Exponent®

Maritime Autonomous Surface Ships (MASS)

The Present and the Future

MARIA LAGOUMIDOU

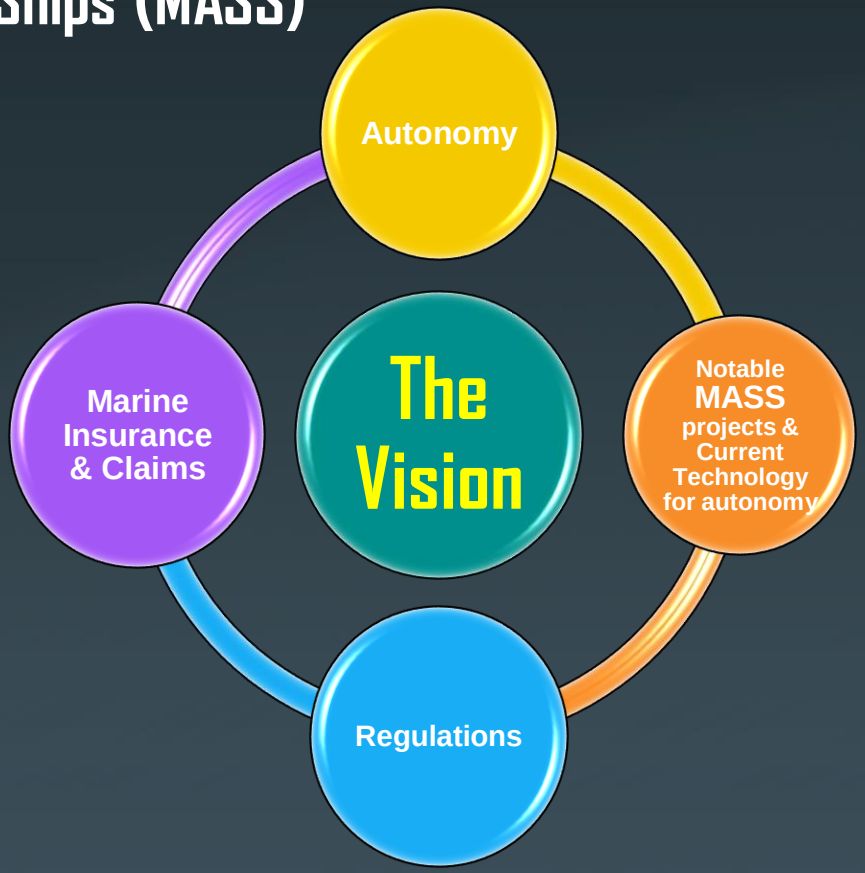
Naval Architect & Marine Engineer,

CEng (MRINA)

25th September 2019

Maritime Autonomous Surface Ships (MASS) The Present and the Future

OUTLINE



THE VISION

It is almost midnight, a full moon is shining over the Thames.

The river is calm, the reflection of a ship's name is on the water: 'CREWLESS'. It is a shame that no one can see this reflection from her weather deck, there are no crew onboard.

She is an autonomous ro-ro cargo ship which just sailed from a nearby berth upstream, after a full cargo of autonomous cars and trucks loaded themselves onboard her seven decks. CREWLESS is heading towards Rotterdam where the cars and trucks will drive themselves off to their destinations without human intervention.

What does 'autonomy' actually mean?

- This word is Greek : αυτονομία, from αυτος 'self' ✚ νομος 'law'.
- The Cambridge dictionary online, gives the following meaning:
  '*The ability to make your own decisions without being controlled by anyone else*'
- For the purpose of the IMO regulatory scoping exercise:
  "Maritime Autonomous Surface Ship (MASS)" is defined as a ship which, to a varying degree, can operate independent of human interaction and described 4 'degrees of autonomy'
- The Society of Automotive Engineers, SAE in US has issued SAE J3016 showing in table format 'levels of driving automation'
  There are 6 levels with the 'driver support features' and 'automation features'

Are there ships realising an autonomous vision at present ?

Yara Birkerland

(Source: https://www.yara.com/news-and-media/press-kits/yara-birkeland-press-kit/)

Are there ships realising an autonomous vision at present ?

Folgefonn

(Source: https://www.wartsila.com/media/news/28-11-2018-wartsila-achieves-notable-advances-in-automated-shipping-with-latest-successful-tests-2332144)

Are there ships realising an autonomous vision at present ?

Falco

(Source: https://www.rolls-royce.com/media/press-releases/2018/03-12-2018-rr-and-finferries-demonstrate-worlds-first-fully-autonomous-ferry.aspx and Finferries Images : Copyright Finferries. Used with Permission.)

Are there vehicles realising an autonomous vision at present ?

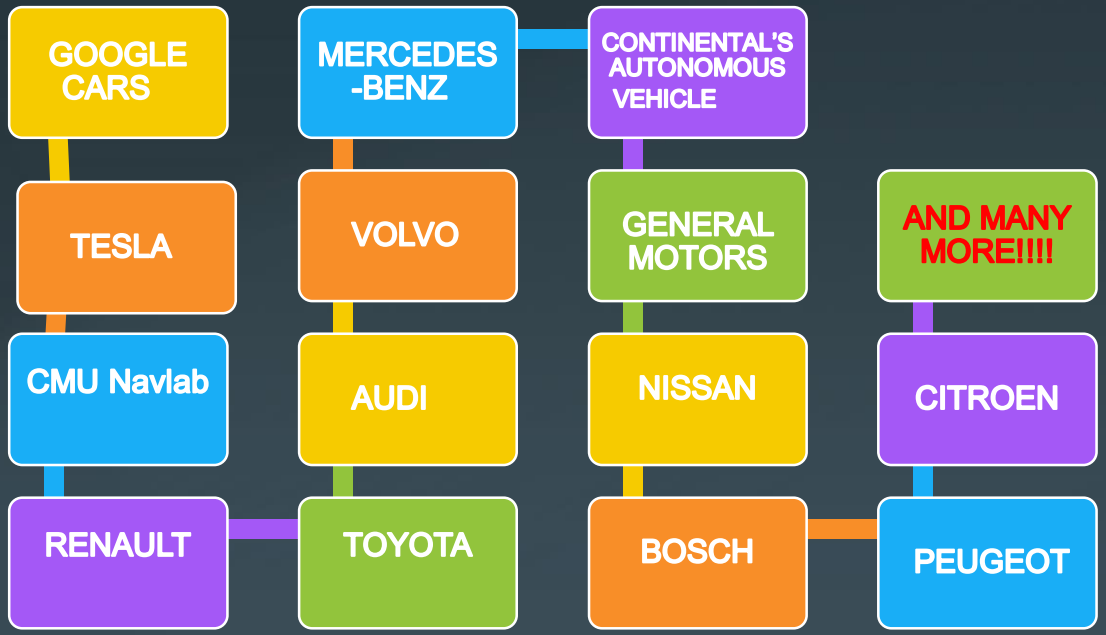
VOLVO'S VERA TRUCKS

(Sources: https://venturebeat.com/2019/06/13/volvos-vera-autonomous-trucks-will-transport-dfds-goods-on-public-roads/ and https://www.volvotrucks.com/en-en/news/volvo-trucks-magazine/2019/jun/Veras-First-Assignment.html)

