and spoofing
  - TOS breaches
  - Denial of services
- New malware
- Human error



Date	Victim	Consequence
NOV2017	Clarksons	Perpetrators gained unauthorised access to computer systems, accessing confidential information and threatening to release information unless ransom payment is made. Company share prices decreased by 2.71%
JUN2017	Ships in Novorossiysk, Russia	At least 20 ships in the Black Sea were reporting false data was being transmitted, indicating the ships were 32km inland of their actual position. It is now believed to have been as a result of a GNSS spoofing attack.
JUN2017	A.P. Moller Maersk	NotPetya also known as ExPetr ransomware led to outages on A.P. Moller Maersk computer systems impacting both oil and gas production and port operations. Following the incident, Maersk claimed to have changed its IT systems to prevent similar incidents from occurring in the future. The incident resulted in an estimated USD 300 million of losses
APR2016	South Korea	280 ships were forced to return to port due to problems on their navigation systems. The issue was largely blamed on North Korea however this remains unconfirmed
2012-14	Danish Port Authority	An email virus spread through the port network that was likely initiated through an infected pdf document. The virus spread and successfully reached other Danish government institutions
2012	Australian Customs and Border Protection Service agency	Cargo systems controlled by customs and border protection were hacked in order to determine which shipping containers were suspected by authorities
2011-13	Port of Antwerp	The port had been a victim of an APT attack since 2011 commissioned by a drug cartel. The attack targeted terminal systems which were subsequently compromised by hackers and used to release containers without port authorities becoming aware. Illicit drugs and contraband worth approximately EUR 307 million (USD 365 million), firearms and EUR 1.3 million (USD 1.5 million) were seized when authorities finally became aware
AUG2011	Iranian Shipping Line (IRISL)	The servers were hacked resulting in damage to data relating to rates, loading, delivery and location. Consequently, the location of many cargo containers remained unidentified and an undisclosed amount of financial losses were incurred as a result

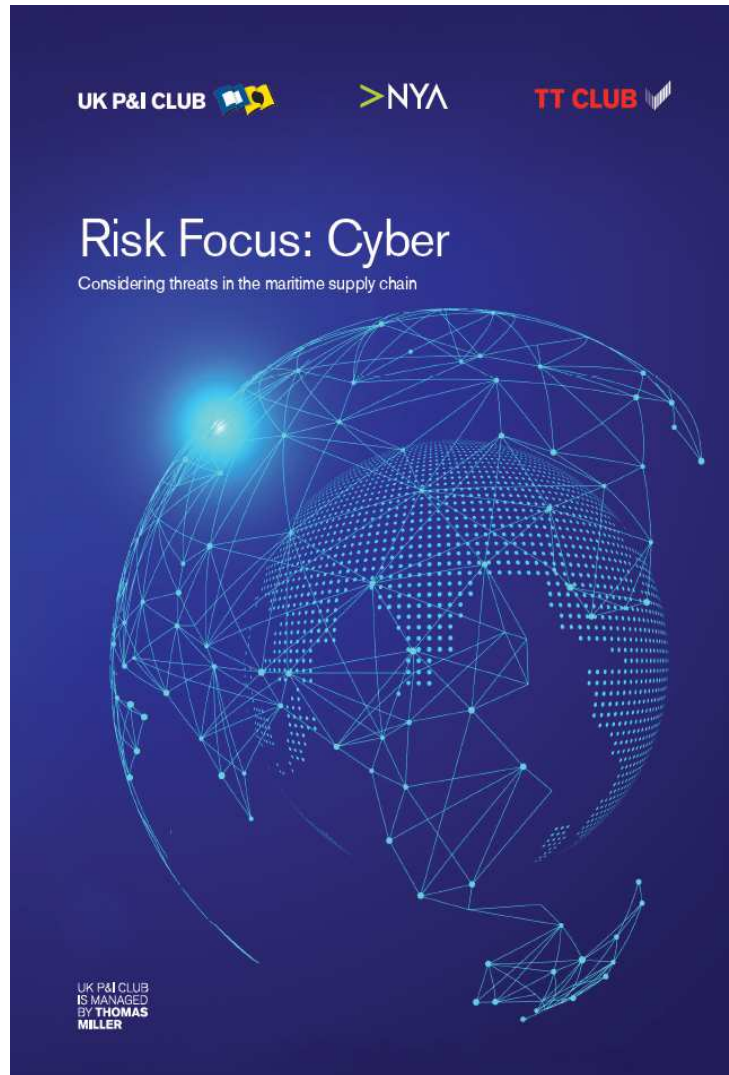
- Financial losses
  - Lost business
  - Remedial costs
  - Investment in new hardware/software
  - Reputational damage
  - Fines





- Implement layers of defence
- Employ network hardening measures
- Segregation & protocol aware filtering techniques
- Ongoing best practice education
- Conduct comprehensive threat assessments
- Vulnerability assessments
- Risk assessment and risk treatment options







Be Prepared

[andrew.huxley@thomasmiller.com](mailto:andrew.huxley@thomasmiller.com)  
[www.ttclub.com](http://www.ttclub.com)