Maritime Cyber Security

Why it's high time to take IT seriously

Ashwin Nair
Cocks Macnish
13 September 2019

Image credit: Maritime-Executive.com

Doops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

   74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-Z2pKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _

Significant features

- Large portion of IT system was disabled
- Digital phones taken offline
- Key-card gates within the Copenhagen HQ and other offices disabled
- Cargo management and booking system was disabled
- Container terminal gates at some ports disabled
- Gantry cranes disabled at some container terminals
- Software to receive and process cargo manifests/information from ships disabled – terminal cargo operations halted

Consequences

- About 10 days before recovery
- Roughly 20% drop in shipping volumes
- Cost of between US$250 to US$300 million (thought to be a conservative estimate)

Observations

- Maersk was not specifically targeted
- Indiscriminate and rapidly spread
- No discernable objective other than to cause maximum damage
- Key vulnerabilities thought to be outdated operating systems which allowed the malware to enter the system and multiply

Outline

A focus on maritime cyber security to the extent it affects ships and their operations

- What is cyber security?
- Broad framework of cyber risk management
- Exploration of the risk landscape
- Regulatory and industry responses
- Potential legal liabilities
- BIMCO allocation of risk
- General response from owners/operators
- Marine insurance
- Final thoughts

Cybersecurity – what does it mean?

- Protecting an organization's cyber environment from unauthorized access, manipulation and disruption
- Cyber environment comprises Information Technologies (IT), Operational Technologies (OT), information and data.
- IT and OT systems intersect on board and are a central part of the cyber environment
- IT – the whole range of technologies for information processing (including hardware, software, communications technologies and other services)
- OT – the software and hardware that detects and causes action/change through monitoring or control of physical devices or processes
- Industry guidelines on *Cyber Security Onboard Ships:*

  "OT systems control the physical world and IT systems manage data"

IT and OT systems

IT	OT
IT network	Programmable Logic Controllers (used for control of physical functions). Eg bilge monitoring, alarm and bilge pump control.
Email system	Supervisory Control and Data Acquisition or Distributed Control System – SCADA or DCS (control systems used for high level process supervision/management). Eg, power management systems, bunkers and ballast water management system.
Administrative matters – crew lists and personal information, accounts	ECDIS, GPS, AIS, weather routing
Planned maintenance monitoring, spares management incl requisitioning	Cargo handling and management system; TRAXENS (MSC – smart containers)
Electronic manuals, certificates and other documents eg B/Ls	Remote support for engines
Passenger manifests, cargo manifests	Propulsion and machinery management, DP

Cyber risk management generally

- According to industry Guidelines, cyber risk management should:
  - Identify the roles and responsibilities of users, key personnel, and management both ashore and on board
  - Identify the systems, assets, data and capabilities, which if disrupted, could pose risks to the ship's operations and safety
  - Implement technical and procedural measures to protect against a cyber incident and ensure continuity of operations (including isolating system and retrieval plan for backups)
  - Implement activities to prepare for and respond to cyber incidents
- Generally, an effective cyber risk mitigation strategy (embedded within a larger organizational strategy for risk management) should encompass
  - perimeter defences around key IT, OT and data infrastructure, including regular software updates and patching
  - 'target hardening' including things like network segmentation, control of removable media like USBs
  - regular education and training
  - detailed contingency planning, including regular backups, reactivation/recovery plans etc

Discernable motivations of cyber attackers

- Theft of money/cargo
- Theft of valuable data – personal, commercial
- Facilitation of illegal activity – smuggling, transmission of illicit material
- Terrorism/acts of war

- Jack Sparrow in a hoodie?
- Let others be the low-hanging fruit

Other examples

- Stolen pin codes for cargo delivery – Port of Antwerp (*Glencore v MSC* [2017] EWCA Civ 365)
- Theft of personal information – Svitzer (Notifiable Data Breach under *Privacy Act 1988* (Cth))
- Use of on board computer as a proxy to transmit/store illicit material
- Payment fraud – intercepted/manipulated invoices (*K v A* [2019] EWHC 1118)
- Spoofing – test by University of Texas in 2013 on a 65-m yacht, 20 ships in the Black Sea in June 2017; STUXNET
- GPS jamming – MODU in Gulf of Mexico 2015 as reported by USCG