Press Images:
https://www.volvotrucks.com/en-en/about-us/automation/vera.html

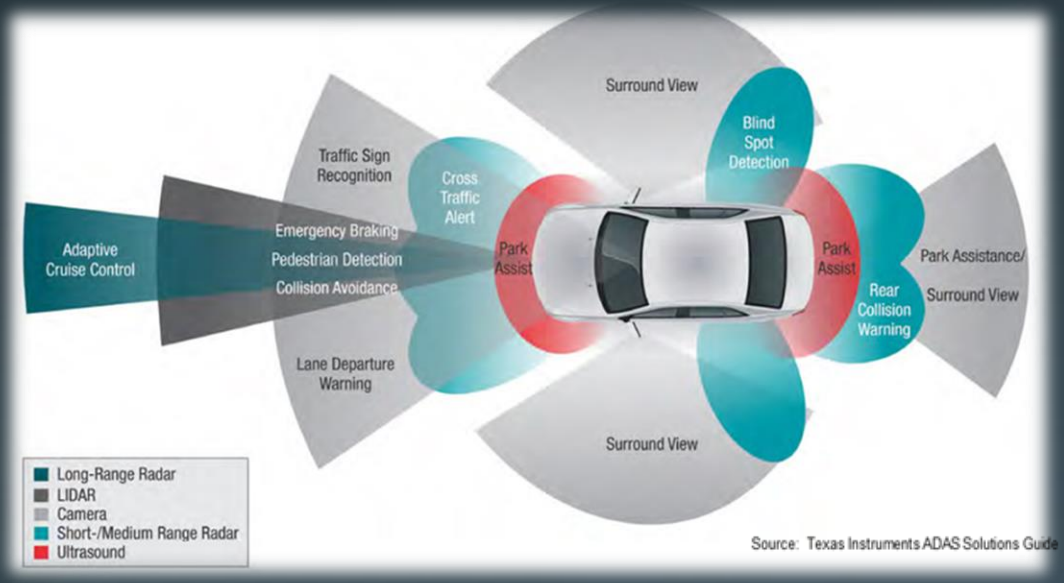
Are there vehicles realizing an autonomous vision at present ?

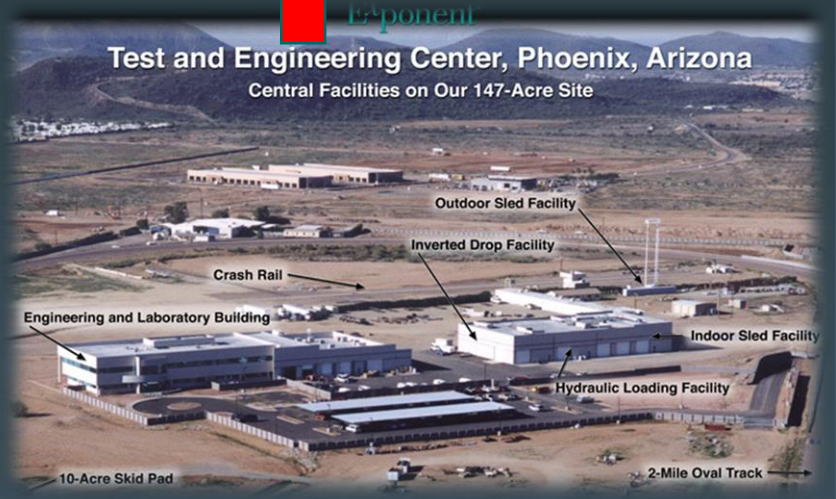
Autonomous cars or self-driving cars



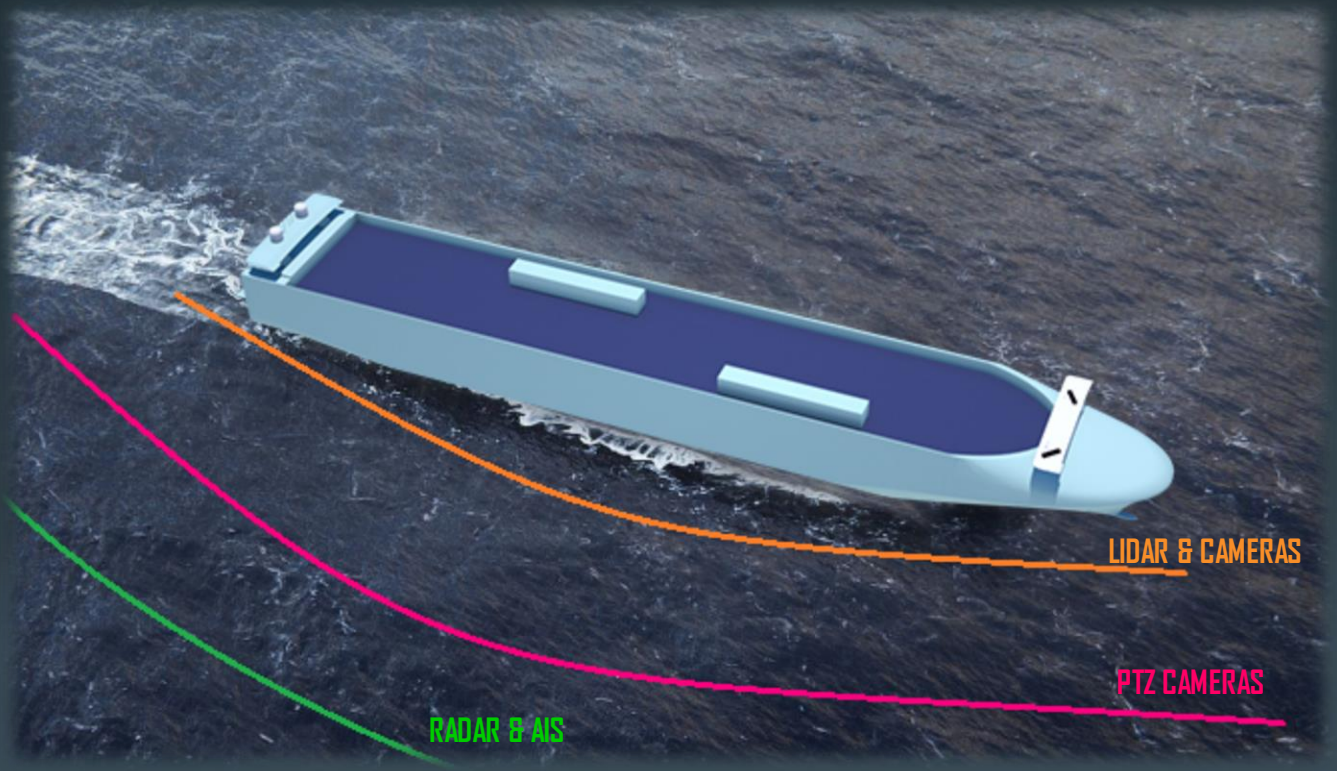
Autonomous technology for vehicles

Advanced Driver Assistance Technologies (ADAS)





