Cyber Marine:
Risks & Loss Scenarios

...

John Walker – Chief Surveyor, Braemar SA

Jonathan Spencer – Average Adjuster, The Spencer Company

Outline

SECTION 1 INTRODUCTION

A) What is Cyber Threat

B) Information, Technology, People

C) The Good … Safer, More Efficient Connected Vessels

SECTION 2 The Bad & Ugly… What has happened?

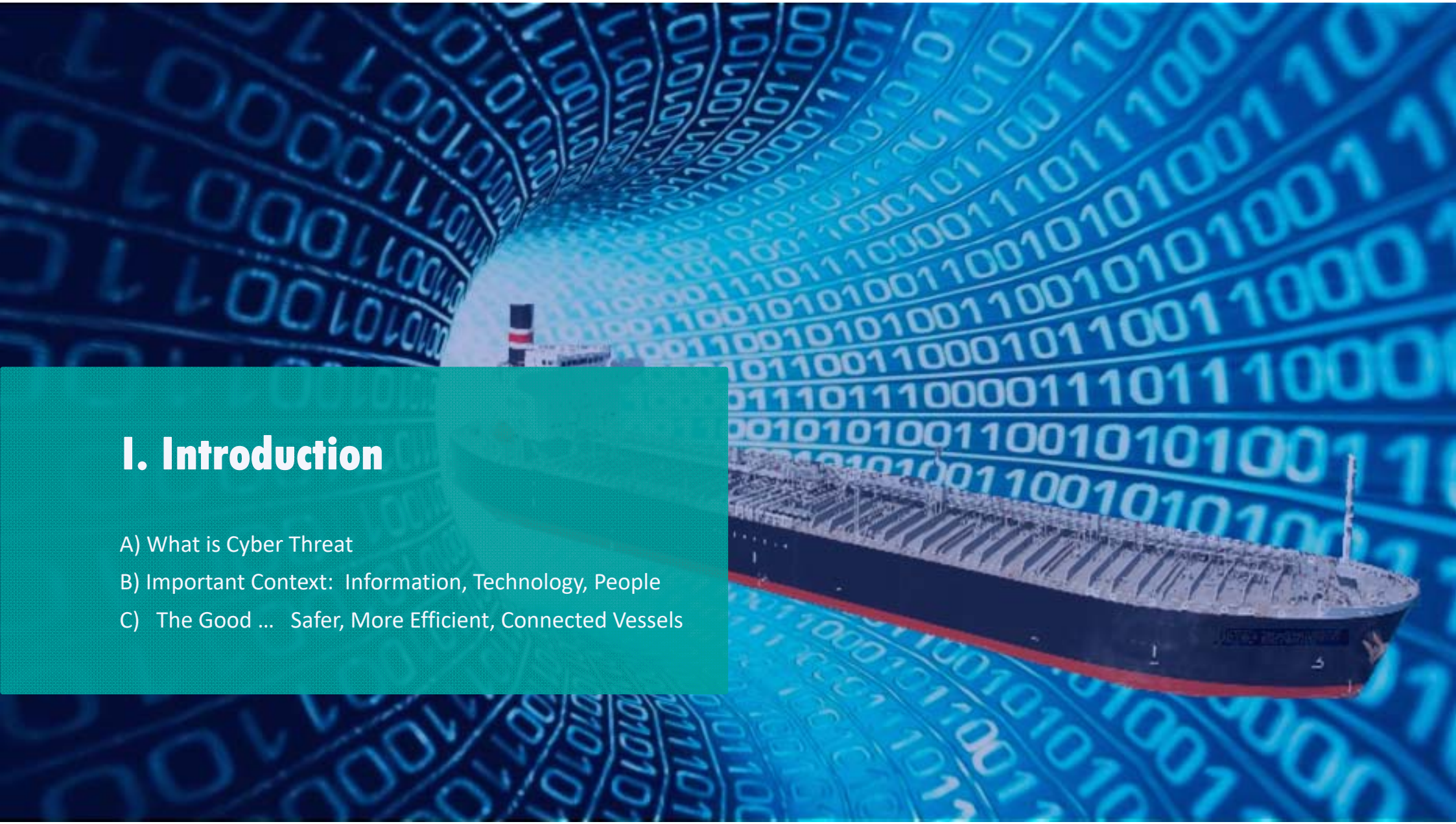
Review of major incidents: Who What & Why

SECTION 3 An Average Adjuster's viewpoint

SECTION 4 A Surveyor's perspective

SECTION 5 Realistic Loss Scenarios (Interactive)

Q & A



I. Introduction

A) What is Cyber Threat

B) Important Context: Information, Technology, People

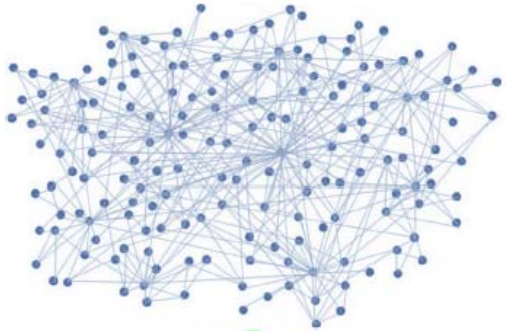
C) The Good … Safer, More Efficient, Connected Vessels

A) What is a Cyber Risk Threat?

