DEL VISO AVOCATS

PARIS - MARSEILLE - AJACCIO - DOUALA

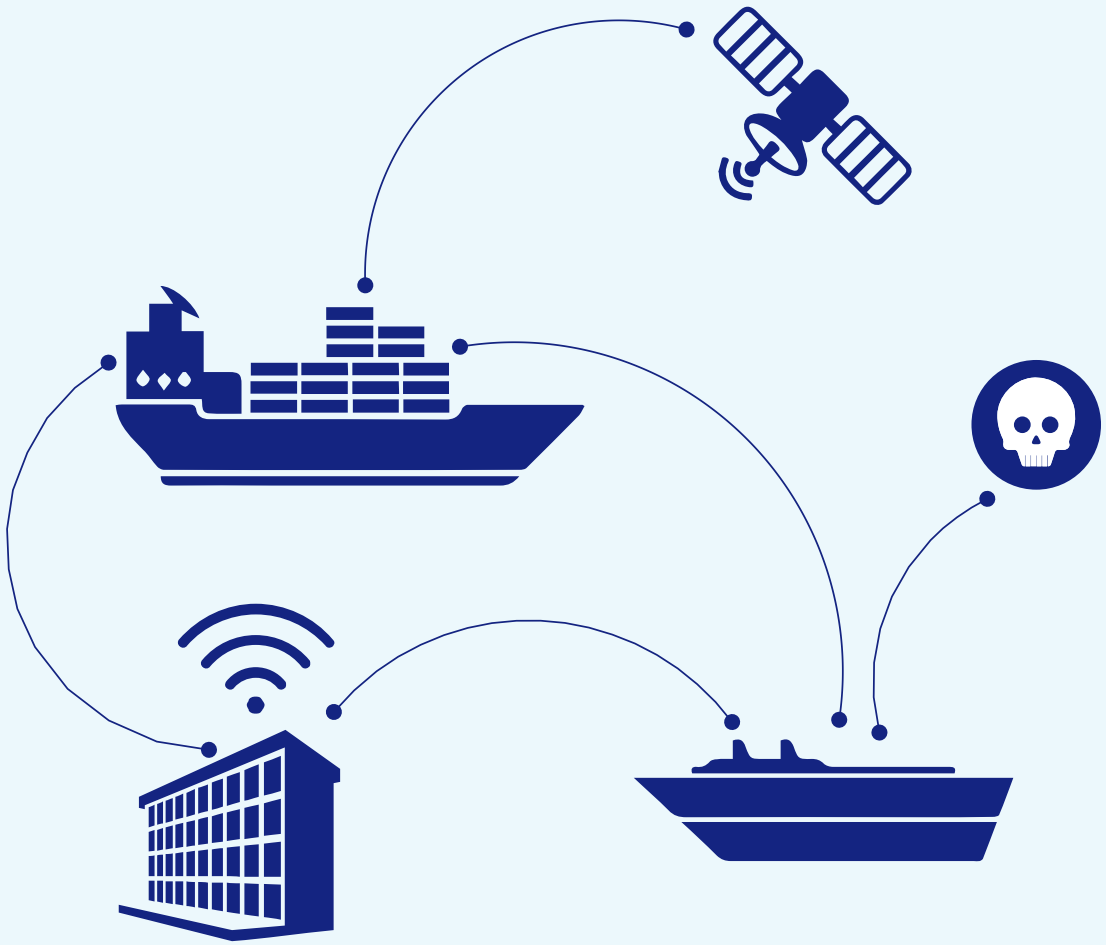
# CYBER EVENTS
# … AND MARINE LIABILITIES

Henri R. NAJJAR | www.delviso-avocats.com | delviso-avocats@avocatline.fr

# WHAT IS
# A CYBER EVENT ?

An occurrence, which actually or potentially results in **adverse consequences to an onboard system, network and computer or the information that they process, store or transmit**, and which may require a response action to mitigate the consequences.

