

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’



1. Is cybercrime really a big problem?

- The 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

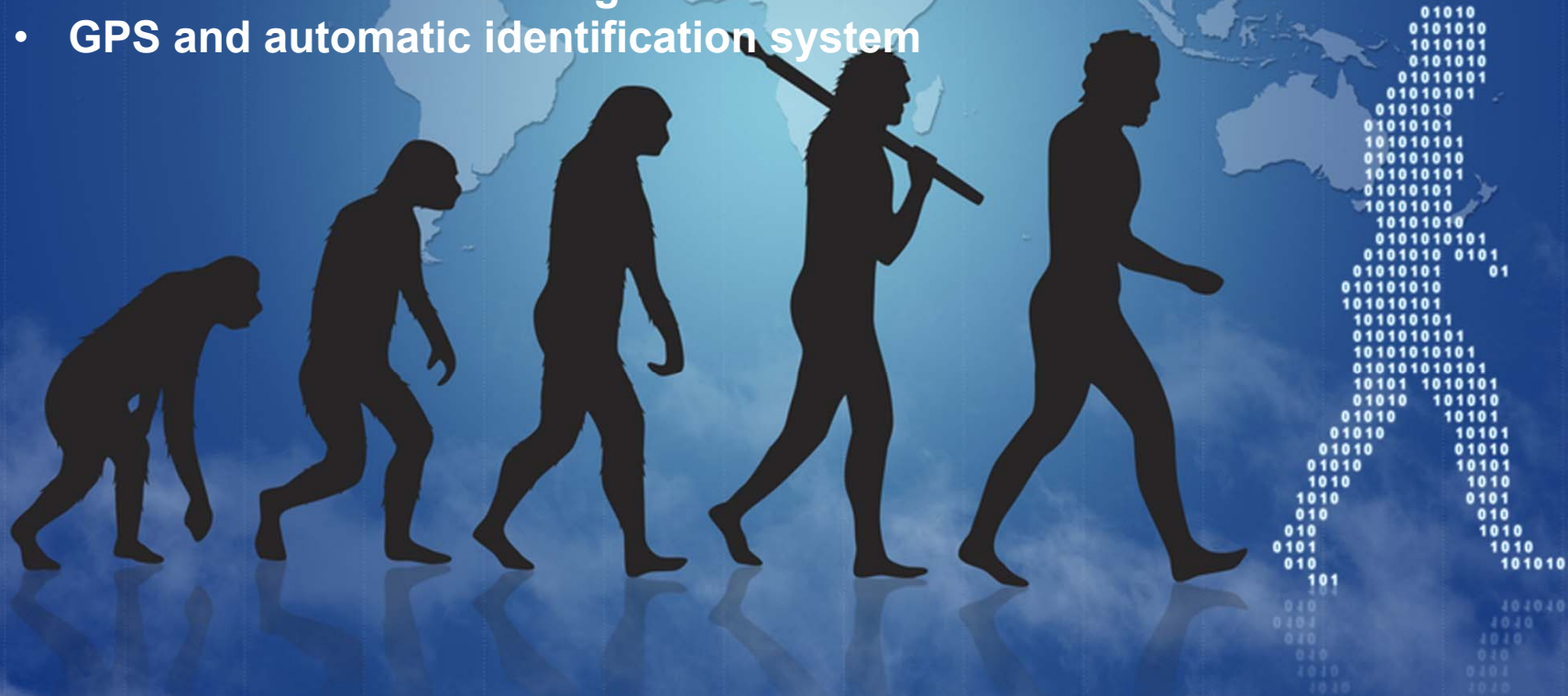
For commercial reasons, many losses and data breaches are not reported



2. Why are the risks getting worse?

Everything is going digital:

- Telecommunications and informatics (telematics)
- Terminal operating systems
- Electronic chart display and information system
- Electronic data interchange
- GPS and automatic identification system