CYBER RISK – covers the risks of doing business, including managing and controlling data, in a digital or "cyber" environment

Factors influencing the threat landscape

- The Cloud
- Shadow IT
- Mobile and flexible working
- Bring your own devices
- Internet of things



Sources

- Human/ system error
- Cyber crime
- Lone hackers
- State-backed

Tools and expertise needed to exploit vulnerabilities are becoming more widely available

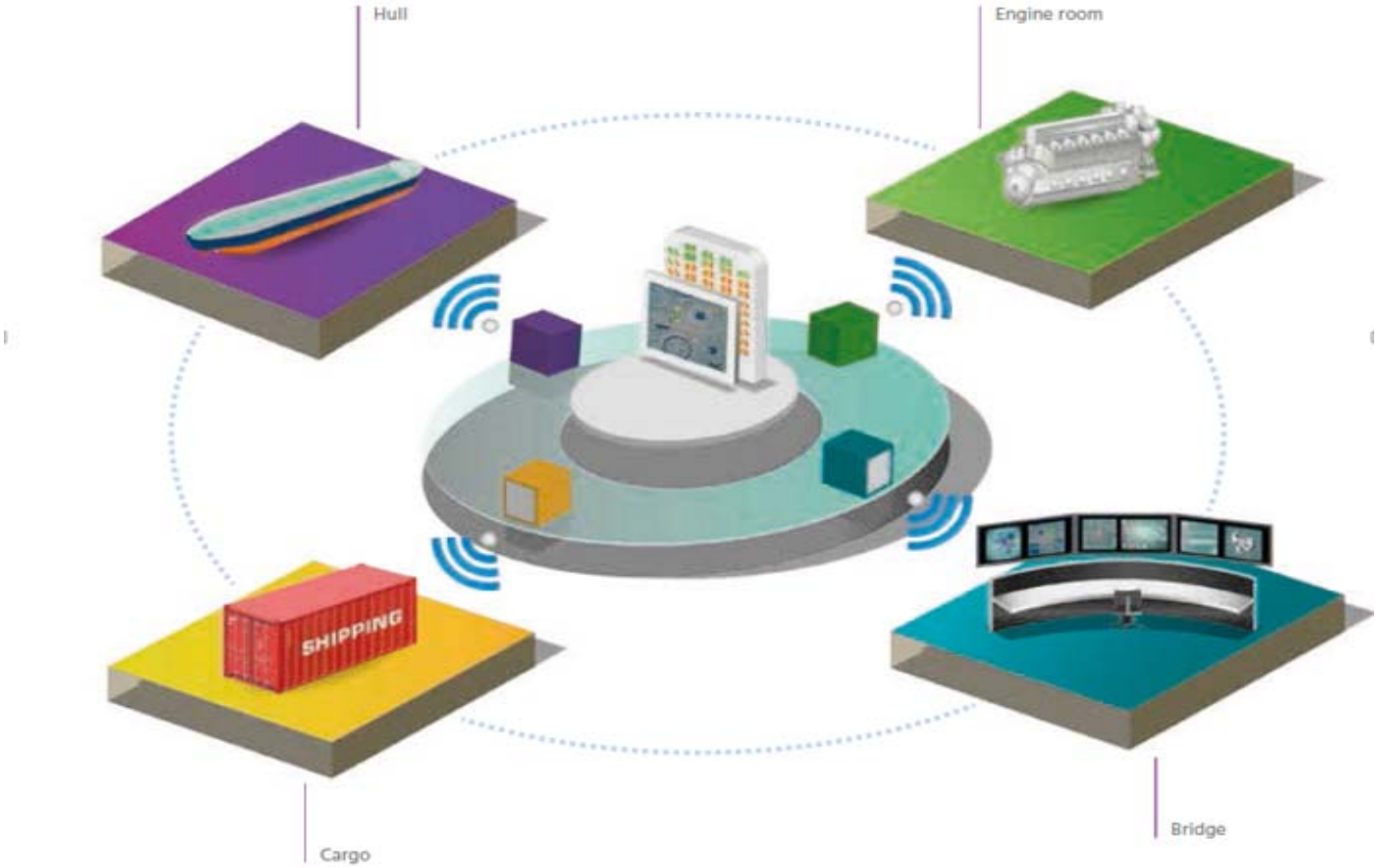
Ability to carry out an attack is therefore simpler

