A presentation by

HILL DICKINSON

Cybercrime in the shipping industry

An overview of the risks and how they apply to you

Julian Clark
Global Head of Shipping
Hill Dickinson LLP

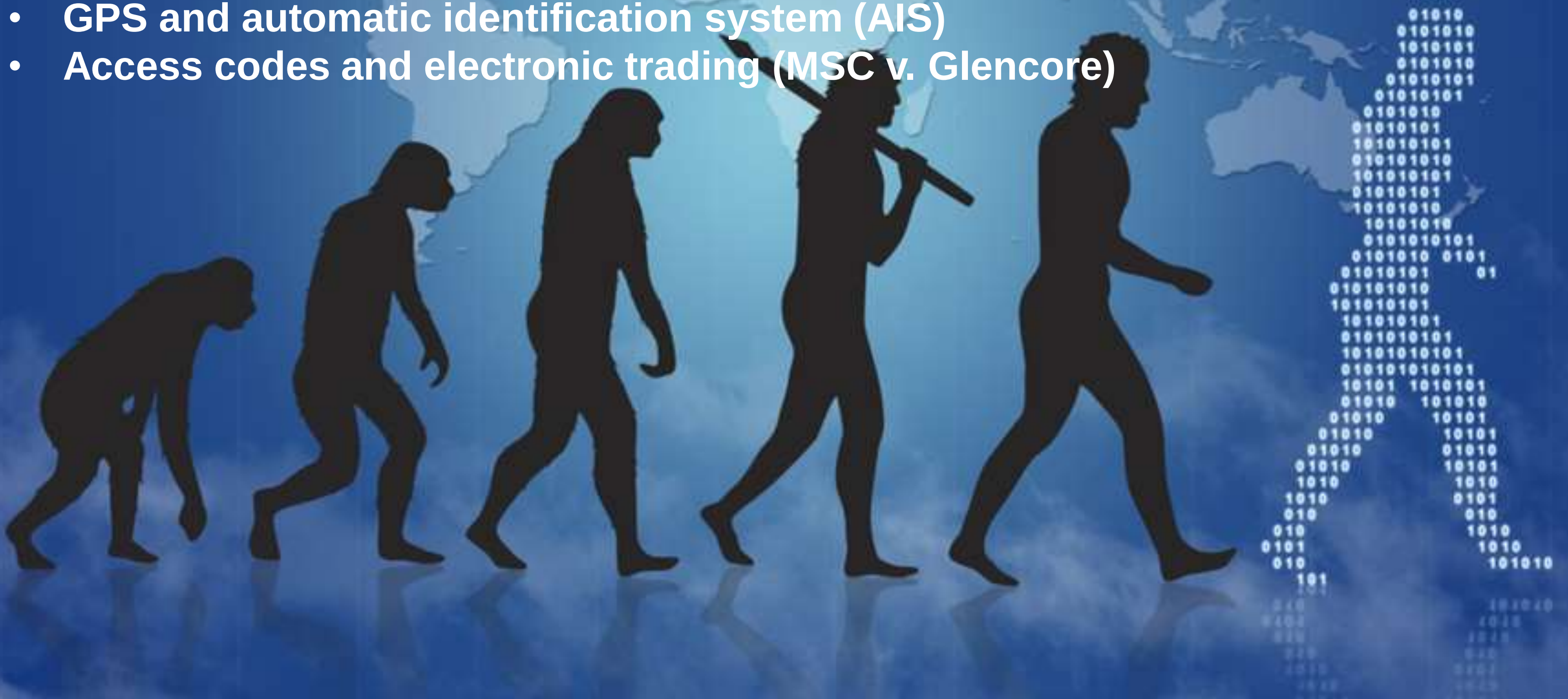
Cybercrime

‘Criminal activity or a crime that involves the internet, a computer system, or computer technology’

Why are the risks getting worse?

Everything is going digital:

- **Telecommunications and informatics (telematics)**
- **Terminal operating systems**
- **Electronic chart display and information system (ECDIS)**
- **Electronic data interchange**
- **GPS and automatic identification system (AIS)**
- **Access codes and electronic trading (MSC v. Glencore)**



HILL DICKINSON

Is cybercrime really a big problem?

- UK government is investing £1.9 billion in cyber-security over five years
- The global cost of cybercrime will reach $2 trillion by 2019
- Of 383 organisations asked who suffered at least one data breach in 2016, the average cost per breach was $4 million
- Last year International Data Group (IDG) detected 38% more cyber-security incidents than the year before
- 48% of data security breaches are caused by acts of malicious intent. Human error or system failure account for the rest

For commercial reasons, many losses and data breaches are not reported

Who is committing cybercrimes?