Autonomous technology for ships - Navigation



Autonomous technology for ships - Mooring

Autonomous technology for ships

Ports & Terminals

Big data transfer & storage

Road Network

Connectivity

Energy supply

…

Infrastructure

Ship Main Functions

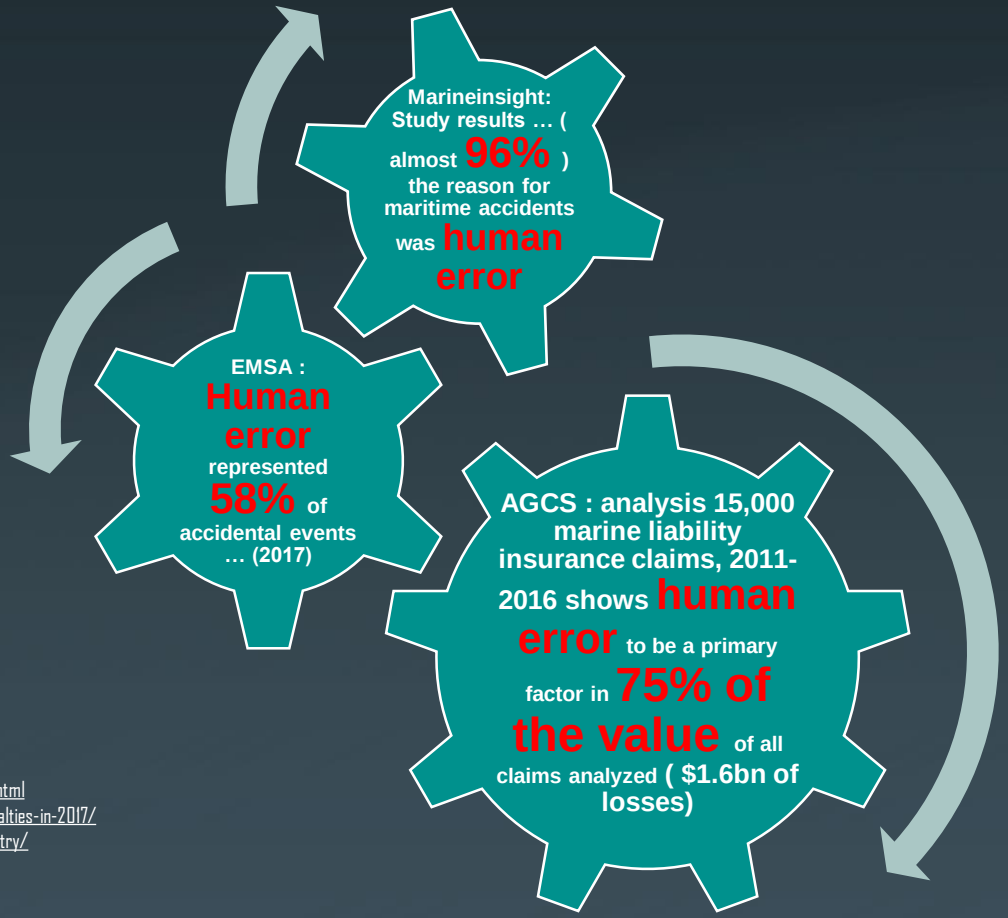
- Power Generation
- Weathertight & Watertight integrity
- Strength
- Steering
- Propulsion
- Ballasting
- Drainage & Bilge pumping
- Anchoring & Mooring
- Cargo handling
- Navigation
- Communication
- Safety systems

How increased automation and autonomous technology on ships will affect marine insurance ?

'Maritime autonomous surface ships-Zooming in on civil liability and insurance'
by CORE Advokatfirma and Cefor, December 2018

'In a global context, the increased automation and the introduction of MASS is expected to reduce the level of risks and marine casualties, while at the same introducing risks that have not previously been quantified or insured.'

'...the introduction of MASS is expected to reduce the level of risks and marine casualties.'



Sources :
https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/human-error-shipping-safety.html
https://www.iims.org.uk/european-maritime-safety-agency-publishes-an-overview-of-maritime-casualties-in-2017/
https://www.marineinsight.com/marine-safety/the-relation-between-human-error-and-marine-industry/

'... introduce risks that have not been previously quantified or insured'

CONVENTIONAL SHIPS

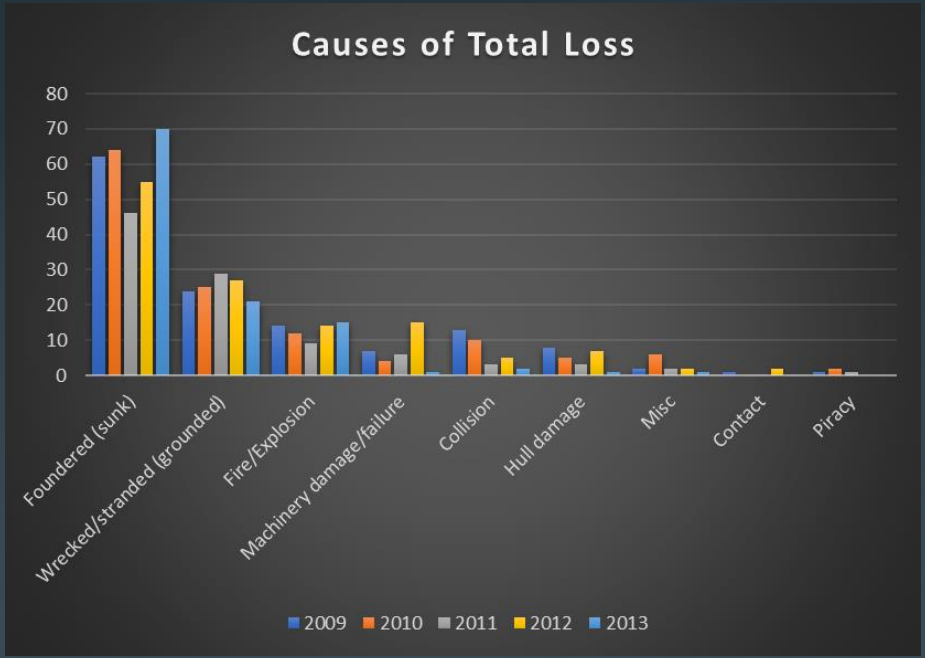
RISK PROFILE

CLAIMS HISTORY

STATISTICS

DATA ANALYTICS

...