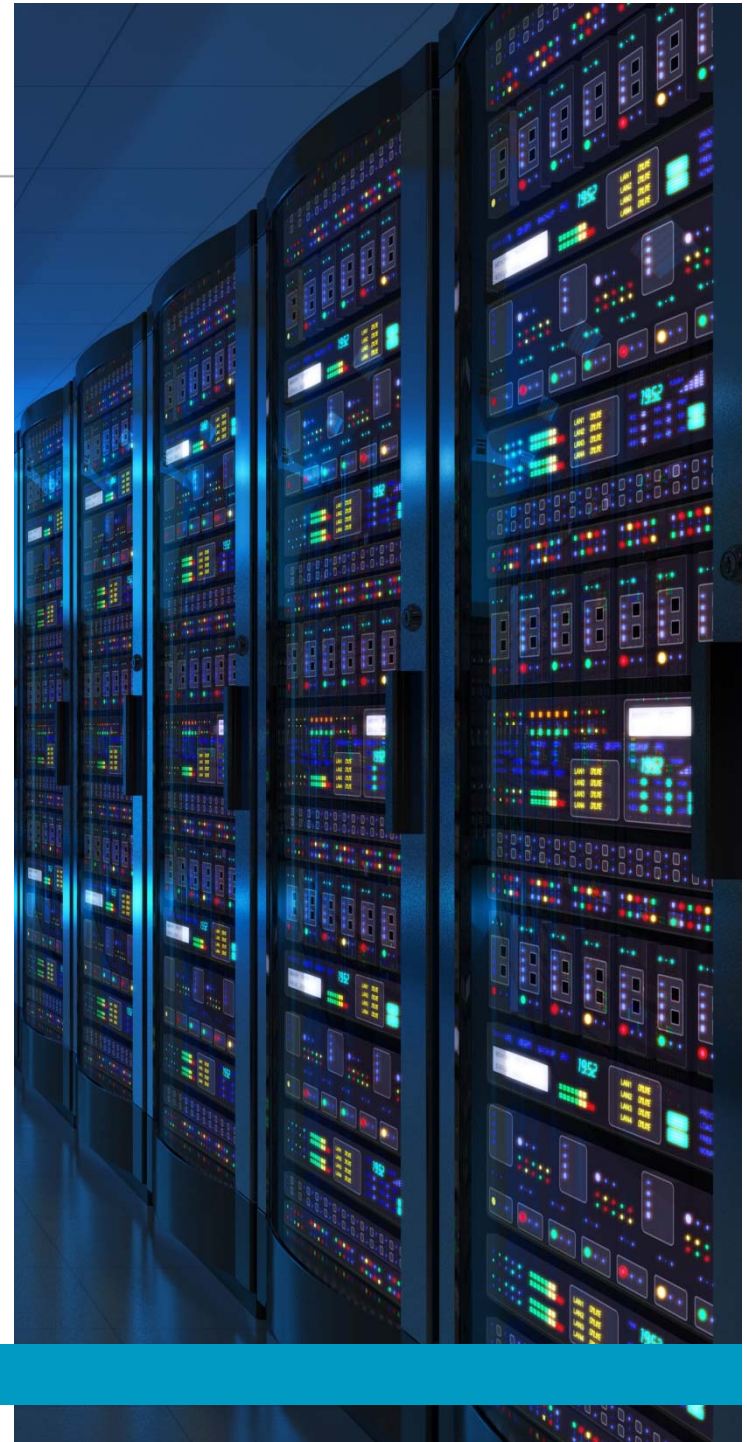


3. Who is committing cybercrimes?

- **Criminals** – TalkTalk data breaches
- **Terrorists and government organisations** – Al Qaeda has threatened the use of ‘electronic jihad’/the USA and Stuxnet
- **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