Regulatory response - IMO Resolution MSC.428(98)

- Adopted on 16 June 2017
- Recognises the '*urgent need to raise awareness of cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks*'
- Recommend a risk management approach to cyber risks that '*evolves as a natural extension of existing safety and security management practices*'
- '***Encourages***' flag/port state administrations to ensure that cyber risks are dealt with in the ship's SMS and verified in the first DOC verification after 1 January 2021

IMO and industry guidelines

- Guidelines on Maritime Cyber Risk Management (IMO, MSC-FAL.1/Circ.3, 5 July 2017)
- The Guidelines on Cyber Security Onboard Ships (v.3, produced by BIMCO, CLIA, ICS, Intercargo, Intermanager, Intertanko, IUMI, OCIMF, World Shipping Council)
- Classification society guidelines, eg:
  - IACS – 12 Recommendations on Cyber Security
  - DNV-GL: Recommended practice: Cyber security resilience management (DNVGL-RP-0496)
  - ClassNK – Cyber Security Approach – a strategic document, a 'vision statement' for dealing with cyber risk
  - KR – Cyber Security Guidelines

Other industry response

- Cyber security provisions for vessel audits in:
  - OCIMF's TMSA and SIRE programmes
  - Rightship's dry bulk inspections
- These focus on the existence of documented procedures, not the substance and implementation

Flag, port state response

- Reliance on DOC and class notations sufficient?
- Technical know-how – personnel with suitable skills – staffing/cost implications
- Search and rescue, salvage assistance
- Clarity at the enforcement level

Potential legal liabilities

- Non-delivery or misdelivery of cargo - *Glencore v MSC*
- Liability for lost/damaged cargo - breach of Art III r 1 (due diligence to make ship seaworthy) and/or Art III r 2 (properly and carefully carry and care for cargo throughout the voyage)
- Breach of seaworthiness obligations in charterparties (especially time and voyage charters)
- Breach of seaworthiness obligations in marine insurance policies (esp. voyage policies)
- Delay – system failure/breakdown
- Piracy – tracking of vessel/cargo, spoofing/jamming to lead vessel into vulnerable waters
- Inability to recover GA contribution - *CMA CGM Libra* [2019] EWHC 481
- Third party liability – collision, FFO
- Misdirected payment – *K v A*
- PSC non-compliance/detention
- Vessel detention on account of discrepancies in cargo/import/customs declaration (interface between shipper/charterer, carrier and agent)
- Pollution liability
- Criminal penalties for breach of privacy legislation
- Criminal penalties for use of carriage service to transmit illicit material
- Potential OH&S exposure in respect of crew members?

BIMCO Cyber Security Clause 2019

- In this clause the following terms shall mean:
- ‘Cyber security incident’ is the loss or unauthorised destruction, alteration, disclosure of, access to, or control of a Digital Environment.
- ‘Cyber security’ is technologies, processes, procedures and controls that are designed to protect digital environments from cyber security incidents.
- ‘Digital environment’ is information technology systems, operational technology systems, networks, internet-enabled applications or devices and the data contained within such systems.
- (a) Each party shall:
- (i) implement appropriate cyber security measures and systems and otherwise use reasonable endeavours to maintain its cyber security
- (ii) have in place appropriate plans and procedures to allow it to respond efficiently and effectively to a cyber security incident
- (iii) regularly review its cyber security arrangements to verify its application in practice and maintain and keep records evidencing the same.
- (b) Each party shall use reasonable endeavours to ensure that any third party providing services on its behalf in connection with this contract complies with the terms of subclause (a)(i)-(iii).
- (c) If a party becomes aware of a cyber security incident which affects or is likely to affect either party’s cyber security, it shall promptly notify the other party.
- (i) If the cyber security incident is within the digital environment of one of the parties, that party shall:
- - promptly take all steps reasonably necessary to mitigate and/or resolve the cyber security incident
- - as soon as reasonably practicable, but no later than 12 hours after the original notification, provide the other party with details of how it may be contacted and any information it may have which may assist the other party in mitigating and/or preventing any effects of the cyber security incident.
- (ii) Each party shall share with the other party any information that subsequently becomes available to it which may assist the other party in mitigating and/or preventing any effects of the cyber security incident.
- (d) Each party’s liability for a breach or series of breaches of this clause shall never exceed a total of USD _____ (or if left blank, USD 100,000), unless same is proved to have resulted solely from the gross negligence or wilful misconduct of such party.