1st Question

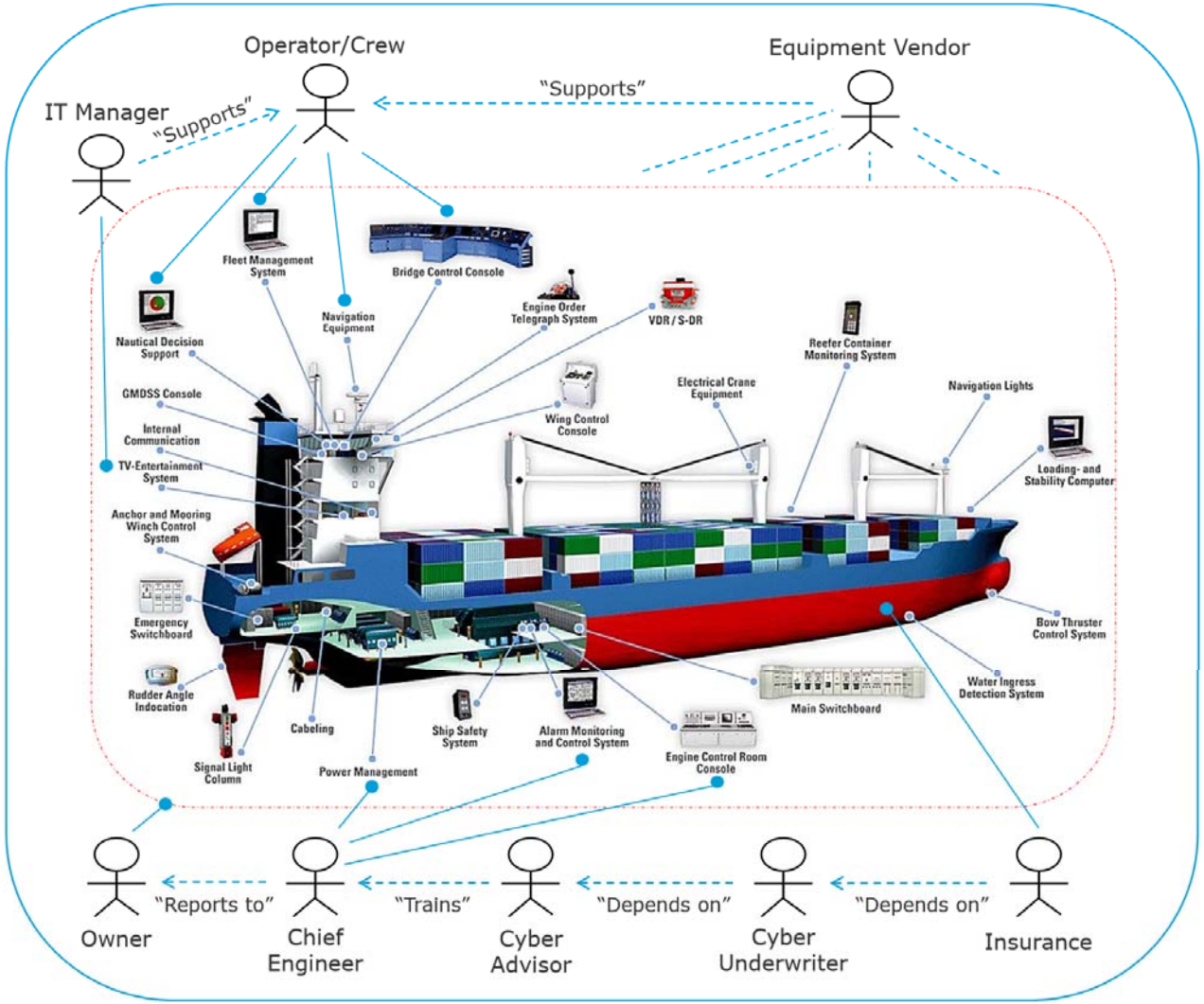
Have you have had to deal with a cyber attack?