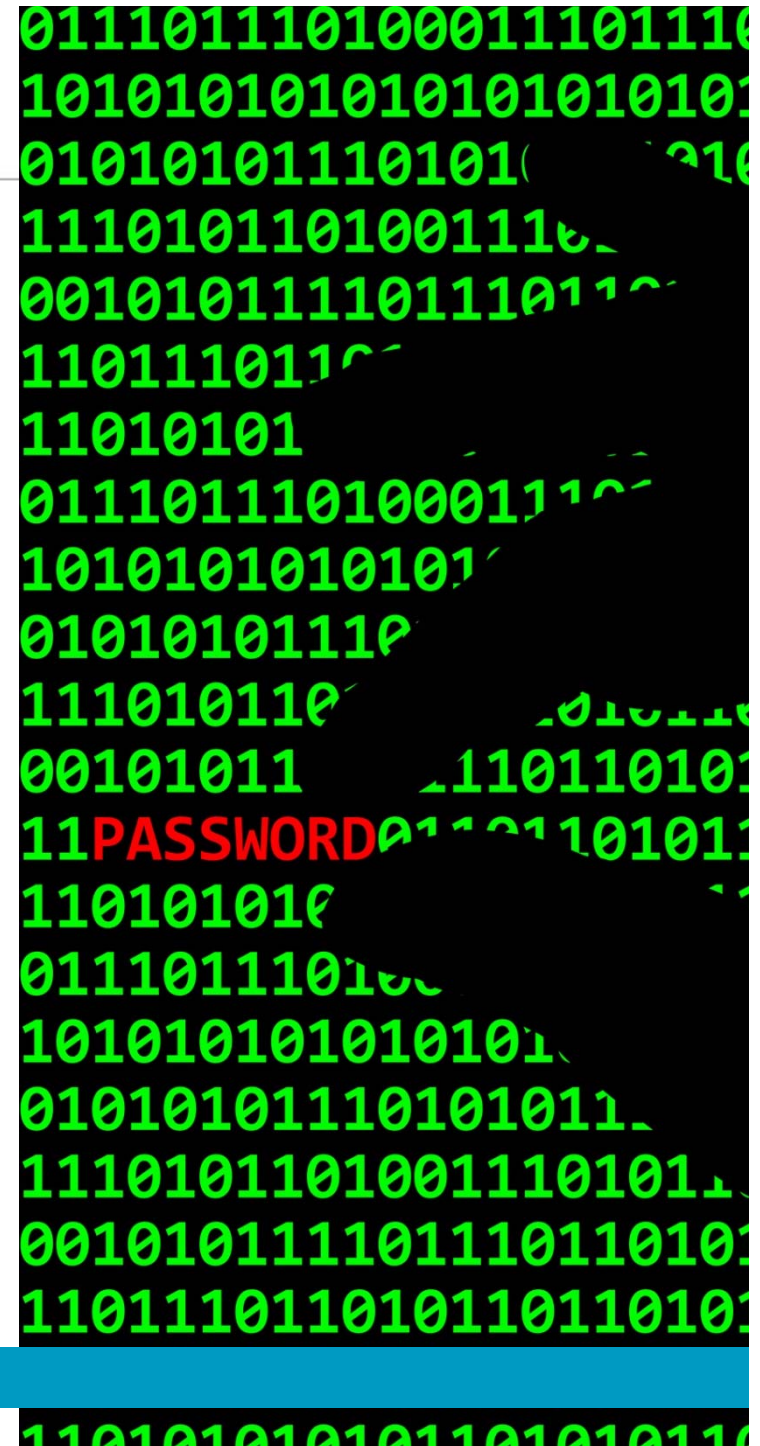
4. What is cybercrime?

