15 - 18 SEPTEMBER
TORONTO 2019 IUMI

# Cyber Risk : Cargo - new solutions?


**David Grant**
Class Manager, Cargo
CNA / HARDY

**Mike Roderick**
Partner, Clyde & Co.
CLYDE&CO


# Introduction

- Cl. 380 – and its limitations
- Regulatory pressures
- The Joint Cargo Committee's position
- JCC 2019/004 – cyber coverage clause
- Its practical application
- Developments since Toronto
- Conclusions

# Cl.380 : Institute Cyber Attack Exclusion Clause

1.1 Subject only to Clause 1.2 below, 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 for inflicting harm**, of any computer, computer system, computer software programme, malicious code, computer virus or process or any electronic system.

1.2 Where this Clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

# Cl.380 :

- Its use is often resisted as not being “fit for purpose”
- It excludes cover where cyber is simply a trigger for a loss insurers might otherwise be prepared to cover e.g. a hack of a vessel’s navigation system leading to a grounding and cargo damage
- It only excludes cover where there is a cyber attack – but what of a “fat finger” loss (accidental) or a maintenance upgrade that goes wrong (technical)?
- A policy may (a) afford silent cyber cover if Cl.380 is not used or (b) afford silent cyber cover for non-malicious cyber even if Cl.380 is used

# Regulatory issues

- The UK regulatory authorities – the PRA and Lloyd's - have made it clear that it is no longer acceptable to grant silent cyber cover – insurers must either give affirmative cyber cover or exclude it
  - Cf. PRA's Dear CEO letter 30 January 2019
- Insurers need to be able to "*identify, quantify and manage*" their cyber exposures
- Cl.380 may not be sufficient to meet requirements going forward
  - Cf. Lloyd's Market Bulletin Y5258 and 01/10/19 statement - applicable to first party property policies incepting on or after 01/01/20

# The options ...


shutterstock.com

# The JCC's position

- The Joint Cargo Committee consulted widely and felt that the appropriate way forward was a clause giving affirmative cyber cover but with limitations to reflect cargo insurers' risk appetite

- JC2019-004 was introduced for use in July 2019

- It is intended to be used instead of Cl.380

# JC2019-004 : Cyber Coverage Clause

1.1 It shall be a condition of cover under this insurance that the Insured can demonstrate that they have implemented reasonable measures to ensure compliance with the US or UK National Cyber Security Centre recommendations, or equivalent national recommendations, current at inception of this insurance. If the Insured cannot provide evidence that these measures, or such other measures that may be required by Insurers were undertaken, then there shall be no cover under this insurance for losses arising from the use of Software.

# JC2019-004 : Cyber Coverage Clause

1.2 Subject to paragraph 1.1 above, this insurance shall indemnify the Insured for any physical loss or damage, liability or expense, **which would otherwise be covered under this insurance**, which **affects solely the Insured or the Insured's property**, and arises from the use of Software.

For the purpose of this clause, Software shall mean the programs, source codes, scripts, applications and other operating information used to instruct computers to perform one or more task(s).

1.3 Other than whilst the subject matter insured is on board any means of conveyance, this insurance excludes physical loss or damage, liability or expense arising from the use of Software, which leads to a Systemic Loss.

**A Systemic Loss shall mean** physical loss or damage, liability or expense otherwise recoverable under paragraph 1.2 but which affects more than this Insured or this Insured's property.

1.4 Any cover granted by virtue of this clause shall be limited to:

USD [X] each and every loss, or a series of losses arising out of one event and

USD [X] in the annual aggregate

# JC2019-004 : Cyber Coverage Clause

- It was felt that cyber cover should be subject to a due diligence obligation on the insured – by reference to an objective external standard rather than in the abstract
  - https://www.cyber-center.org
  - https://ncsc.gov.uk
- The clause applies whether a loss involves malicious or non-malicious cyber
- Insurers' primary concerns are systemic risk and aggregation
- The perception is that whilst cargo is on board a conveyance in transit there is less of an aggregation risk
- The greater concern is whilst cargo is in port or storage
- The any one event and annual aggregate cyber limits ought to afford insurers protection

# JC2019-004 : practical application

- XYZ Co. Limited is a major fashion retailer
- It has a dedicated distribution warehouse
- Criminals mount a cyber attack disabling the warehouse security alarms and steal the latest fashion lines
- Will JC2019-004 apply?