1. Never had so much as a virus on my home computer
2. Have some experience but was easily resolved with no significant loss of data or costs.
3. Major incident resulting in a loss

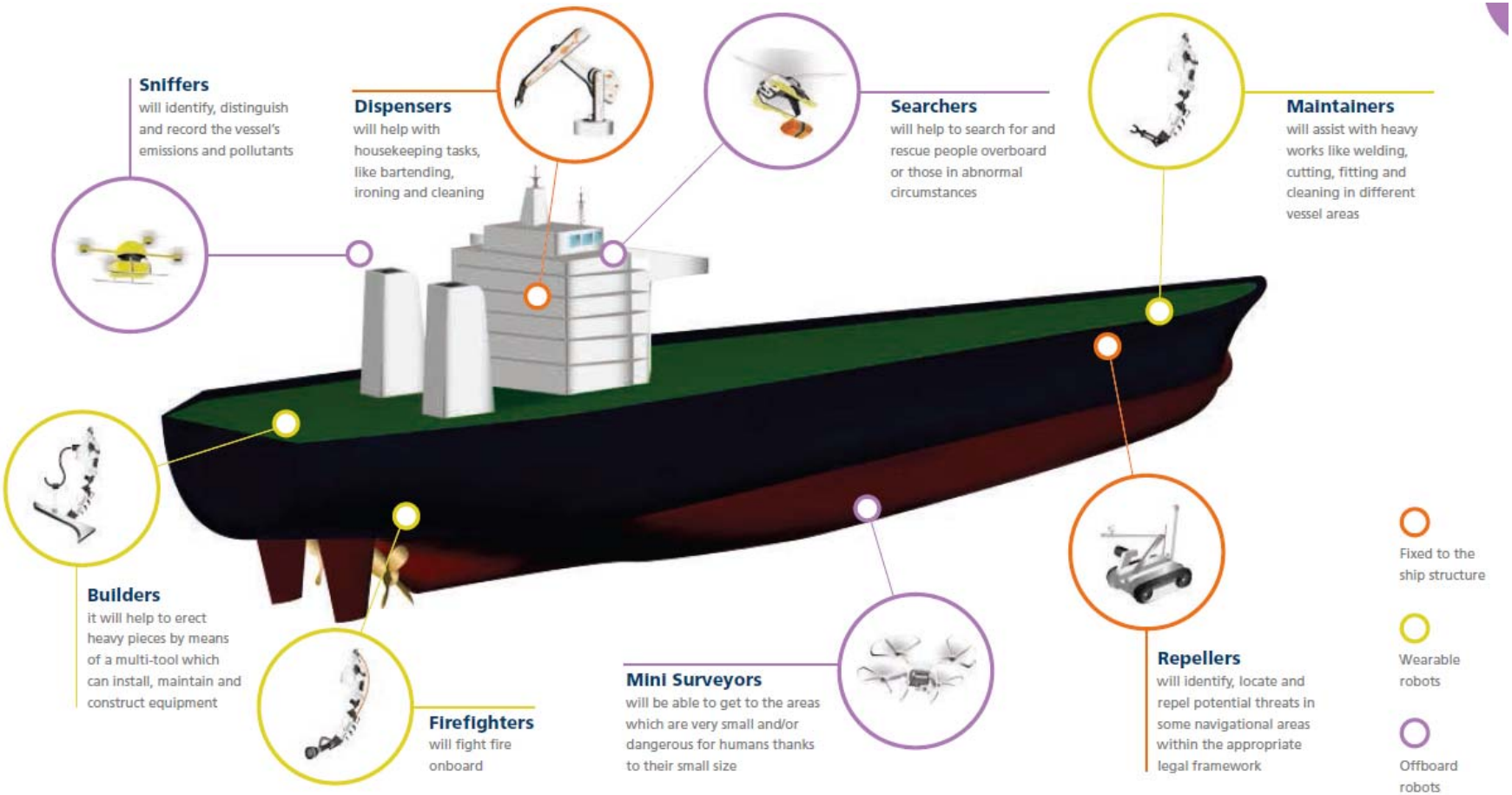
Hull, Machinery and Cargo - Networked Together



Integrated Ships Systems - Current



Additional Connected Technology (Future)



Sniffers
will identify, distinguish and record the vessel's emissions and pollutants

Dispensers
will help with housekeeping tasks, like bartending, ironing and cleaning

Searchers
will help to search for and rescue people overboard or those in abnormal circumstances

Maintainers
will assist with heavy works like welding, cutting, fitting and cleaning in different vessel areas

Builders
it will help to erect heavy pieces by means of a multi-tool which can install, maintain and construct equipment

Firefighters
will fight fire onboard

Mini Surveyors
will be able to get to the areas which are very small and/or dangerous for humans thanks to their small size

Repellers
will identify, locate and repel potential threats in some navigational areas within the appropriate legal framework

Fixed to the ship structure

Wearable robots

Offboard robots

Joint Hull Committee Paper – September 2015

"No identified systemic risk to ships. The risk of a loss to a ship as a result of cyber disruption is foreseeable, but is not yet a reality. A systemic threat which could conceivably result in multiple losses on a scale which might impact the solvency of the world's insurers and reinsurers does not yet exist."