There are two main types of cybercrime:

- **Untargeted attacks** – e.g. phishing and ransomware
- **Targeted attacks** – e.g. spear-phishing and subverting the supply chain

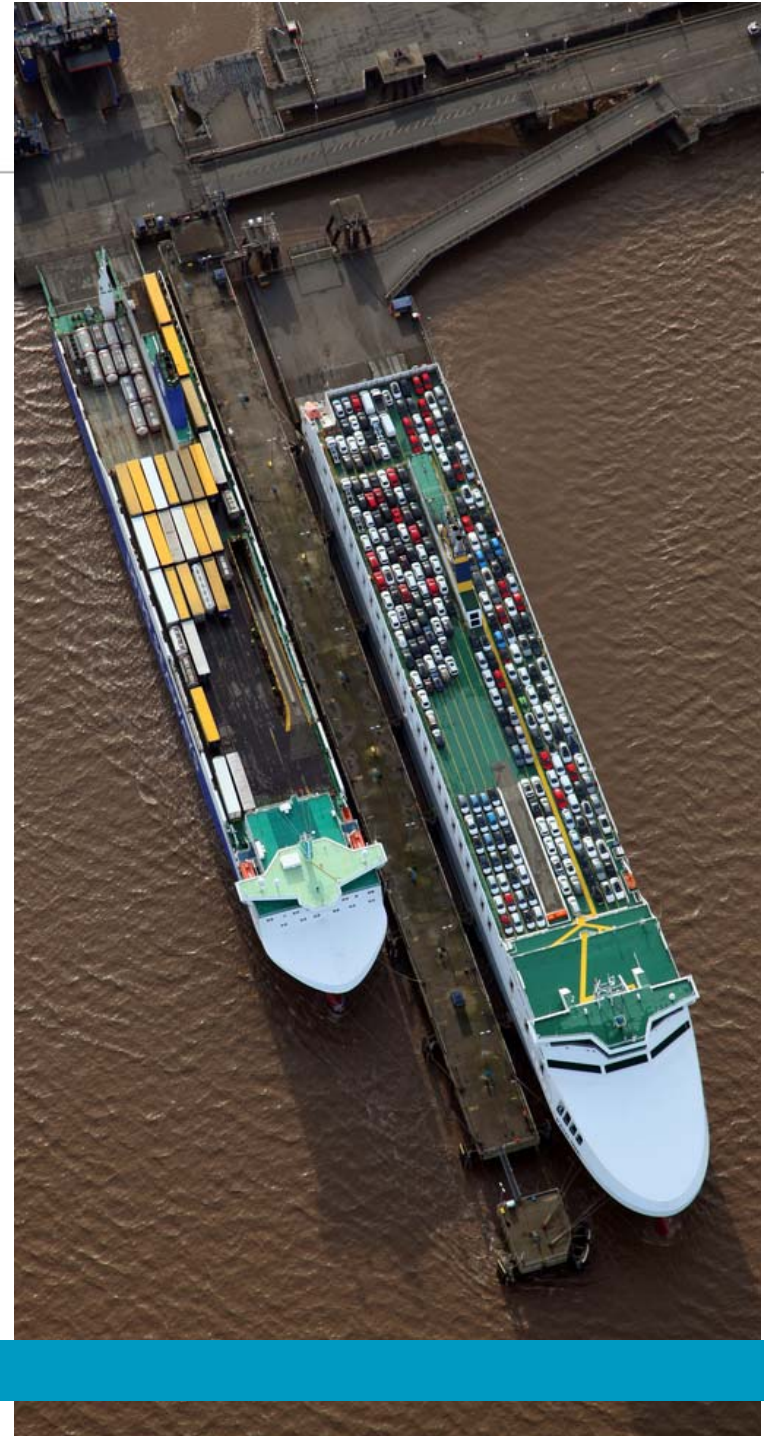
Untargeted attacks tend to be less sophisticated and work under the assumption that, by increasing the number of attacks, the criminals will increase their chances of success

Targeted attacks require more time and research into the criminals' intended victim and the attacks can be extremely sophisticated and occur in multiple stages