# CYBER EVENTS **IN SHIPPING**



Spoofing of ships

Phishing scam to divert freight/hire

Extract codes and generate documents (eBOLS/manifests)

Hacking and manipulating data to facilitate drug smuggling, intervene on cargo process, disrupt businesses

Misappropriation of goods

Damage to Cargo

Pollution

Personal injury

Damage to Hull

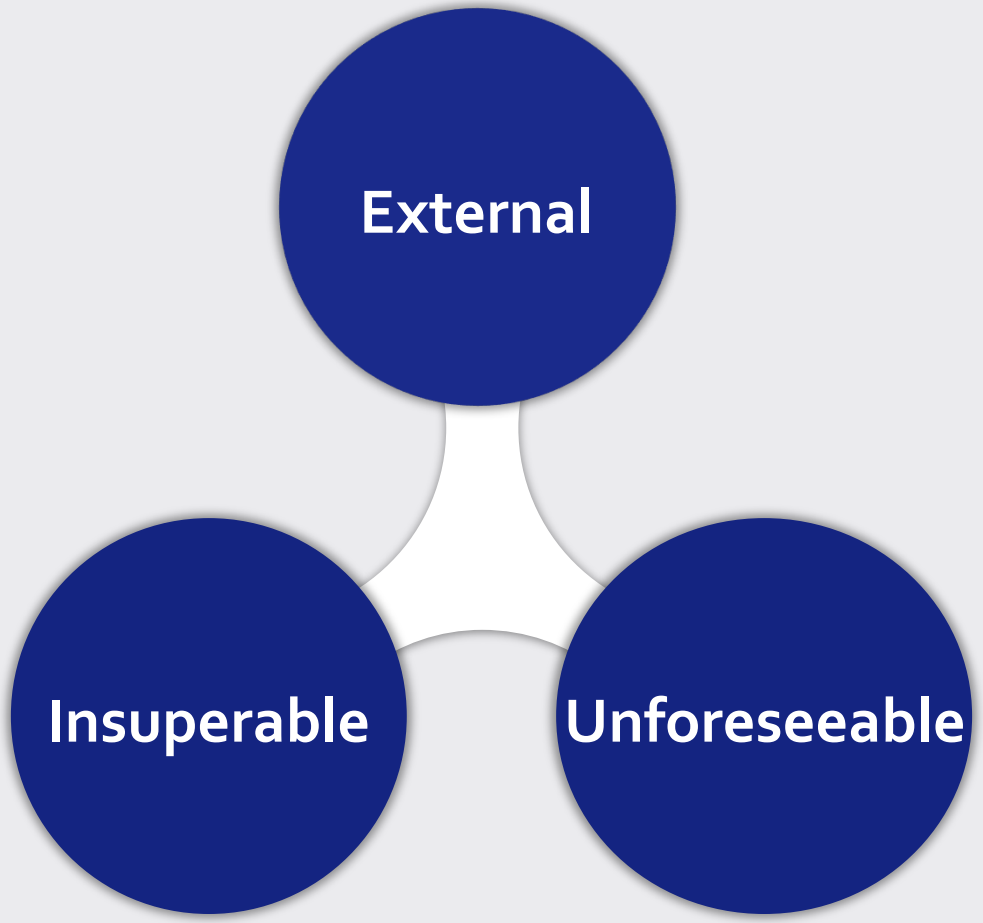
Access to personal data & business secrets

Delay

Financial loss

Damage to reputation

# FORCE MAJEURE




## One has to prove

- Compliance with all applicable laws and regulations
- Execution of all remedy measures

# REGULATIONS AND GUIDELINES

NIS Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union **(NIS)**

EU Data Protection Regulation 2016/679 of 27 April 2016 **(GDPR)**

Guidelines (IMO, Direction des Affaires Maritimes, more recently the UK Ministry of Transport, BIMCO, CLIA ICS, INTERCARGO, INTERTANKO, IUMI, OCIMF)

ISM CODE

## Identify Threats

- Understand the external cyber security threats to the ship
- Understand the internal cyber security threat posed by inappropriate use and lack of awareness

## Identify vulnerabilities

- Develop inventories of onboard systems with direct and indirect communications links
- Understand the consequences of a cyber security threat on these systems
- Understand the capabilities and limitations of existing protection measures