Source : AGCS-Safety-Shipping-Review-2019

'... introduce risks that have not been previously quantified or insured'

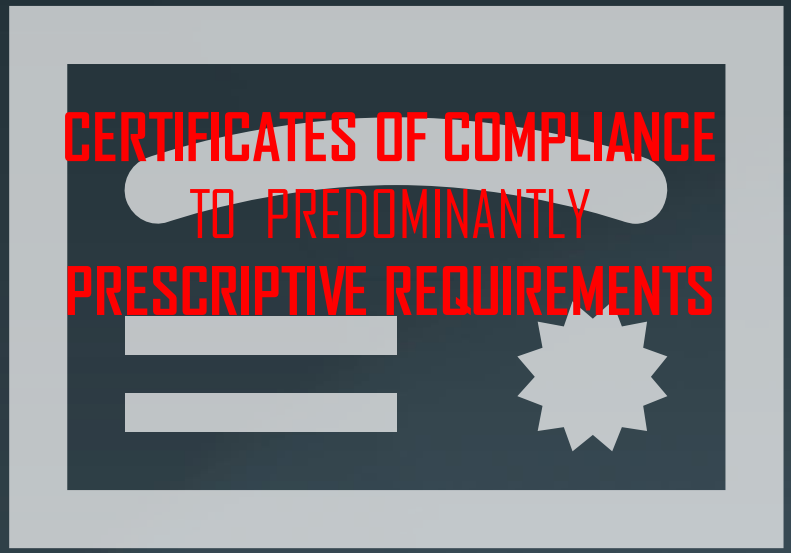
AUTONOMOUS SHIPS

RISK PROFILE

?

*This page intentionally left blank *

Traditional way of assuring risk related to technology for marine insurance



CLASSIFICATION RULES

STATUTORY REGULATIONS

Do we have Classification Rules and Statutory Regulations for autonomous ships?

PRESCRIPTIVE

CLASSIFICATION S[illegible] & F[illegible] ADMINISTRATIONS

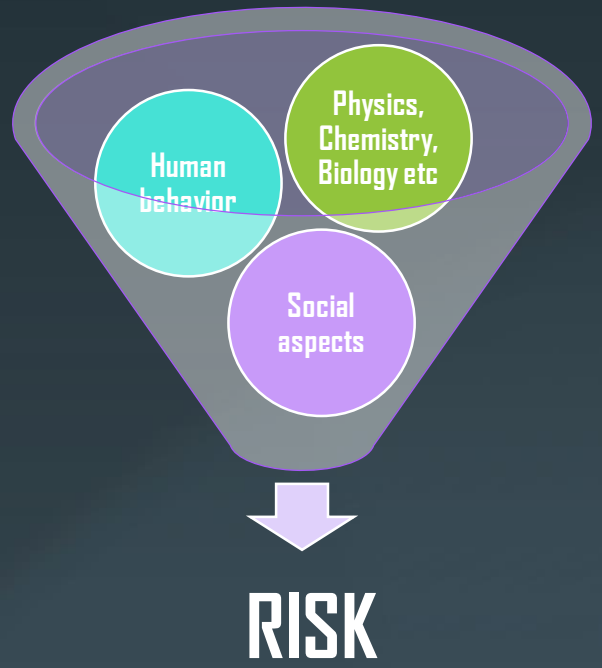
'CODE', 'GUIDELINE'

[illegible]ULATORY FRAMEWORK EXERCISE'

'INTERIM GUIDELINES FOR MASS TRIALS'

RISK ASSESSMENT

RISK as a systemic product



RISK ASSESSMENT

- Hazard Identification

What could possibly happen within this system which could lead to harm?

- Risk analysis

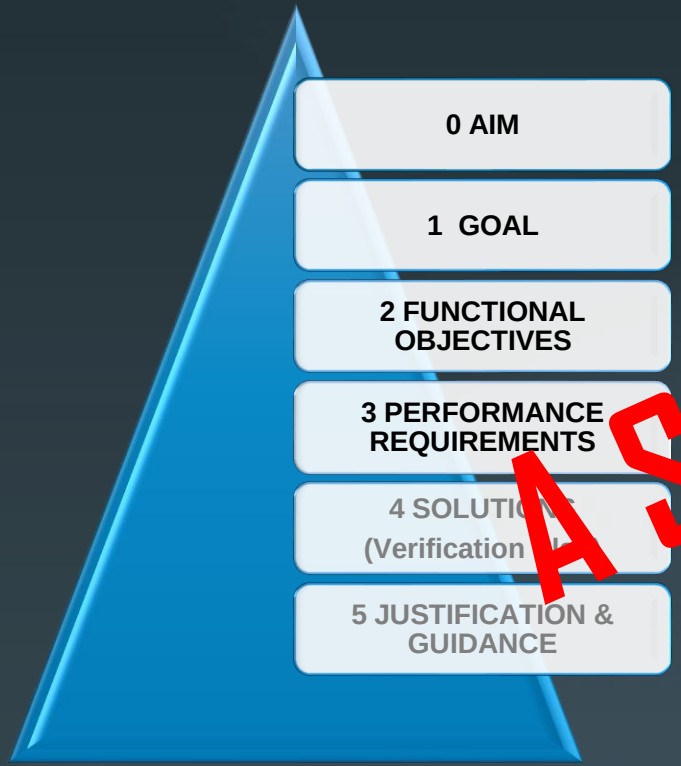
What are the chances of particular consequences?

- Risk Evaluation

What are acceptable risks and what changes do we need to make to the system, if any, to ensure that the risks are acceptable?

Source: 'Risk Assessment and Safety Management' [D21RA], Herriot Watt University 2011

LLOYD'S REGISTER – Code for Unmanned Marine Systems



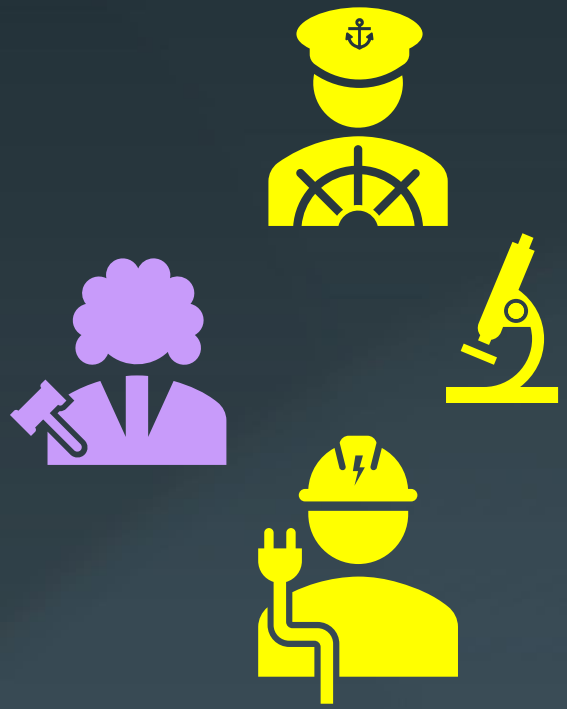
- structure
- stability
- control system
- electrical systems
- navigation systems
- propulsion & manoeuvering
- fire
- auxiliary systems

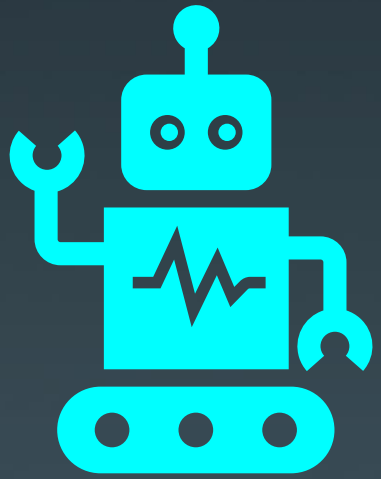
Verification activities for each UMS system will depend on the **Safety & Operational Levels of Integrity**

Consequences based

A SAFETY CASE

MARINE CLAIMS – The engineering expert's perspective for MASS





Exponent®

Maritime Cybersecurity

Nick Batara, Ph.D.