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

- **Data breaches** – intangible damage. Often more easily quantifiable and protectable but nonetheless damaging
- **Physical damage** – causes physical damage and/or bodily injury. These types of damage could be covered by other insurances. For example, it could be covered by a separate P&I insurer altogether or dealt with under hull and machinery cover



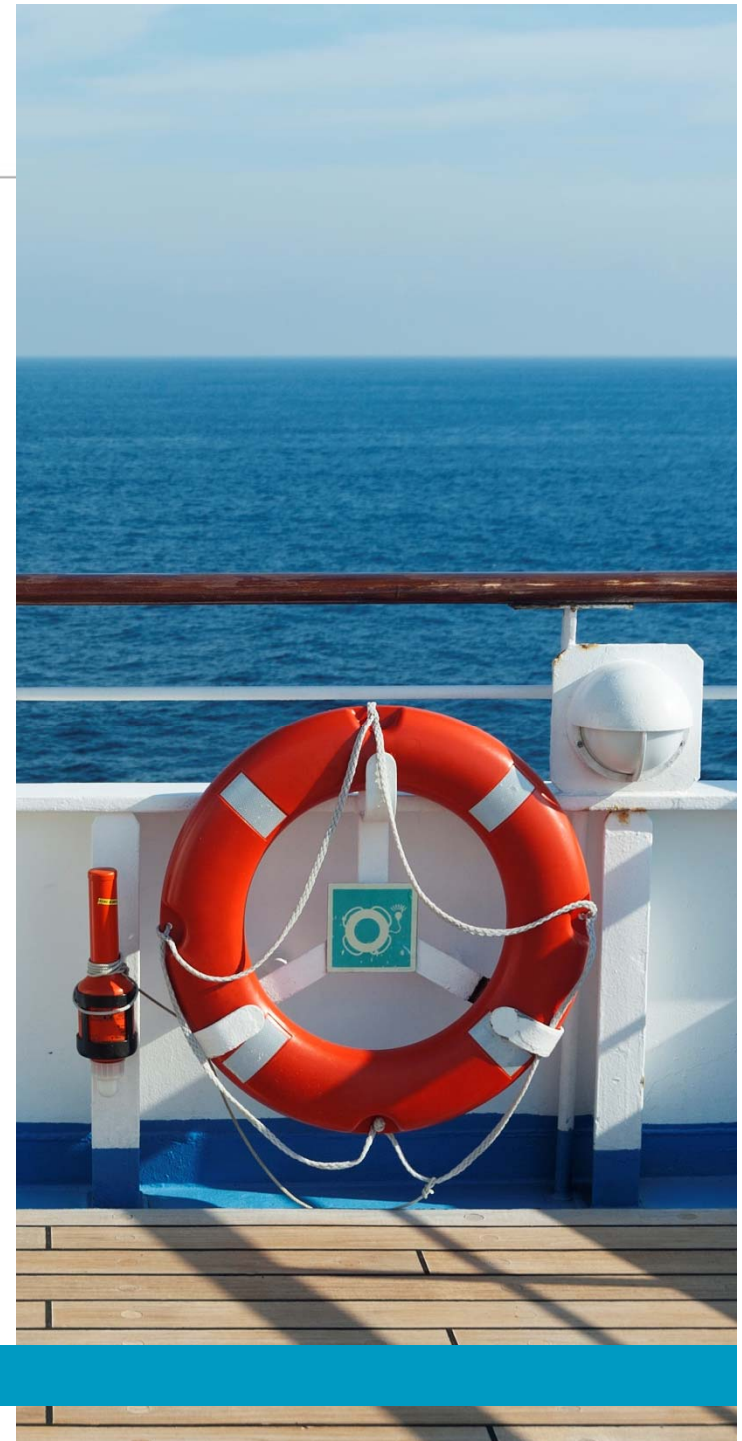
6. Examples of specific risks and their consequences to the shipping industry

Risks are company and organisation specific. The cyber-risk is wherever the weakness is:

- **Spear phishing emails** – requesting payment or goods to be sent to a seemingly familiar and/or legitimate destination
 - **Ports and terminals** – are seen as targets by those looking to disrupt national infrastructure and hostile governments
 - **Data security** – e.g. pirates can board ships already knowing where the most valuable cargo is by obtaining the container references prior to their attack
 - **Insurance** – what types of cyber attack do insurers cover and how far does this cover extend? This uncertainty can leave policy holders as well as the clubs unaware or uncertain of the extent of their coverage or liability
- 

6. Examples of specific risks and their consequences to the shipping industry

- **Duplicate bills of lading** – there is an ever increasing push towards electronic bills of lading (e.g. Bolero, e-title and essDocs) this generates further potential to create duplicate bills and international trade contracts
- **Changing cargo manifestos** – by changing the cargo manifestos remotely, cybercriminals are able to hide substances in containers or disguise them as something else
- **Consequences** – e.g. damage to reputation, delay and monetary consequences




7. Unprepared and unprotected

Due to the historical nature of the shipping industry, as technology has evolved, it has not been able to keep pace. Current legal precedents does not always cater to these developments because, as yet, they haven't needed to. These cases have not yet been taken to court and ruled upon.

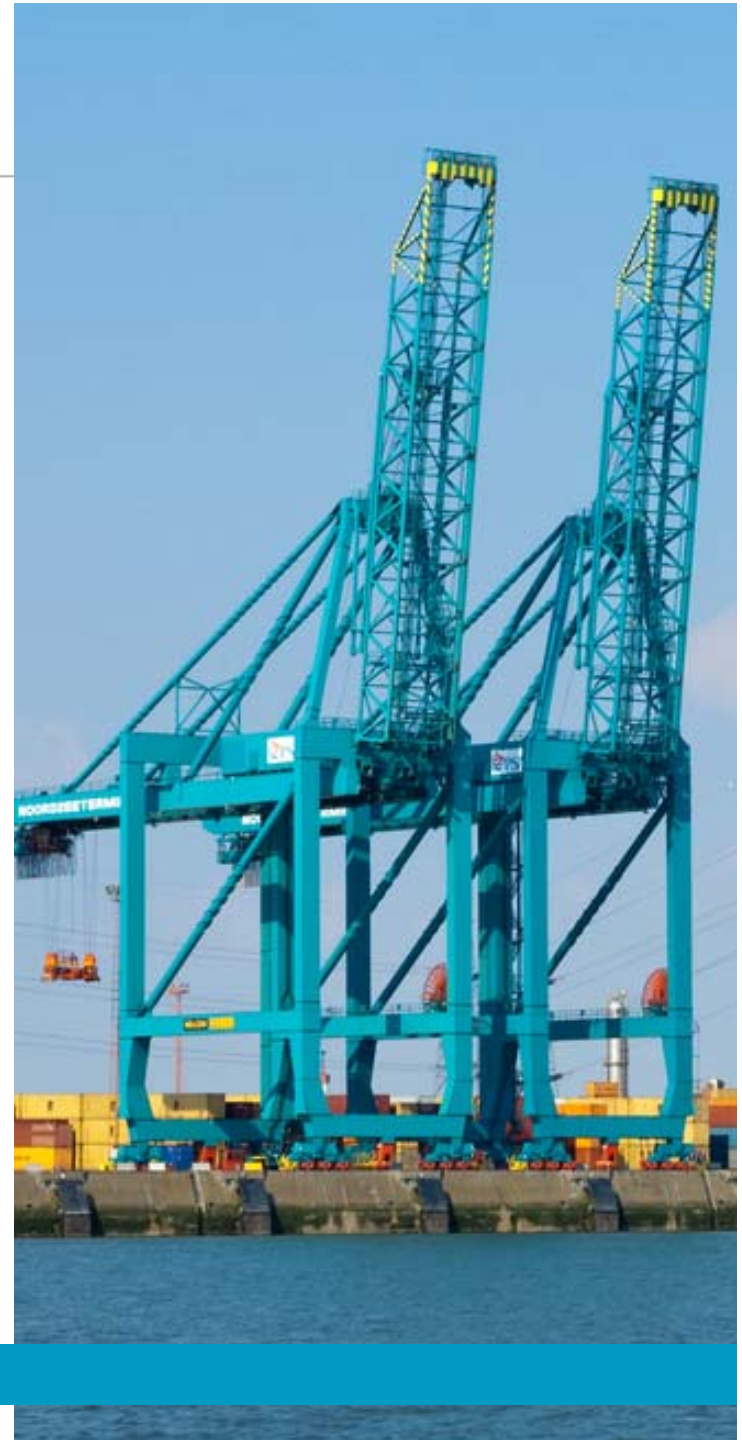
- *F.C. Bradley & Sons -v- Federal Steam Navigation* (1926) 24 L1.L.Rep. 446 – definition of seaworthiness - the ship 'must have that degree of fitness which an **ordinary careful and prudent owner** would require his vessel to have at the commencement of her voyage having regard to **all the probable 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

