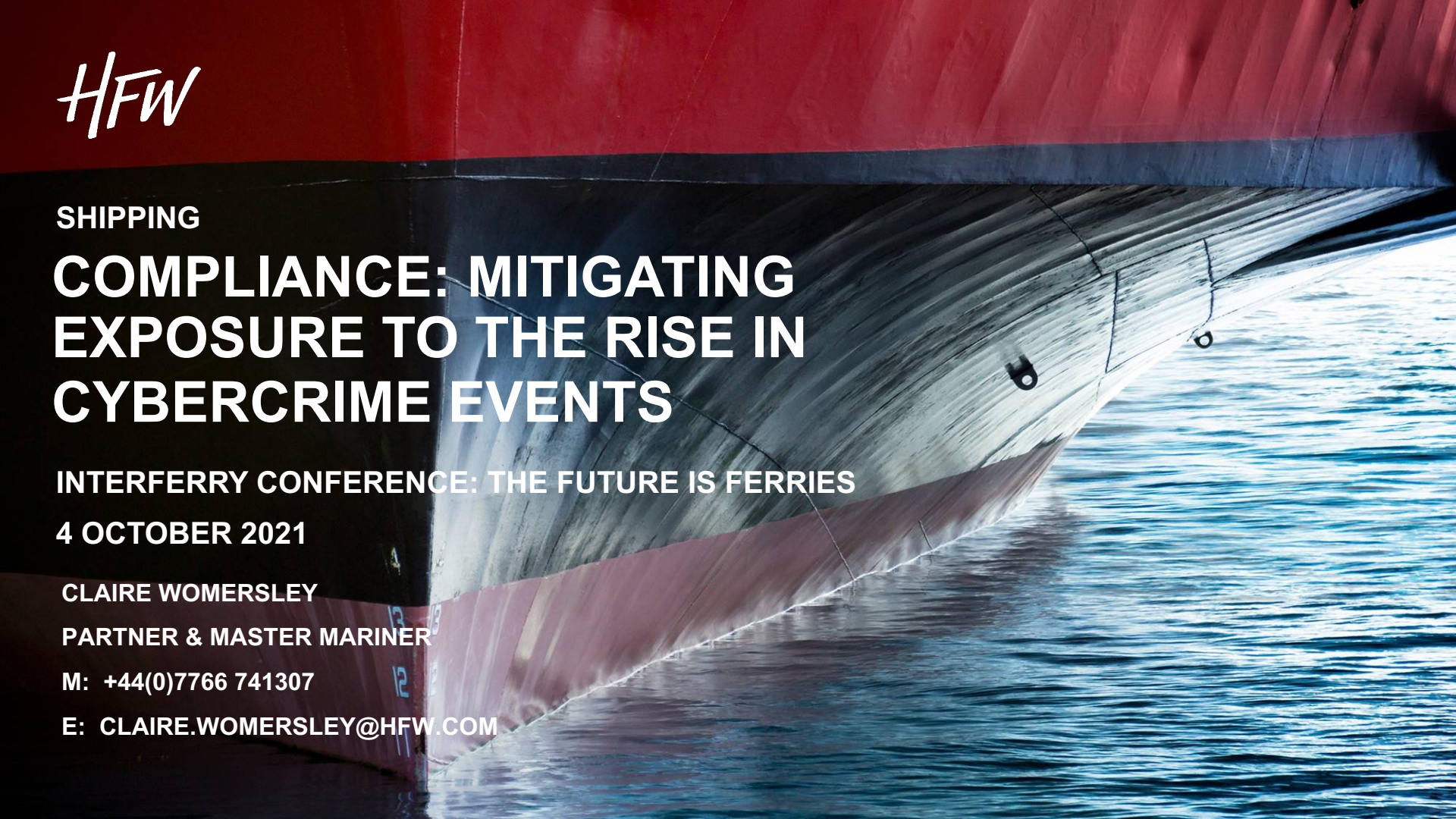


SHIPPING

COMPLIANCE: MITIGATING EXPOSURE TO THE RISE IN CYBERCRIME EVENTS

INTERFERRY CONFERENCE: THE FUTURE IS FERRIES

4 OCTOBER 2021

CLAIRE WOMERSLEY

PARTNER & MASTER MARINER

M: +44(0)7766 741307

E: CLAIRE.WOMERSLEY@HFW.COM

HFW – THE FIRM

HFW is a leading global law firm in the aerospace, commodities, construction, energy, insurance and shipping sectors. The firm has 600 lawyers, including 170 partners, based in 19 offices across the Americas, Europe, the Middle East, Asia and Australia.