# JC2019-004 : practical application

- In the lead up to Christmas XYZ Co has to use several third party warehouses to take overflow stock
- The third party warehouses are mixed use
- Those third party warehouses suffer a cyber hack
- XYZ's stock is stolen - along with other stock
- Will JC2019-004 apply?

# JC2019-004 : practical application

- XYZ Limited has a major Christmas shipment on a container vessel
- The vessel's navigation system is subject to a hack
- The vessel grounds leading to cargo damage
- Will JC2019-004 apply?


Photo by chuttersnap on Unsplash.com


shutterstock.com

# Developments since

- 11/11/2019 LMA 5402
- 11/11/2019 LMA 5403
- 18/11/2019 JCC Cyber Exclusion and Write Back Cl.437
- Broker cyber clarification clauses

# LMA 5402

This clause shall be paramount and shall override anything in this insurance inconsistent therewith.

1. In no case shall this insurance cover any loss, damage, liability or expense directly or indirectly caused by, contributed to by or arising from:

   1.1 the failure, error or malfunction of any computer, computer system, computer software programme, code, or process or any other electronic system, or

   1.2 the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.

# LMA 5402

- It is drafted for use across all marine lines – it is not cargo specific
- It excludes cyber loss whether malicious or non-malicious
- It contains wide exclusionary language
- It is drafted as a paramount clause

# LMA 5403

1. Subject only to paragraph 3 below, 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, computer process or any other electronic system.
2. Subject to the conditions, limitations and exclusions of the policy to which this clause attaches, **the indemnity otherwise recoverable hereunder** shall not be prejudiced by the use or operation of any computer, computer system, computer software programme, computer process or any other electronic system, if such use or operation **is not as a means for inflicting harm**.
3. Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, paragraph 1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

# LMA 5403

- It excludes malicious cyber loss, in line with 5402
- It affirms cover for non-malicious cyber provided a loss would otherwise be recoverable under the policy
- There is no aggregation wording
- There is no paramount language
- What of theft?

# JCC - CI 437 Cyber exclusion and write-back

1. [Exclusion as per LMA 5402, Clause 1]

2. In consideration of an additional premium and subject to any deductibles contained within the Policy to which this insurance attaches, paragraph 1 will not apply to physical loss or physical damage, general average or salvage charges covered elsewhere in this insurance where directly caused by or arising from one or more the perils listed below:

   (a) Fire or explosion;

   (b) Vessel or craft being stranded, grounded, sunk or capsized;

   (c) Overturning or derailment of land conveyance;

   (d) Collision or contact of vessel, craft or conveyance with any external object;

   (e) General average sacrifice;

   (f) Jettison;

   (g) Theft;

   Where such peril results from:

   2.1 The failure, error, or malfunction of any computer, computer system, computer software program, code or process or any other electronic system, or

   2.2 The use or operation as a means for inflicting harm of any computer, computer system, computer software program, malicious code, computer virus or process or any other electronic system.

3. [Aggregation]

4. [Additional premium]

# JCC – Cl.437

- It excludes cyber loss whether malicious or non-malicious using wide exclusionary language
- It affords a write back of specific named perils based on Institute Cargo Clauses (C), plus theft, whether due to malicious or non-malicious cyber
- By contrast, the earlier JC2019-004 wording is not restricted to named perils
- Cl.437 contains aggregation wording

# Conclusions

- There are a range of options available
- No clause is mandatory – all are illustrative
- Individual underwriters may have a greater, or lesser, cyber risk appetite to suit client and internal management needs


shutterstock.com

# QUESTION

Is cargo cyber risk a major concern for you?

a) Yes
b) No
c) I Don`t Care

# QUESTION

## How will cargo cyber risk be managed in your market going forward?

a) Will your market use Cl.380?

b) Or use specific wordings defining – or excluding - cover?

c) There are no specific measures in place

shutterstock.com

**Don't let the perfect be the enemy of the GOOD**
**{Voltaire said that}**

⟵ ***{That's this guy}***

15 - 18 SEPTEMBER
TORONTO 2019 IUMI

# Cyber risk : Cargo – new solutions?


**David Grant**
Class Manager, Cargo
CNA / HARDY

**Mike Roderick**
Partner, Clyde & Co.
CLYDE&CO