Sonal Kothari Phan, Ph.D., P.E., Network+, Security+

Brian D'Andrade, Ph.D., P.E. CISSP, CCNP-Security, PMP

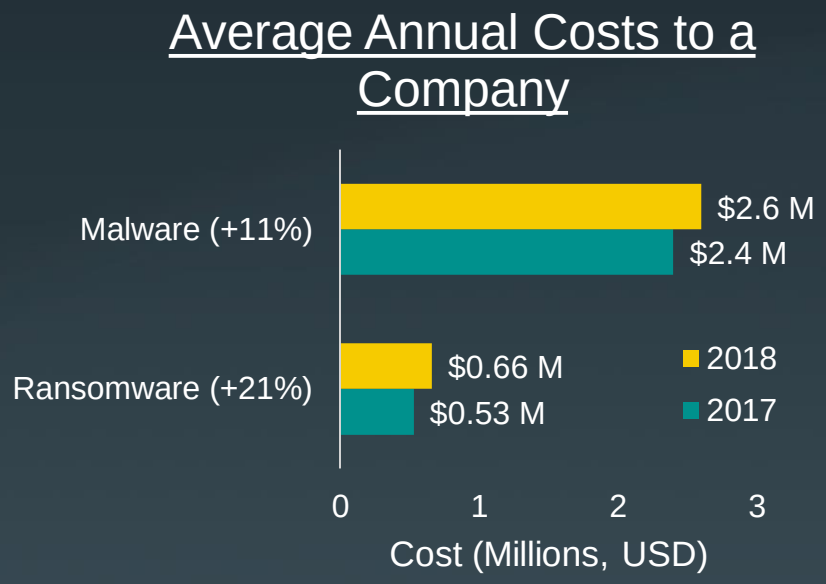
September 25, 2019

Outline

- Cybersecurity Trends
- Maritime Vulnerabilities
- Cyberinsurance Policies
- Case Studies
- Summary and Outlook

Global Trends

- USD **$600B**: Global cybercrime cost in 2017
- Increasing complexity of attacks
- Cyberinsurance growth:
  - USD $2.5B: Premiums in 2014
  - USD **$7.5B**: Expected premiums in 2020



2,647 Interviews, 355 Companies, 11 Countries

1. https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html
2. Ninth Annual Cost Of Cybercrime Study, https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

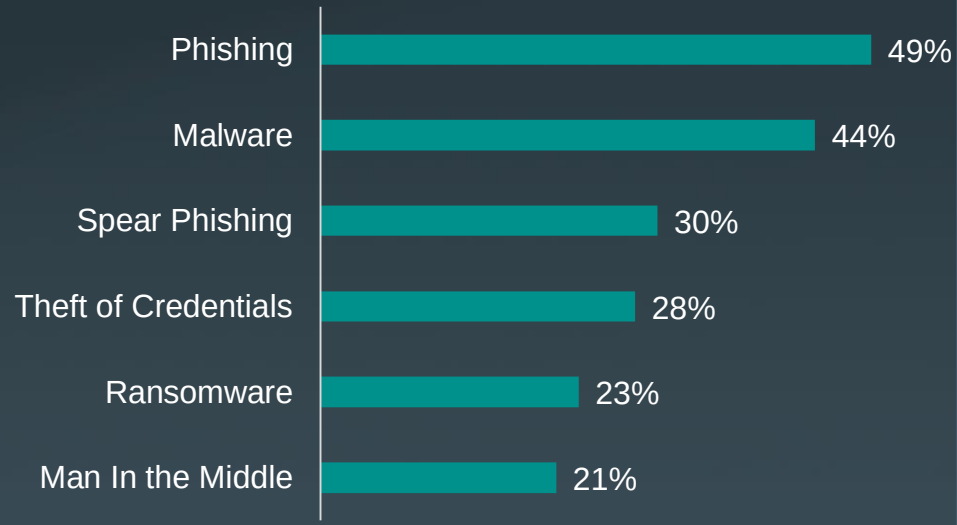
Poll

- How many maritime industry professionals have been victims of cyber crime?
  - A: 1 in 2
  - B: 1 in 5
  - C: 1 in 10
  - D: 1 in 50

Maritime Trends in Cybersecurity

- More than 1 in 5 victim of cybercrime
- **Phishing and malware attacks**
- Increased guidelines, standards, and incident information sharing

Incident Types, Past 12 Months



2018 Survey of 237 Maritime Professionals

1. Fairplay and BIMCO Maritime Cyber Security survey 2018

Why Attack the Maritime Industry?

"The international shipping industry is responsible for the carriage of around 90% of world trade."

Group	Motivation	Objective
Activists (including disgruntled employees)	■ reputational damage ■ disruption of operations	■ destruction of data ■ publication of sensitive data ■ media attention ■ denial of access to the service or system targeted
Criminals	■ financial gain ■ commercial espionage ■ industrial espionage	■ selling stolen data ■ ransoming stolen data ■ ransoming system operability ■ arranging fraudulent transportation of cargo ■ gathering intelligence for more sophisticated crime, exact cargo location, ship transportation and handling plans etc
Opportunists	■ the challenge	■ getting through cyber security defences ■ financial gain
States **State sponsored organisations** **Terrorists**	■ political gain ■ espionage	■ gaining knowledge ■ disruption to economies and critical national infrastructure

1. http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade
2. ICS, The Guidelines On Cyber Security Onboard Ships, V3

Maritime Cybersecurity Guidance and Regulation

- International Maritime Organization (IMO)
  Guidelines on maritime cyber risk management, 2017

- International Chamber of Shipping (ICS)
  Guidelines on Cyber Security Onboard Ships, 2018