Offices worldwide, include:

- **Europe**

London, Paris, Brussels, Geneva, Piraeus

- **Middle East**

Abu Dhabi, Dubai and associations in Saudi Arabia, Kuwait

- **Asia**

Singapore (including FLA HFW AsiaLegal), Shanghai (including association with Wintell & Co), Hong Kong, Jakarta (including association with Rahayu & Partners)

- **Australia**

Melbourne, Sydney, Perth

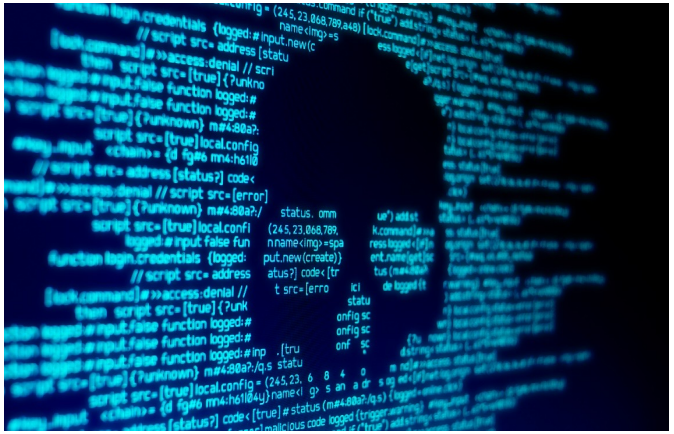
- **Americas**

Houston and São Paulo (including cooperation with Costa, Albino & Lasalvia Advogados) and Rio de Janeiro (including cooperation with Costa, Albino & Lasalvia Advogados)

HFW has a reputation worldwide for excellence and innovation and aims to deliver a practical and commercial response to the legal requirements of businesses throughout the world.

MITIGATING EXPOSURE TO THE RISE IN CYBER CRIME EVENTS

- CYBER THREATS TO THE FERRY INDUSTRY
- CONTROL OF DATA
- CYBER ATTACKS & UNSEAWORTHINESS
- CONTRACTUAL PROVISIONS FOR CYBER ATTACKS
- INSURANCE COVER FOR CYBER ATTACKS



Since Feb 2020: Cyber attacks have increased by 400%

CYBER THREATS TO THE FERRY INDUSTRY
TYPES OF CYBER EVENT

SOCIAL ENGINEERING / MANDATE FRAUD – The doctoring or the giving of **fraudulent payment instructions** so that funds are then redirected from the intended recipient to the fraudster

DENIAL OF SERVICE – The attacker attempts to **make it impossible for a service to be provided** (i.e. preventing access to services, devices or networks). This is often accompanied by a ransom demand

GPS SPOOFING – The attacker will **hack into the GPS** and display incorrect readings / disrupt the ability to obtain readings. This might be to assist cargo theft

CREDENTIAL PHISHING – The attacker will **steal login credentials** to access private information / impersonation of the cyber victim. Used to obtain classified information and usually demand a ransom. This has wide-ranging ramifications with data protection laws as it may give access to passenger's data. (*Misdelivery of cargo (Glencore International AG v MSC Mediterranean Shipping Co [2017] EWCA Civ 365*)

MALWARE – The attacker imports **malicious software** in to the IT infrastructure, blocking access and stealing information. (*Maersk suffered a ransomware cyber attack in 2017 costing over £300 million*)

CYBER THREATS TO THE FERRY INDUSTRY
EFFECT

- **LOSS OF TIME / DELAY CLAIMS**
- **MONEY SPENT RECTIFYING THE ATTACK / COMPENSATION FOR DELAY**
- **PENALTIES FOR GDPR BREACHES**
- **PASSENGER CONFIDENCE / REPUTATIONAL DAMAGE**
- **FREIGHT CLAIMS**
- **CASUALTY (COLLISION, GROUNDING, SALVAGE ETC.)**

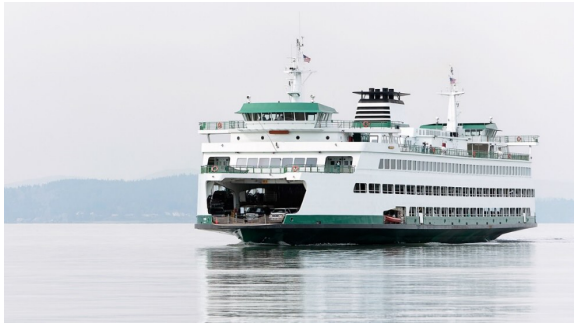
Areas of vulnerability: Agency, Ticketing systems, Freight management, ECDIS, AIS, GPS, ARPA

CYBER ATTACK ON PERSONAL DATA: GENERAL DATA PROTECTION REGULATION

- GDPR is concerned with handling personal data (i.e. any data that either (i) relates to an individual or (ii) can identify an individual)