The industry is in need of more certainty and current definitions and terminology should be reconsidered to determine how and where the changes in technology fit into them



8. Antwerp port

- Only 5% of containers shipped into American ports are physically inspected and the percentage of those entering European ports is even lower
- A gang hired hackers to break into the Antwerp port's computer systems that controlled the movement and location of containers. Together they attacked the port over a two-year period starting in 2011
- 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



8. 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 before the company was able to stop them
- A number of mistakes were made by the pirates, such as failing to use proxy servers

But what about next time?

The marine industry is a pirate's playground



8. Tilting and disabled oil rigs

- Oil rigs and their networks are notoriously poorly protected
- In Mexico, an entire oil rig was shut down because its networks had been accidentally infected with viruses that smart devices had caught from various online sights
- 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 tilted over to one side
- This tilting forced the oil rig to shut down completely for a week while the incident was identified and fixed
- Very little is known about these stories – under-reporting for commercial reasons?




8. AlienSpy RAT

The Consolidated Marine Management's (CMM's) cyber security department has identified a serious and malicious risk to the shipping industry

'AlienSpy is very powerful in the hands of an attacker' – Lampis Alevizos, CMM cyber security expert

The AlienSpy RAT can collect system information for duplication and display this on the attacker's controller dashboard.

Key features supported by the RAT:

- A file system, process and registry explorer with the ability to view and modify
 - Ability to run console commands
 - Key logging to capture user inputs
 - Ability to download and execute secondary payloads
 - Credential theft from various browser stores
 - Ability to spy on victim through screenshots, webcam, microphone
 - Remote desktop ability with infected clients
 - Ability to mine various types of digital currency, such as Bitcoin
- 

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



9. The Cyber Security Guidelines

- Leading shipping organisations including BIMCO have launched 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 will be regularly updated.
- The guidelines detail the minimum requirements that contingency plans should include and are split into 4 categories:
 1. Understanding the cyber threat
 2. Assessing the risk
 3. Reducing the Risk
 4. Developing contingency plans