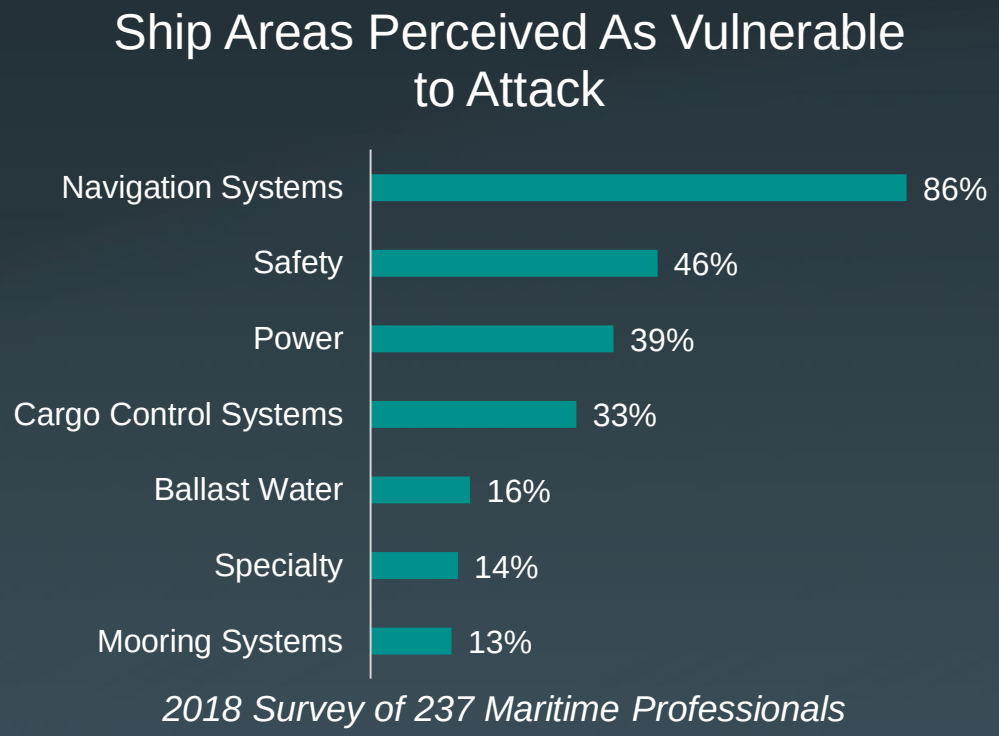
- Safety of Life at Sea (SOLAS) Cybersecurity Regulation, 2021

Poll #2

- Which shipborne systems are most vulnerable to attack?
  - A: Navigation Systems
  - B: Cargo Control Systems
  - C: Mooring Systems
  - D: Power Systems

Ship Vulnerabilities

- 8% of attacks affected shipborne systems in 2018
  - 2x increase from 2016
- Navigation and safety systems of highest concern



1. Fairplay and BIMCO Maritime Cyber Security survey 2018

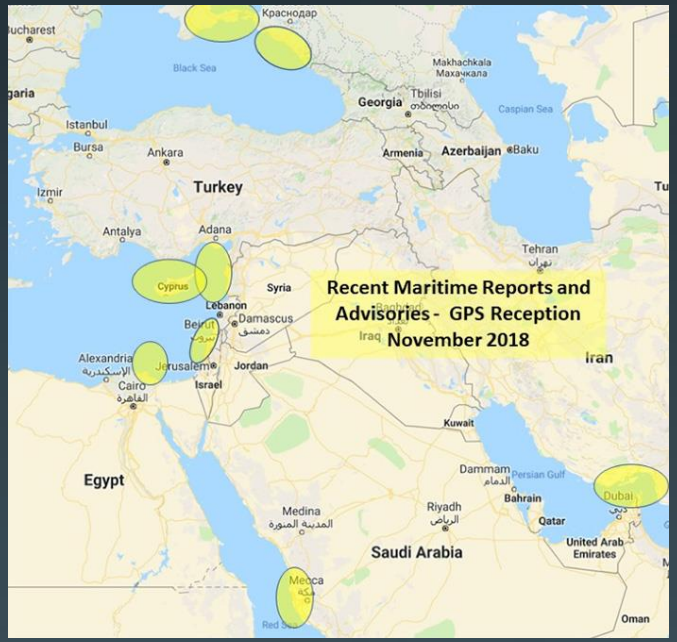
Navigation and Safety Systems

- Electronic Chart Display and Information System (ECDIS)
- Automatic Identification System (AIS)
- Voyage Data Recorder (VDR)
- Global Maritime Distress and Safety System (GMDSS)
- Integrated Bridge Systems
  - Engine control
  - Autopilot

1. Photo Credit: Paris MoU

GNSS Jamming

- GNSS jamming equipment is cheap and readily available
- GNSS jamming for illegal activities
- Loss of GNSS signal can affect navigation if undetected and degrade satcom

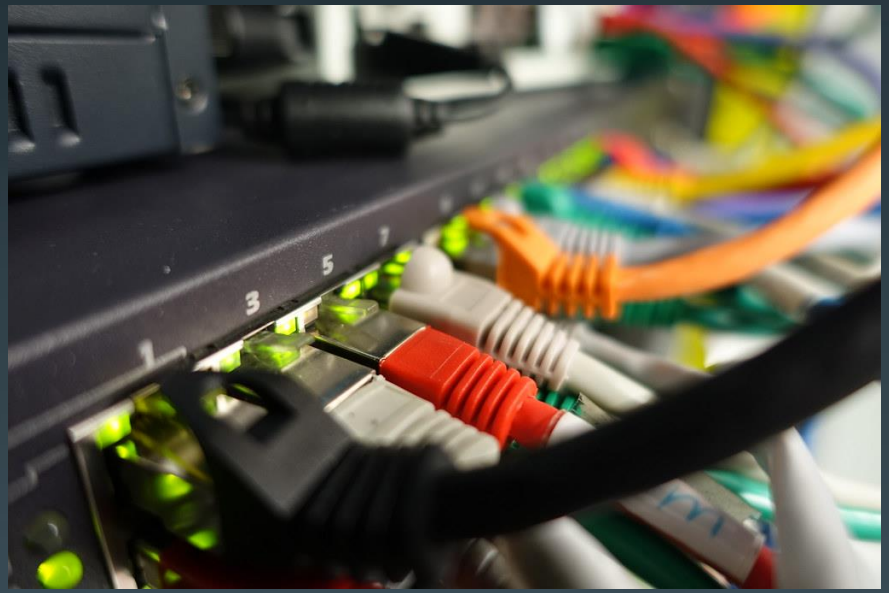


1

1. https://www.gpsworld.com/gps-disrupted-for-maritime-in-mediterranean-red-sea/
2. https://www.newscientist.com/article/dn20202-gps-chaos-how-a-30-box-can-jam-your-life/

Vessel Networking

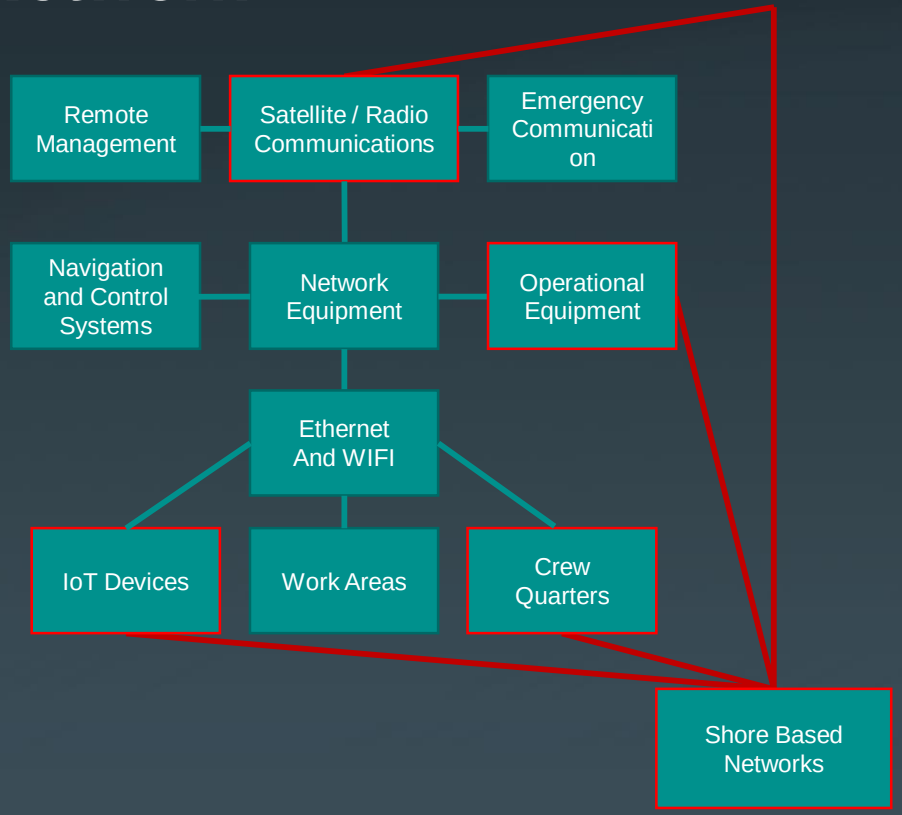
- Ships are increasingly designed as floating networks
- Wide variety of network hardware and communication protocols based on ship size and equipment:
  - Wired: Ethernet / Fiber Optic / NMEA 2000 / SCADA / Serial
  - Wireless: WiFi / 2G-5G / Satellite / Radio