US Maritime Resource Center (USMRC): Sample survey responses - 2015

- “Why would someone want to attack my business? We own and operate ships? They’re not connected to the internet.”

- “Who would want to attack this little marine terminal? Besides, we have followed the advice of our lawyers and insurers. They provide us with the compliance direction.”

- “What’s the threat?” Or “Where’s the threat – Nothing has happened yet!”

Question 2

How much of a risk do you think cyber is in shipping?

1. Not much at all – ships would be low on a hackers priority list
2. A very real risk – we need to work together as an industry to put measures in place
3. It’s not covered, so why worry about it!

II. .. and the Bad & Ugly…
What has happened so far?

Review of major incidents: Who What & Why
Source: Various internet reports and surveyor findings

USMRC Findings - 2016
Majority of ships surveyed had significant vulnerabilities!

- Little to no evidence of cybersecurity policy
- Little or no crew cyber awareness
- Unsupported/obsolete operating systems, even in new-build ships
- Many unpatched systems
- Many systems without anti-virus software or updated anti-virus definitions
- Dangerous crew modifications to IT networks and hardware configuration
- Removable media access on shipboard PCs
- No known cyber auditing occurring as a shipboard and safety management procedure
- Ethernet-connected Industrial Control Systems (ICSs)
- Critical systems connected to the internet without protections or segregation

What has happened?

A hacker caused a floating oil-platform located off the coast of Africa to tilt to one side, thus forcing it to temporarily shut down

Hackers infiltrated cyber systems in a port to locate specific containers loaded with illegal drugs and remove them from the port undetected

Somali pirates employed hackers to infiltrate a shipping company's cyber systems to identify vessels passing through the Gulf of Aden with valuable cargoes and minimal on-board security, which led to the hijacking of at least one vessel

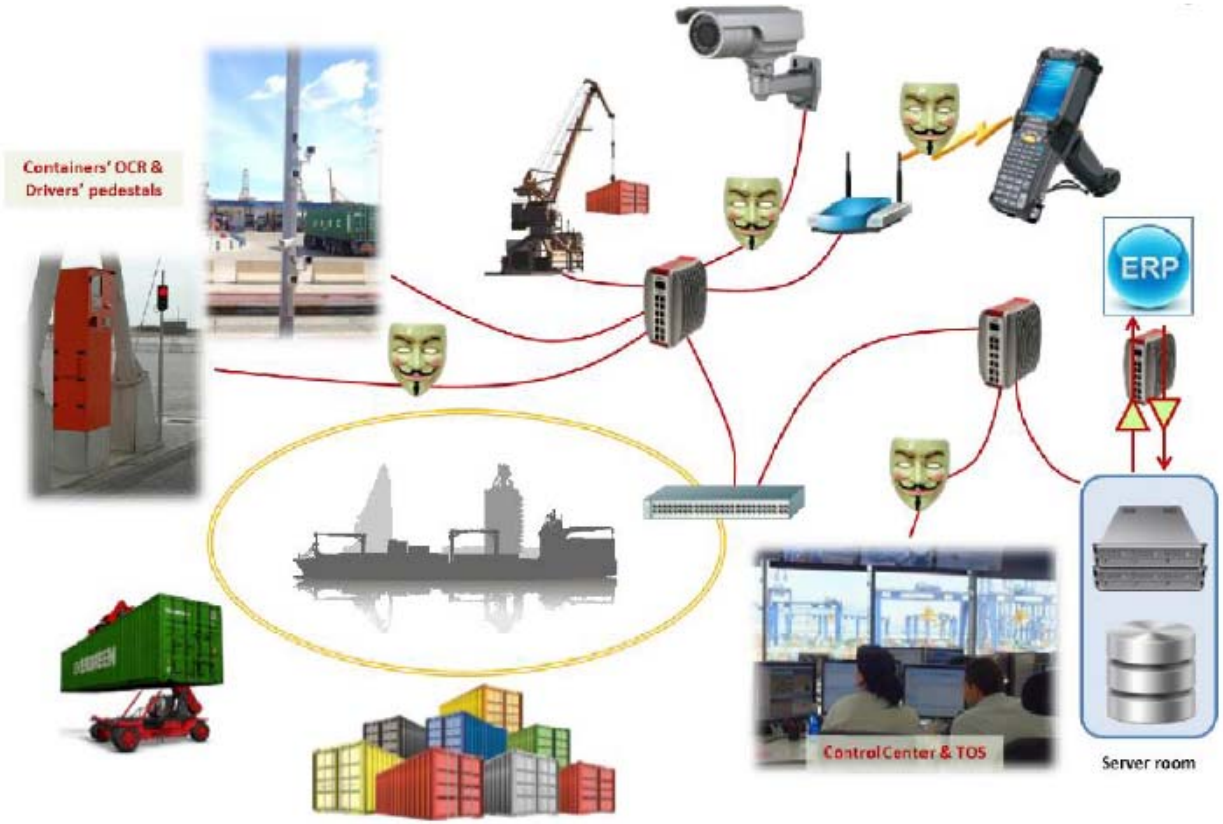
In the Norwegian energy and oil and gas sector, more than 50 cyber security incidents were detected in 2015