- **Criminals** – TalkTalk/NHS attack/data breaches
- **Terrorists and government organisations** – Al Qaeda has threatened the use of ‘electronic jihad’
- **Hackers** – groups such as Anonymous and other activists or ‘hacktivists’ e.g. the attack on Sony
- **Employees and ex-employees** – individuals who are either aggrieved or acting under duress
- **Experimenters** – ordinary people with no malicious intent

A sophisticated understanding of technology and computer programming is not necessary to cause significant damage and loss

It is unknown who is funding the organisations responsible for the cyber attacks

HILL DICKINSON

The risks to the shipping industry can be split into two categories

- **Data breaches** – financial and reputational damage. Often more easily quantifiable (the financial aspect) and protectable but nonetheless damaging (the new Nigerian fraud)

- **Physical damage** – causes physical damage and/or bodily injury. Terrifying scope of harm and damage.

Unprepared and unprotected

As technology has evolved the law has not been able to keep pace. Current legal precedent does not always cater to such developments because, as yet, it hasn't needed to.

Let's consider existing law and how it applies to cyber risk ?

- *F.C. Bradley & Sons -v- Federal Steam Navigation* (1926) 24 L1.L.Rep. 446 – definition of seaworthiness - the ship 'must have that degree of fitness which an **ordinary careful and prudent owner** would require his vessel to have at the commencement of her voyage having regard to **all the probable circumstances** of it'
- *Kopitoff -v- Wilson* (1876) 1 QBD 377 – 'fit to meet and undergo the perils of sea and other incidental risks to which of necessity she must be exposed in the course of a voyage'
- *"EURASIAN DREAM"* [2002] 1 Lloyd's Rep. 719 – requires the crew to be adequately trained
- *ISPS/(US) MTSA* 2002 – requires ports to implement security protocols but are not designed with cyber attacks in mind

Case examples

In order to put this into context

Let’s consider some examples.

1.1 Maersk – Petya/Goldeneye

The Petya cyber-attack triggered a large-scale crash of Maersk Group's IT systems across the world

- June 2017
- Began in the Ukraine
- Apparently targeting infrastructure
- Ransomware attack demanding $300 in return for files

The crash affected all business units: container shipping, port and tug boat operations, oil and gas production, drilling services and oil tankers
Maersk's port operator, APM terminals, was also attacked in the USA, Spain, India and the Netherlands. 17 terminals, including two in Rotterdam

HILL DICKINSON

1.2 Maersk – Petya/Goldeneye

- Maersk now forecast a $200 - $300 million hit on third quarter revenue due to lost bookings.
- 70,000 FEU booking lost during the two weeks in took to get the systems back on line.

HILL DICKINSON

2 Antwerp port

- Only 5% of containers shipped into American ports are physically inspected and the percentage of those entering European ports is even lower
- Electronic Release System (ERS)
- In 2011 a gang hired hackers to break into a the Antwerp port's computer systems that controlled the movement and location of containers. Together they attacked the port over a two-year period
- They accessed data that told them the location and security details of containers. They could then smuggle drugs and weapons in the containers and extract them in Antwerp before the legitimate owners of the remaining cargo arrived to empty the containers
- The port did not realise it had been hacked until entire containers went missing

3. MSC Mediterranean Shipping Company S.A. -v- Glencore International AG

- Electronic Release System (ERS)
- 69 shipments of cargo delivered successfully
- 70th shipment; the carrier sent pin codes, against Bills of Lading, to Glencore's agent who attempted to take delivery of the cargo
- 2 of the containers stolen
- MSC held liable for breach of contract, bailment and conversion

1. Chain of causation had not been broken by the cyber attack
2. Risk of theft transferred from receiver to the carrier
3. Previous dealing did not amount to a representation giving rise to an estoppel
4. If you want to utilise new technologies, you must provide for them contractually

4 Somali pirates

- Pirates employed hackers to infiltrate a shipping company’s computer network that managed the shipping routes of different vessels within the fleet
- They used this data to target ships with the most valuable cargo
- The pirates were able to board the ship, target specific containers and leave again.
- Infiltration of Citadels