Key features of BIMCO Cyber Security Clause 2019

- Parties responsible for their own cyber security management
- Parties to notify each other of a cyber security incident when they become aware of it
- Affected party to work promptly, but reasonably, to resolve the incident
- Parties to cooperate to achieve resolution
- Unless otherwise agreed, liability limit for US$100,000 – global limit regardless of the number of breaches that might be identified.
- Limit may be broken if the breach (or breaches) is *solely* the result of 'gross negligence or wilful misconduct'. A high bar.

COCKSMACNISH
BARRISTERS SOLICITORS NOTARY

Some questions arising from the use of the clause in a time or voyage charterparty

- Does not expressly cover payment fraud.
- How do the obligations in sub-clause (a) interact with other obligations, for example, the owner's obligation as to seaworthiness?
- Is the clause intended to co-exist with or override a knock-for-knock allocation of risk – for eg in the Supplytime form?
- Would problems arise if the records concerning maintenance and review of a party's cyber security arrangements comprise sensitive/commercial information? Would a counterparty nevertheless be able to rely on sub-clause (a)(iii) to compel production of such records in the event of a cyber security incident allegedly caused by the first party's breach?

Further questions arising from the use of the clause in a time or voyage charterparty

- What would constitute ‘reasonable endeavours’ in sub-clause (b) to ensure a third party complies with the provisions of the clause – for eg, a chartering broker, or a shipping agent? Would drawing their attention to the clause be sufficient?
- In a voyage charterparty incorporating Hague or Hague/Visby limits through a paramount or general paramount clause, how do the distinct limitation regimes interact should the operative cause of a loss be a breach of the cyber security obligation?
- If a cyber security incident triggers the operation of an off-hire clause, would the owner be able to rely on the cyber security limitation to limit the period of off-hire?
- Does the limitation of liability in fact assist insurers to assess and price an insurable cyber risk?

General response by owners/operators

- Generally aware of the risk, but not particularly concerned
  - An IT issue
  - ‘Won’t happen to us’
  - ‘Why would someone attack us? – We’re not Maersk’

- What explains such attitudes?
  - Out of sight, out of mind
  - Cost pressures (eg pressures on hire/freight, BWM, IMO 2020, ageing fleets)
  - Expectation that insured

Marine insurance aspects of cyber security

- There are no market standard cover for maritime cyber security risks, which might include
  - Property damage
  - Theft
  - Third party liability
  - Regulatory liability (data breach, PSC)
  - Investigation and legal costs
  - BI
  - System recovery

- The risk has not sufficiently 'matured' to be adequately structured and priced
- There are bespoke offerings in the market, but they tend to be narrow, with generally low limits
- Loss/Damage or liability arising from a cyber event tends to be dealt - silent cyber (which must change the complexion of existing risks for insurers)
- The operation of 'malice' in perils only policies – eg hulls or war risk policies.
- CL 380 of the Institute Clauses – also adopted in reinsurance programs
- Push to delete of the clause, but does that solve the problem in perils-only policy? The
- IG Clubs have also given effect to wording similar to CL 380 in their excess war risk cover. Potential difference between intended cover and actual wording.

Final thoughts

COCKSMACNISH

BARRISTERS SOLICITORS NOTARY

Ground Floor, 41 Colin Street
West Perth 6005
Western Australia
T: +61 8 9321 6676
F: +61 8 9481 6518
E: comac@cocksmacnish.com.au
W: www.cocksmacnish.com.au