1. Photo Credit: webernetz

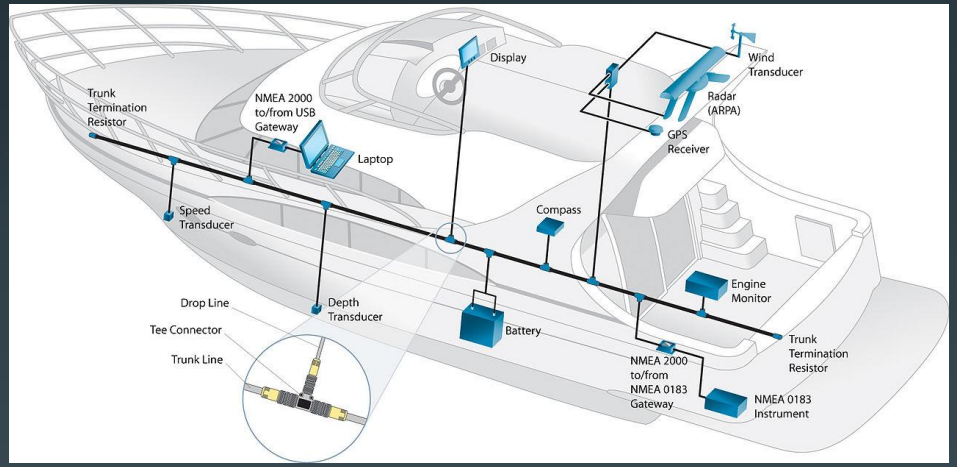
Conceptual Model of Ship Network

- Many systems connected to central network equipment
- Network configurations critical to security
- Ships are increasingly connected
  - Satellite communications at sea
  - Cellular and wifi networks near shore



NMEA 2000

- Adopted from CAN bus
- Modern standard for smaller vessels
- Used on commercial vessels



1. Photo Credit: Femnett/Maretron, LLP - Maretron, LLP

Vehicle Network Bus Vulnerabilities

- CAN bus connects sensors and control electronics
- CAN was first in cars in 1991
- No intrinsic security
- Numerous examples of vulnerabilities through connected systems in cars (entertainment system, OnStar, remote entry system)

1. https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/

Networked Device Vulnerabilities

- Satcom web interfaces provide identifying information
- Frequently out of date software
- Default and weak passwords
- AIS ship data can be correlated to onboard networked devices

1. https://ptp-shiptracker.herokuapp.com
2. https://www.pentestpartners.com/security-blog/tracking-hacking-ships-with-shodan-ais/
3. https://www.pentestpartners.com/security-blog/hacking-ais/

IoT Vulnerabilities

- Increasing use of IoT devices for monitoring of equipment and cargo
- Common IoT Exploits:
  - Hijacking for DDOS attacks
  - Data interception

28 Jun 2019 | 11:44 GMT

Shipping Industry Bets Big on IoT in Bid to Save Billions

Across the shipping industry, IoT technology is finally graduating from pilots to real-world commercial products

By **Manon Verchot**

Photo-illustration: Traxens

1. https://spectrum.ieee.org/tech-talk/telecom/internet/shipping-industry-bets-big-on-iot-in-bid-to-save-billions

Cyberinsurance Policies, a New Insurance Offering

- 2019 Study
  - 235 Cybersecurity Policies and Associated documents from
    - California, New York and Pennsylvania
- Findings:
  - Reputable data for accurate pricing is limited
  - Insurance coverage elements more consistent than exclusions
  - Variety of pricing models

1. Sasha Romanosky, Lillian Ablon, Andreas Kuehn, Therese Jones, Content analysis of cyber insurance policies: how do carriers price cyber risk?, Journal of Cybersecurity, Volume 5, Issue 1, 2019, tyz002, https://doi.org/10.1093/cybsec/tyz002

Direct Losses

- Information
  - Databases and software
- Physical damage
  - Equipment and hardware controlled digitally
- Investigation challenges
  - Response time
  - Confidentiality and regulatory compliance
  - Proper evidence handling

Indirect Losses

- Business interruption
- Contract liability for delayed goods
- Investigation Challenges
  - Lengthier Timescale
  - Legal Disputes
  - Experts

Case Study: US Manufacturing Business

- Attack in July 2018
- 83 Devices Affected
  - Emotet/Trickbot Malware
  - Bitpaymer Ransomware
- Suspected attack vector: phishing email with .doc file
- Ransom of 20 bitcoins paid (Approx. USD$140K)
- Initial investigation and remediation carried out by external vendors

1. Photo Credit: Anna Daley

Case Study: US Manufacturing Business

- One IT staff member at time of attack
- No systematic inventory of devices
- Manufacturing operations hobbled by attack
- insured claimed some devices to be damaged and inoperable
- Retained by insurer to investigate claim

Case Study: US Manufacturing Business

- July 2019 inspection
- Not all devices could be located
- Most devices provided found operational after wiping drives

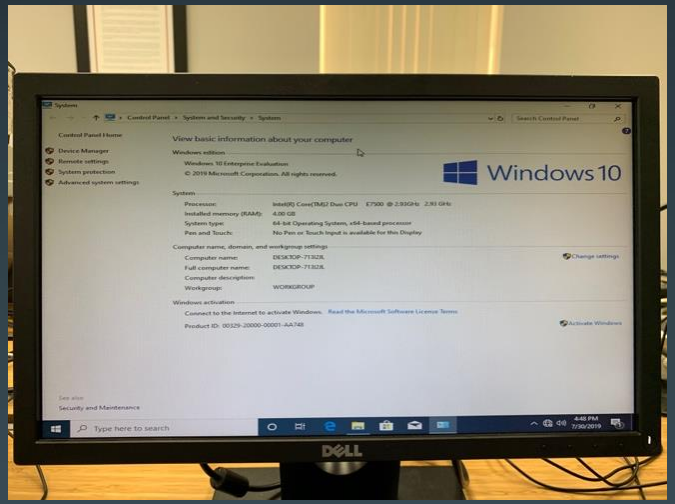
Initially Failed Boot

Hard Removed and Wiped

Case Study: US Manufacturing Business

- Findings: “[no] evidence to support direct physical loss or damage to computer hardware due to the malware attack and thus, [the insured] was not required to replace hardware due to the malware attack.”