Ten years ago, the antivirus company McAfee registered 25 new threats a day - now they register half a million threats daily

Tests have been conducted and found to disrupt vessels ECDIS, AIS and GPS signals remotely.

Antwerp Port Hackers working with a drug smuggling gang infiltrated the computerized cargo tracking system of the Port of Antwerp to identify the shipping containers in which consignments of drugs had been hidden. The gang then drove the containers from the port, retrieved the drugs and covered their tracks. The criminal activity continued for a two-year period from June 2011, until it was stopped by joint action by Belgium and Dutch police

Antwerp Port Case



A crime organization used to transfer to the port of Antwerp huge cargo of drugs, hidden as bananas from South America. For that purpose, the organization hired a Belgian group of hackers, who cracked the management systems of two piers in the port. These systems manage the transport, storage and shipment of thousands of containers passing through the port each day. Cargo management systems now days include television cameras for automatic container identification and for documentation for insurance purposes; the systems manage loading and unloading queues, perform billing and more. The hacking enabled the crime organization to locate every container, even before the real client appeared to collect it. When the security breach was exposed, the port installed a firewall. However, the criminals did not give up; they penetrated physically into the port and installed wireless bridges on the operating computers, opening a direct access to the operating system. It took the port about two years to find the reason for the disappearance of containers at the port. In our virtual world, whatever disappears from the management systems - vanishes.

One Fleet's Problems

Fleet of 27 product tankers

Several vessels reported disruptions, including crashes and slow operating of the cargo control system. This was due to an old an outdated Window's based operating system that had no support or patches available.

Other ships had a failure of the electronic chart and radar system (ECDIS) due to viruses being inadvertently "uploaded" during email chart updates.

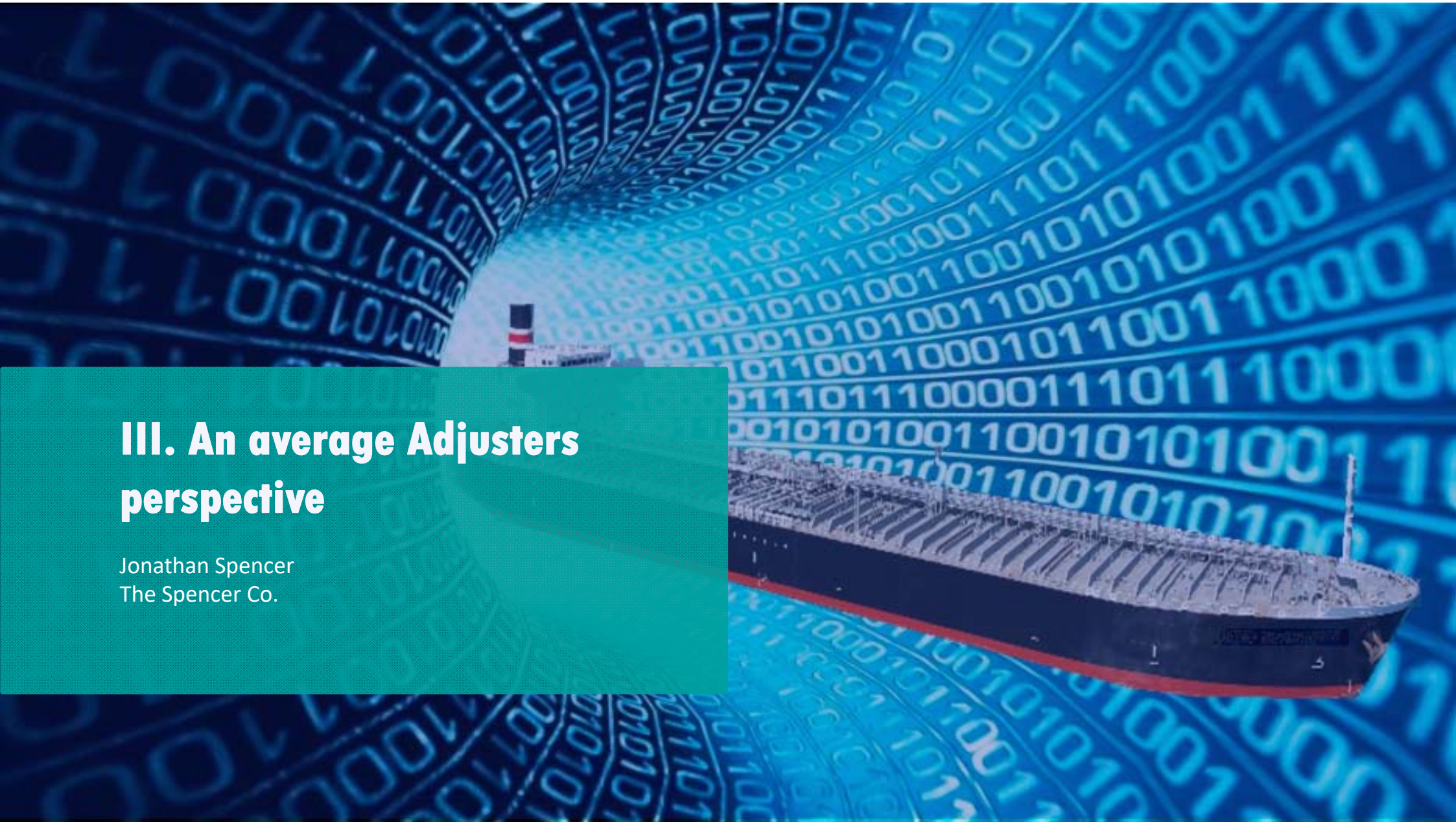
Cost to rectify the problems, including installing new cargo control systems was around EUR 60,000 per vessel. This was a proactive Owner who sought to identify and correct these issues.