## Respond to cyber security incidents

- Respond to cyber security threats that are realized used the response plan
- Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities

## Assess risk exposure

- Determine the likelihood of vulnerabilities being exploited by external threats
- Determine the likelihood of vulnerabilities being exposed by inappropriate use
- Determine the security and safety impact of any individual or combination of vulnerabilities being exploited

## Establish contingency plans

- Develop a response plan to reduce the impact of threats that are realized on the safety and security of the ship

## Develop protection and detection measures

- Reduce the likelihood of vulnerabilities being exploited through protection measures
- Reduce the potential impact of a vulnerability being exploited

# LEGAL CONSEQUENCES

**Exoneration of liability**
(catch all exception – H/V Rules (art.IV.2(q))

**Suspension of Contract**
(obligations/rights)

**Termination of Contract**
(judicial)

# CONTRACTUAL ARRANGEMENTS

> ***Where there is a failure to make punctual and regular payment of hire due to oversight, negligence, errors or omissions on the part of the charterers or their bankers****, the charterers shall be given by the Owners ..... clear banking days (as recognized at the agreed place of payment) written notice to rectify the failure, and when so rectified within those ..... days following the Owners' notice, the payment shall stand as regular and punctual...*

## ANTI-TECHNICALITY CLAUSE

*After delivery in accordance with Clause 1 hereof the Vessel shall remain on hire until redelivered in accordance with Clause 4, except for the following periods :*

*Inability to Perform Services*

*If the Vessel is unable to comply with the instructions of the Charterers on account of :*

*Any damage,* ***defect, breakdown, deficiency of, or accident to the Vessel's hull, machinery, equipment or repairs or maintenance*** *thereto, including drydocking, excepting those occasions where Clauses 7(b) and 16(b) apply ;*

# OFF-HIRE CLAUSE

*« STRIKES AND FORCE MAJEURE*

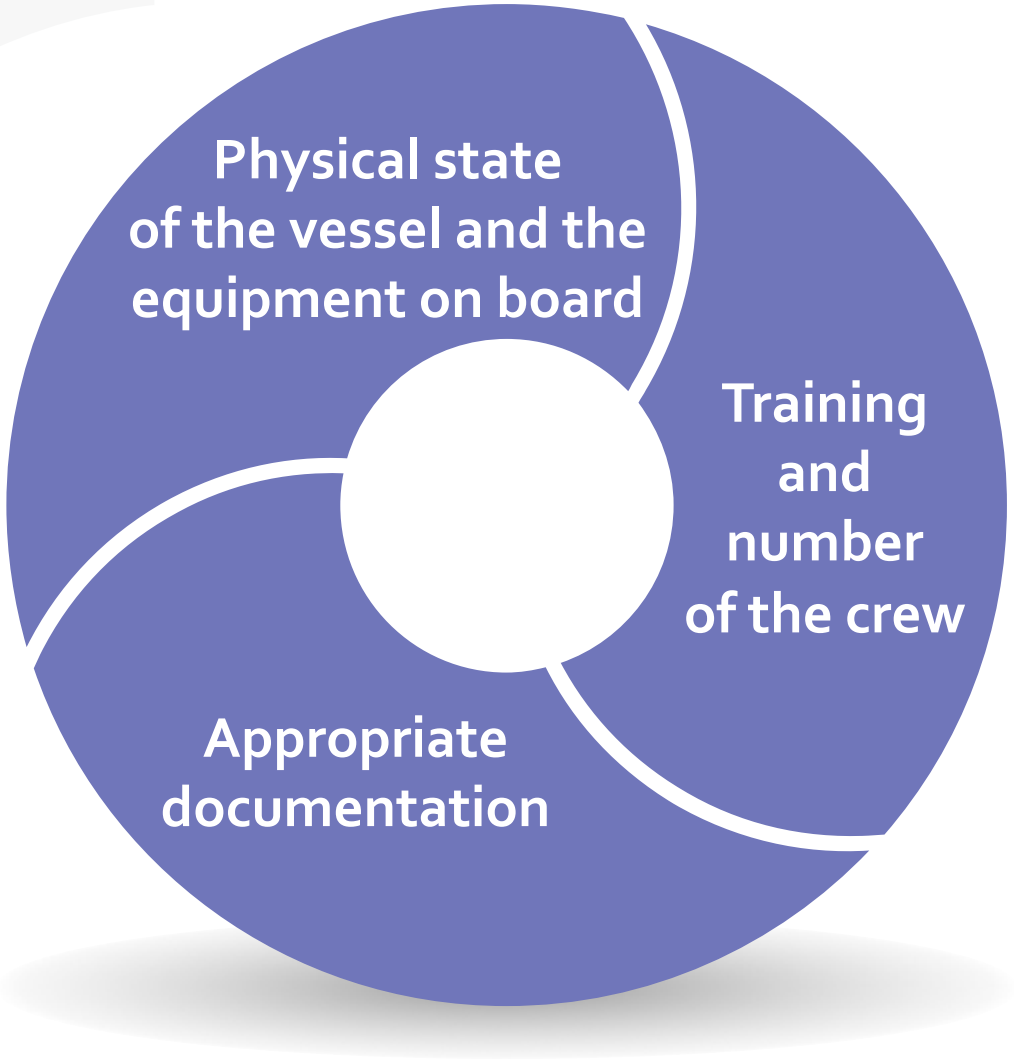
*28.* ***In the event that whilst at or off the loading place or discharging place the loading and/or discharging of the vessel is prevented or delayed by any of the following occurrences*** *: strikes, riots, civil commotions, lockouts of men, accidents and/or breakdowns on railways, stoppages on railway and/or river and/or canal by ice or frost, mechanical breakdowns at mechanical loading plants, government interferences, vessel being inoperative or rendered inoperative due to the terms and conditions of employment of the Officers and Crew,* ***time so lost shall not count as laytime or time on demurrage or detention****. »*