5 Tilting and disabled oil rigs

- In 2014 in Mexico, a semi submersible rig was shut down because its networks had been accidentally infected with viruses that smart devices had caught from various online sights. It took 19 days to eradicate the malware and put the rig back into production.
- The networks of an oil rig off the coast of Africa were allegedly hacked and, by tampering with the ballast controls, the rig itself was dangerously destabilised.
- This forced the oil rig to shut down completely for a week while the incident was identified and fixed

6 AIS, ECDIS and other systems

- Trend Micro – ability to change AIS date transmitted by a port by the use of a $100 VHF radio and a few components.
- NCC Group – evidence of hacks into ECDIS systems to modify charts
- Ability to fake GPS signals and force vessels to alter course.
- The RAT trap – ALIEN SPY

9. The paradox

Jordan Wylie, JWC International:

- 450 company security officers
- 100 ship security officers
- 25 heads of IT departments

1. What did the shipping company understand about maritime cyber security threats?
2. How would they manage those cyber security maritime threats?

- 67% cyber security officers said that cyber security is not a serious threat to them or their vessels
- 91% ship security officer said they don’t have the training, knowledge or skills to deal with the cyber threats
- 100% heads of IT confirmed that their company did not provide cyber security training for their crews
- 53% said that they have IT systems and/or cyber related policies

The cyber security guidelines – *the guidelines on cyber security onboard ships*

- The original guidelines were published in 2016.
- Leading shipping organisations including BIMCO created these guidelines to help the shipping industry minimise the risk of cyber-attacks on ships
- ‘The guidelines…should help companies take a risk-based approach to cyber security that is specific to their business and the ships they operate.’ - Angus Frew, secretary general of BIMCO
- They are the first of their kind, free to download for members and are regularly updated
- The first edition of the guidelines detailed the minimum requirements that contingency plans should include and are split into four categories:

  1. Understanding the cyber threat
  2. Assessing the risk
  3. Reducing the risk
  4. Developing contingency plans

HILL DICKINSON

9. The cyber security guidelines v2

- The second edition of the guidelines were released in June 2017
    - Insurance issues
    - How to effectively segregate networks
    - Practical advice on managing the ship to shore interface
    - Cyber-security during port calls
- Section on response and recovery from attacks is more substantial and focuses on the isolation a ship experiences if its defences are breached
- Subchapter on insurance issues and coverage after a cyber incident

9. The cyber security guidelines v2

- Companies are recommend to check with their insurer/brokers whether their policies cover claims caused by cyber incidents and/or cyber-attacks
- Aligned with the recommendations given in the International Maritime Organization’s (IOM’s) guidelines on cyber risk management which were adopted in June 2017
- The Annex, which talks about ships’ networks, has been re-written based on the real experiences of shipowners and how they have segregated networks on their ships
- Angus Frew, BIMCO Secretary General and CEO – **“Ignorance is no longer an option, as we are all rapidly realising”**

Insurance?

Lloyds List 31 August 2017

Leading article

- Owners should seek coverage x10 more than what is currently available
- Sundeep Khera head of marine AXA Singapore – “limits need to be $50 - $100 million not what they are at $5 - $10 million)
- Likely that Charterers will start to ask Owners for evidence and scope of their cyber assessment process and incident response procedures.

HILL DICKINSON

9. What do you need to do?

- Look at the guidelines and other information available to you
- Risk assessments should be carried out
- Staff must be trained
- IT systems must be implemented – e.g. firewalls and antivirus
- Issues cannot be left to the IT team to solve
- Silent policies must stop
- Specific insurance
- Check whether you’re covered
- The gap between data loss and physical loss needs to be bridged
- The strength of your company’s own defence systems as well as the systems of any third parties you work with must be considered

10. Thoughts for the future – what an ex SAS commander told me last week to forget about !

HILL DICKINSON

Don’t quote me – seriously don’t quote me

What if pirates did not need to physically board ships in order to take control of them?

‘Autonomous shipping is the future of the maritime industry. As disruptive as the smartphone, the smart ship will revolutionise the landscape of the ship design and operations’ – Mikael Makinen, President Rolls-Royce Marine

Automated transportation technology has already received criticisms for its potential security problems and many believe that automated ships will not be introduced in the next few years, due to concerns over cyber-security

The Question ………………

The Answer …………………………………...

Thank you

Any questions?

A presentation by

HILL DICKINSON

For further information please contact:

Julian Clark
Global Head of Shipping
Hill Dickinson LLP

Direct dial
+44 (0)20 7280 9731

Email
julian.clark@hilldickinson.com

Fax
+44 (0)20 7283 1144

Website
www.hilldickinson.com