The Offshore Hotel

A fully dynamically positioned hotel and maintenance vessel (stationed and linked to an offshore drill platform) had several unexplained thruster command failures.

Investigations showed that the main “bus” carrying the information from the bridge control system to the thrusters was overloaded with packets of information, causing the signals to be dropped or corrupted. The bus was common with the ballast system and other ships operating systems.

Major off hire claim and also minor damages to the rig and walkway



III. An average Adjusters perspective

Jonathan Spencer
The Spencer Co.

Cyber Loss

The London Market cyber exclusion clause:

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 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.

10/11/03

CL380

Cyber Loss

The AIMU cyber clause – part I:

American Institute
CYBER EXCLUSION CLAUSE
(11/06/2015)

This clause shall be paramount and shall override anything contained in this insurance (including any endorsement(s)) inconsistent therewith.

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

1. any “malicious act” involving the use of any “computer system”, "electronic data communications system", “computer virus”, or process or any other electronic system; and/or
2. any access to or disclosure of any “personally identifiable information” or any person's or organization's confidential information, including, but not limited to, patents, trade secrets, processing methods, customer lists, financial information, credit card information, or any other type of nonpublic information; and/or
3. any action or omission that violates or is alleged to violate any federal, state or local statute that addresses, prohibits, or limits the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating, or distribution of any written or electronic material or information.

Where this policy provides coverage for War Risks, section 1 above shall not operate to exclude losses which would otherwise be covered by such War Risks coverage.

Cyber Loss

IMCC
INTERNATIONAL
MARINE CLAIMS
CONFERENCE

The AIMU cyber clause – part II:

Definitions

"Computer system" means computer hardware of any kind; "electronic computer program"; "electronic data processing media"; operating system; media microchip; microprocessor (computer chip); integrated circuit or similar device; computer network and networking equipment; firmware; server; website; extranet; and all input, output, processing, storage, and off-line media libraries.

"Computer virus" means any corrupting, harmful or otherwise unauthorized instructions or code including, but not limited to, any maliciously introduced unauthorized instructions or code, programmatic or otherwise, that propagate themselves through a "computer system" or network of whatsoever nature.

"Electronic computer program" means computer software, application software, and other recorded instructions for the processing, sequencing, collecting, transmitting, recording, retrieval, or storage of "electronic data".

"Electronic data" means information or knowledge recorded or transmitted in a form usable in a "computer system", microchip, integrated circuit or similar device in non-computer equipment, and which can be stored on "electronic data processing media" for use by an "electronic computer program".

"Electronic data communications system" means any communication system, including a "computer system" and the internet, which provides the Assured with access to another "computer system", microchip, integrated circuit or similar device in non-computer equipment, or which provides any party access to the Assured's "computer system", microchips, integrated circuits or similar devices in non-computer equipment.