9. What are other organisations doing?

Thome Group

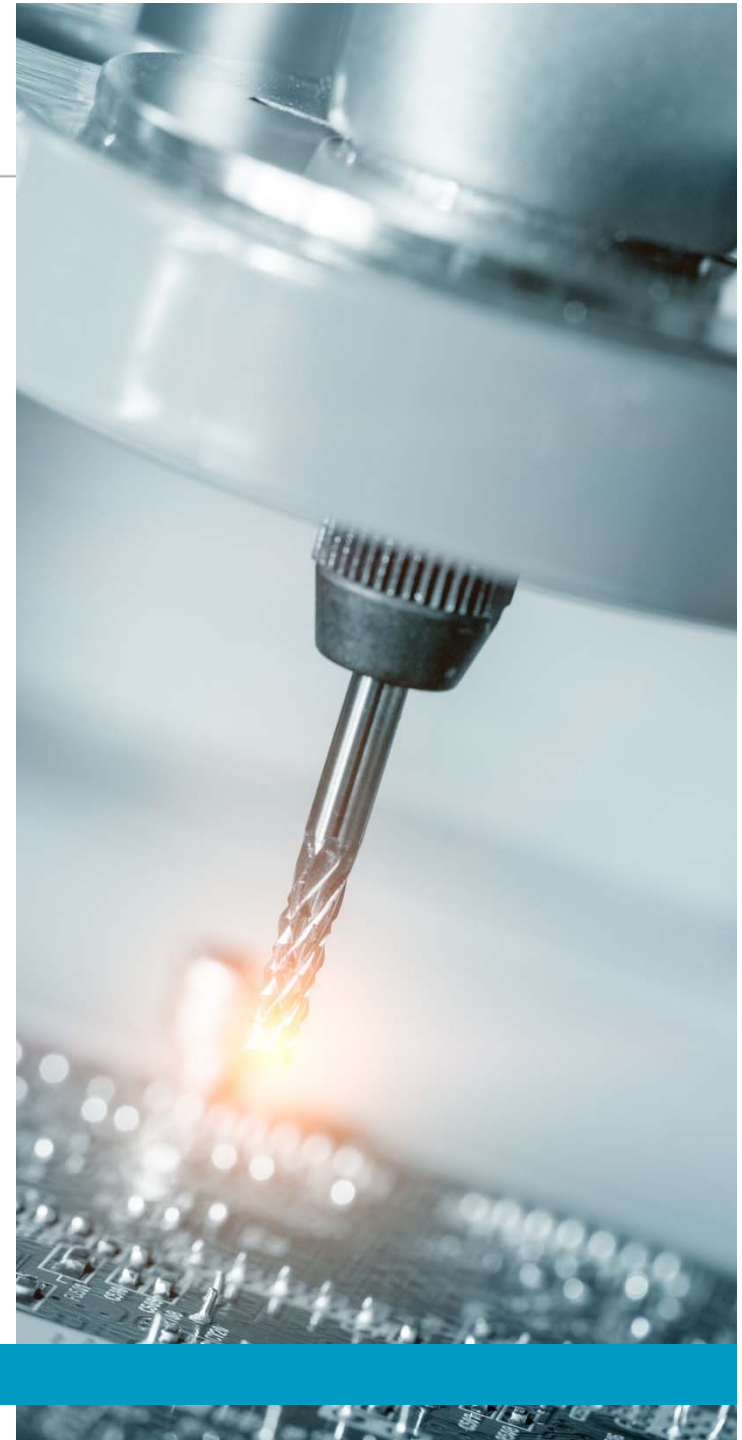
- Has invested in a layered approach to network security
- It is reviewing its cyber security protocols and educating crew to prevent cyber attacks and reduce their impact
- They have noticed that a large proportion of cyber threats are passed on via email and have therefore focused their defences on this area

ABS

- Have formed a dedicated cyber safety team to try and help manage the cybercrime threat
 - They have also launched ABS CyberSafety, a series of five industry guides, again to help manage the cybercrime threat and mitigate and losses
 - Chief Technology officer, Howard Fireman said that ABS has an obligation to keep pace with the disruptive threat posed by cybercrime and that ABS publications aim to bring clarity to the industry
- 

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
- These issues cannot be left to the IT team to solve
- Silent policies must stop
- Specific insurance
- 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



HILL DICKINSON

Thank you

Any questions?



For further information please contact:

Julian Clark
Global Head of Shipping
Hill Dickinson LLP

Direct dial

+44 (0)20 7280 9363

Email

julian.clark@hildickinson.com

Fax

+44 (0)20 7283 1144

Website

www.hildickinson.com



A presentation by
HILL DICKINSON