Successful Reinstallation of Software



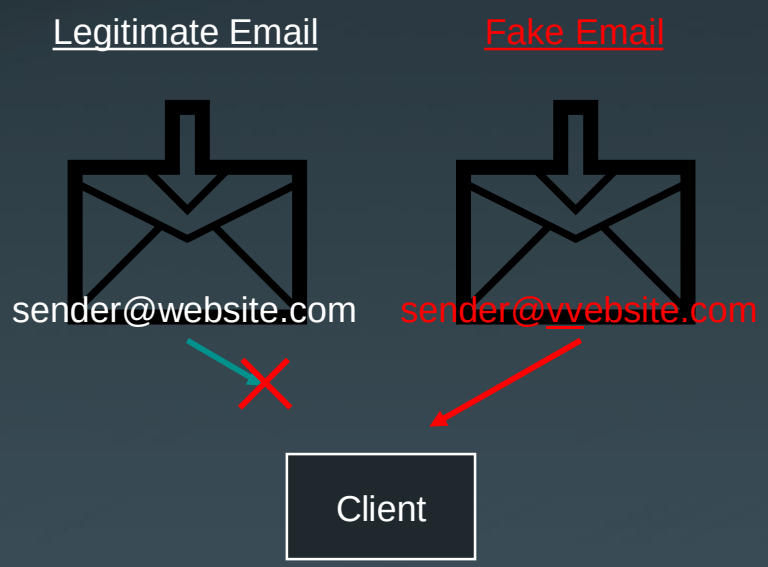
Case Study: Management Consulting Firm

- Incident December 2018 – February 2019
- Compromise of Microsoft Office 365 account
- USD $500K paid to falsified bank account
- Claim filed for loss business income
- Retained to evaluate claim

1. Image Credit: Vectortoons

Case Study: Management Consulting Firm

- Account operated by employee
- Email rules created to hide emails from clients
- Invoices intercepted and modified
- Modified invoices sent to clients with altered billing information
- Invoices sent using spoofed email address “VV” instead of ”W’



Case Study: Management Consulting Firm

- Separate Outsider and Insider Attack Coverages
- Coverage Limitations:
  - Random or multiple attacks
  - Systems not owned, operated or utilized pursuant to a written contract by insured
- Investigation Findings:
  - Attack consistent with outsider attack coverage

Case Study: Maersk 2017 Cyber Attack

- Broadly affected by malware attack starting June 27, 2017
- 4,000 servers, 45,000 PCs and 2,500 applications affected
- Cost: $250 – 300 Million dollars

MAERSK

Cyber attack update

June 28, 2017

ANNOUNCEMENT

A.P. Møller - Mærsk A/S — cyber attack update

We can confirm that Maersk has been hit as part of a global cyber attack named Petya on the 27 June 2017. IT systems are down across multiple sites and select business units.

We have contained the issue and are working on a technical recovery plan with key IT-partners and global cyber security agencies.

We have shut down a number of systems to help contain the issue. At this point our entities Maersk Oil, Maersk Drilling, Maersk Supply Services, Maersk Tankers, Maersk Training, Svitzer and MCI are not operationally affected. Precautionary measures have been taken to ensure continued operations.

Maersk Line vessels are maneuverable, able to communicate and crews are safe. APM Terminals is impacted in a number of ports.

We continue to assess and manage the situation to minimize the impact on our operations, customers and partners from the current situation.

Business continuity plans are being implemented and prioritized. The aggregate impact on our business is being assessed.

1. Securing a Common Future in Cyberspace, World Economic Forum Annual Meeting, January 24, 2018
2. http://investor.maersk.com/node/19831/pdf

Case Study: Mondelez v. Zurich

- Also affected by ransomware on June 27, 2017
- Claim initially denied under war exclusion clause
- Mondelez alleges a “failure to modify that historical language to specifically address the extent to which it would apply to cyber incidents”[1]

Mondelez sues Zurich over $100m cyberhack insurance claim

Zurich refused to pay out for NotPetya attack, relying on war exclusion

Thu, Jan 10, 2019, 11:16 | Updated: Thu, Jan 10, 2019, 12:26

A Cadbury chocolate egg production line. Mondelez, the US food company that owns the Oreo and Cadbury brands, is suing its insurance company, Zurich, over a NotPetya cyberattack claim. Photograph: Simon Dawson/Bloomberg

1. Mondelez International Inc., v. Zurich Americna Insurance Company, Complaint, October 10, 2018
2. https://www.irishtimes.com/business/technology/mondelez-sues-zurich-over-100m-cyberhack-insurance-claim-1.3753475

Case Study: Mondelez v. Zurich

- Litigation Ongoing
- "*the case could have wide implications for the insurance market, potentially pushing insurance buyers to either buy cyber-specific policies or demand tighter terms for their non-cyber coverage*"

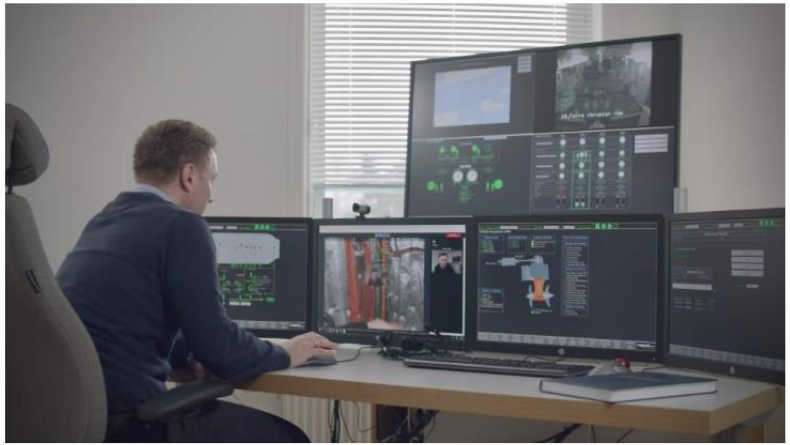
1. https://www.irishtimes.com/business/technology/mondelez-sues-zurich-over-100m-cyberhack-insurance-claim-1.3753475

Summary and Outlook

- Increasing reliance on IT
- Cybersecurity insurance premiums are growing rapidly
- Cyberattacks increasing in frequency, details remain scarce
- Expertise is essential to evaluate risks and investigate attacks

ROMAS moves engine room control to shore

June 11, 2019 in NAVIGATION AND AUTONOMOUS VESSELS



Kim Gunnar Jensen, project engineer at Fjord1, at the shore-based engine control centre used in the ROMAS project. PHOTO: Fjord1

1. https://smartmaritimenetwork.com/2019/06/11/romas-moves-engine-room-control-to-shore/

Thanks! …. Questions?