- This will apply if your company operates within the EU but also if your company operates outside of the EU and, among other things, offers goods or services to persons in the EU

- Fines up to the greater of either £17.5 million or 4% of worldwide group turnover / reputational damage



LEGAL FRAMEWORK

- **Contracts of Carriage import a seaworthiness obligation (chartering / freight)**
- **At common law, the obligation is absolute. If the Hague Visby Rules apply, the duty is reduced to 'exercising due diligence'**
- **The test - would a prudent owner have required that the defect should be made good before sending his ship to sea, had he known of it** (*McFadden* v *Blue Star Line* [1905] 1 KB 967 at [70])
- **Falling below industry standards of cyber protection could also be a "failure to exercise due diligence to make the vessel seaworthy"**

- **No system in place to deal with the ordinary incidents of a voyage** (*The Aconcagua* [2009] EWHC 1880)
- **Ignorance of the crew and failings by the managers** (*The Eurasian Dream* [2002] 1 Lloyd's Rep 719)
- **Failings of proper systems, manning and ship's documents** (*The Silver Constellation*) [2008] EWHC 1904)
- **Faulty systems** (*The Maersk Karachi* [2019] EWHC 1099)
- **Defective passage plan / charts** (*The CMA CGM Libra* [2020] EWCA Civ 293 – Supreme Court Appeal outstanding)

Industry Standards of Cyber Protection

ISM codes require shipowners to protect vessels and personnel from all risks, which includes cyber risks

MSC.428 (98) – in force as of 1 January 2021

- **Cyber risks now need to be addressed in a SMS in line with the objectives / functional requirements of the ISM (IMO (MSC-FAL.1/Circ.3))**
- **Systems and management must be in place to handle cyber risks in the SMS**
- **No later than the first annual verification of the company's Document of Compliance this year**

Non-compulsory guidance:

- BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, WORLD SHIPPING COUNCIL
- ISO/IEC 27001 Standard on Information Security Management Systems)
- US NIST Framework for Improving Critical Infrastructure Cybersecurity
- UK National Cyber Security Centre – Guidance
- Rightship's Inspection and Assessment Reports now contain a cyber security section

Cyber Seaworthiness Clause

"Owner and Charterer agree that the Owner's duty to provide a seaworthy vessel includes cyber risk management and failure to put in place adequate measures is a breach of Owner's obligation to exercise due diligence to make the vessel seaworthy and cargoworthy. Owner shall ensure that adequate measures have been put in place onboard the vessel and ashore that, as a minimum, protect:

a) The operational technology against the consequences of a **Cyber Attack**;
b) Information and communications system and the information contained therein from damage, unauthorised use or modification, or exploration; and
c) Against interception of information when communicating and using the internet."

Cyber off-hire clause

In the event of the loss of time from deficiency of men or stores, fire, breakdown or damages to hull, machinery or equipment, grounding, detention by average accidents to ship or cargo, drydocking for the purpose of examination or painting bottom, **Cyber Event**, or by any other cause preventing the full working of the vessel, the payment of hire shall cease for the time thereby lost.

'Cyber Attack' / 'Cyber Event' need to be clearly defined to avoid any ambiguity as to the triggering event

Standard Force Majeure Clause

"Force Majeure Event" means any event ***beyond the reasonable control of a Party and without the fault or negligence of the Party affected*** which, by the exercise of due diligence, such ***Party is unable to provide against***, such as, but not limited to, acts of God, acts of public enemies, war (whether declared or undeclared), restraint of governments, princes or peoples of any nation, riots, nationwide strikes or lock outs, insurrections, terrorist attacks, civil commotion, floods, fire, restrictions due to quarantines, epidemics, and storms

Beyond the control of the relevant party = party has taken all reasonable steps to avoid its operation or mitigate its results (*Channel Island Ferries Ltd* v *Sealink UK Ltd* [1968] 1 Lloyd's Rep 323)

Effect? Suspends obligations / relieve from liability / terminate the contract

Cyber Attacks as Force Majeure? Expressly include 'Cyber Event'

Transnet, (South Africa's state owned ports) declared FM in June because of a Cyber Event

Institute Cyber Attack Exclusion Clause 380

1.1 Subject to only clause 1.2 below, **in no case shall this insurance cover** loss damage liability or expense directly or indirectly caused by or contributed to be 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 other 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

Discretionary P&I cover - unreasonable conduct?

- Failure to follow industry standards
- Failing to act as a prudent insured
- Did “senior management” have knowledge

THANK YOU

CLAIRE WOMERSLEY

PARTNER & MASTER MARINER

T: +44(0)7766 741307

E: CLAIRE.WOMERSLEY@HFW.COM