"Electronic data processing media" means punch cards, paper tapes, floppy disks, CD-ROM, hard drives, magnetic tapes, magnetic discs or any other tangible personal property on which "Electronic data" or "electronic computer programs" are recorded or transmitted, but not the "electronic data" or "electronic computer programs" themselves. Money or securities are not "electronic data processing media".

"Malicious act" shall mean the intentional and wrongful action or actions of one or more persons, whether or not agents of a sovereign power.

"Personally identifiable information" shall mean information, whether printed or digital, encrypted or unencrypted, in the care custody or control of any Assured which alone or in conjunction with other information can be used to uniquely identify an individual. However, "personally identifiable information" does not include information which is lawfully available to the general public.

Cyber Loss

IUA and AIMU clauses appear substantially equivalent, applying to ‘loss, damage, liability or expense’ —

IUA’s ‘*means for inflicting harm*’ essentially the same as AIMU’s definition, ‘*“Malicious act” shall mean the intentional and wrongful action or actions of one or more persons*’

However, what is ‘harm’?

(AIMU does not have an exclusion equivalent to the IUA exclusion for war risks)

Cyber Loss

Question 3:

Does the cyber factor have to be the proximate cause of the loss for the Cl. 380 exclusion to operate?

Cyber Loss

- What is the cargo insurance position?
- What is the P&I position?

Cyber Loss

A recent survey of major brokers indicated that the London market is standing firm on the cyber exclusion, partly driven by the conditions of reinsurance contracts

The sole exception:

…we are finding that London Uwrs are prepared, on Hull and Machinery policies, to delete this clause and/or renew a policy without it on certain fleets where doing so gives Uwrs a competitive advantage and realistically only on the larger 'blue water' fleets.

IV. A surveyor's perspective

John Walker
Chief Surveyor, Braemar (Salvage Association)

Cyber risk exposure – Where do we go?

- Previously managed by Insurers with policies containing full exclusion clauses…however…
- Growth in use of technology to build, manage and run vessels leading to increased Insured reliance on electronic systems and awareness of associated risks
- Means that the insurance industry must adapt policy coverage to remain relevant in the medium to long term.
- Mitigation of risk must be stepped up
- Training of crew, owners and surveyors to ensure safeguards are in place and maintained – similar to physical risks.

What is required?

- Currently several organisations, including IACS and IMO are looking at introducing Cyber related regulation. Only guidance in place at present, which is not binding.
- New rules for ECDIS systems, coming in 2017 have no provision for cyber security standards
- Currently separate equipment is class tested and approved, however the backbone of the integrated ships systems is often overlooked with respect to design and serviceability
- Condition inspection checklists (e.g. JHC, P&I, Flag State) do not have any specific checks for cyber security

V. Realistic loss scenarios

INTERACTIVE

Product Tanker Bayonne Bridge NJ
Grounding/ Spill/ Channel Blocked

Scenario

- Product tanker with several packages of liquid cargo onboard - some packages are marine pollutants - is grounded under the Bayonne Bridge following a loss of navigational systems
- The loss of systems is down to the navigational systems and chart plotter being compromised by a hacker (Anonymous).
- Potentially the hacker has developed the program to corrupt the integrated bridge system, and a crew member has inadvertently uploaded the corrupt program to the ships system during a chart update.
- The vessel is grounded, pollution has occurred, there are significant hull damages and salvage costs.

Our bridge over the main channel into Port Newark

Close up map


PORT NEWARK
GLOBAL
MOTEY
RED HOOK MARINE TERMINAL
SOUTH BROOKLYN MARINE TERMINAL
HOWLAND HOOK MARINE TERMINAL
STAPLETON
Bayonne Bridge
STATEN ISLAND

Scenario (cont'd)

- The vessel is grounded, pollution has occurred, there are significant hull damages and salvage / removal costs.
- Lightering of the vessel is done in an emergency fashion and some of the high grade cargo is taken off to achieve this. The cargo is no longer fit for purpose and needs disposal.
- Due to the location of the vessel there are large BI claims from the various terminals, shippers and cargo owners in Newark / Bayonne that now can't use the port. Other ports up and down the east coast are overwhelmed with capacity issues.
- So cargo is lost, we have a hull claim, salvage issues and the vessel needs to be lightered to refloat and clear the channel, resulting in the sacrifice of cargo.

Cyber Loss

IMCC
INTERNATIONAL
MARINE CLAIMS
CONFERENCE

Thank you!

Hard questions:

John Walker, Chief Surveyor, Braemar (Salvage Association), New York

john.walker@braemar.com, +1 (917) 392-0463

Easy questions:

Jonathan Spencer, Average Adjuster, The Spencer Company, New York

jss@jssusa.com, +1 (917) 696 5467