# LAYTIME DEMURRAGE CLAUSE

# SEAWORTHINESS

The ship must be reasonably fit in all respects to encounter the ordinary perils of the seas of the adventure insured.

Failure to protect the vessel against a cyber event could be a failure to exercise due diligence to make the vessel seaworthy.



# SAFE PORTS

A port will not be safe unless, in the relevant period of time, the particular ship can reach it, use it and return from it without, in the absence of some abnormal occurrence being exposed to danger, which cannot be avoided by good navigation and seamanship

If the impact was such that the port had no effective navigational aids then the port would be unsafe.

# WILFUL MISCONDUCT

> Act or omission done with the intent to cause damage or recklessly and with knowledge that damage would probably result

## Must be personal

In practice, extension to :

- Crew management
- Compliance with security & safety regulations

Insufficiency of training of the crew and absence of cyber-management system on board would amount to wilful misconduct

# RECOMMENDATIONS

## 1. Insure your risks

**Hull & Cargo Insurance policies: exclude Cyber risks (French/English markets)**

*"In no case shall this insurance cover loss damage liability or expense directly 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 program, malicious code, computer virus or process or any electronic system."*

**P&I :** Cover as any traditional risk (exclusion: paperless trade/war risks)

**Insurance of fines?** Administrative: Yes – Criminal : No

# CYBER INSURANCE POLICIES

| Advertisement Personal Injury | IP Infringement | Errors & Omissions | Security | Privacy |
|---|---|---|---|---|
| • Libel<br>• Slander<br>• Defamation<br>• Privacy | • Copyright<br>• Trademark<br>• Patent | • Tech Services<br>• Tech Products | • Unauthorized Access<br>• Hacking<br>• Denial of Service<br>• Virus | • Unintentional Disclosure<br>• Breach of Confidentiality |

## 2. Abide by guidelines!

## 3. Instruct audit companies!
incl. classification societies (e.g. ABS Cyber-Safety Program)

## 4. Instruct good lawyers!

DEL VISO AVOCATS

PARIS - MARSEILLE - AJACCIO - DOUALA