Cyber – The Ongoing Evolution

American Institute of Marine Underwriters (AIMU)
10 May 2017

USMRC
UNITED STATES MARITIME RESOURCE CENTER

Today's Discussion

- **CYBER – The On-Going Evolution - Do we understand the exposure?**
- **Does current *wording* work?**
- **Understanding Cyber Security and E-Navigation**
- The Digitization of Maritime
- The Problem to be Solved and Why We Should Care
- Our Research – the Bottom-Up Approach
- What We Have Found (Understanding the Exposure)
- Case Studies
- Completing the Digital Transformation
- Initiatives
- Regulation Approaching?
- Summary

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

The Digitization of Maritime

This is the biggest transformation of the maritime industry since the invention of the sea container - 1956

- “The Box” changed the world – global trade, intermodal transport, and access to any country
- Streamlined the global supply chain – efficiency and optimization

Connecting shore with the global maritime commons

- Information sharing, data collection, remote access and maintenance
- Efficiency, optimization, and safety
- Marine terminal operations with minimal human physical exposure

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

The Problem to be Solved

Reliance and dependency on rapidly evolving and innovative technologies

- Decisions are increasingly enabled by digitization – ***changes in the Human-Machine Interface (HMI)***
- Some decisions are mostly digital with little or no human “trust but verify” process, and no “manual” option
- Some vessel systems are ***mandated for carriage by the IMO*** – ECDIS, VDR, and (soon) BWM

Cyber is inherently vulnerable

- More technology in operations = greater vulnerability
- Likelihood of disruptions of significant impact to operations, business, and safety is increasing.
- Very limited incident data or reports on Marine Physical Loss

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

The Exposure to Cyber Risk…

…is long-proven and well-known across all other industries, so why don't we call it like it is in maritime?

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Words Drive Acceptance

- *Words like "hack" and "attack" focuses the attention on the malicious, but not the big picture.*
- Limited C-Suite acceptance of maritime cyber as a risk
- What reporting will be sufficient to change minds?
- Security and resilience is only as good as the management and governance behind it.
- Clause 380 – How will excluding losses to cyber disruption help the shipowner?

"Cyber has not yet presented tangible risk, unlike other maritime risks, and does not have sufficient reporting to change minds of the shipowners. However, this can be seen as a systemic risk, which may require a different approach."

- Loss Prevention Committee member (IUMI) to USMRC, 2015

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Maritime Operational Technology

USMRC
UNITED STATES MARITIME RESOURCE CENTER

Modern Navigation Bridge

Modern Engine Control Room

Greater Human Dependency/Trust in Technology

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Modern Terminal Operations

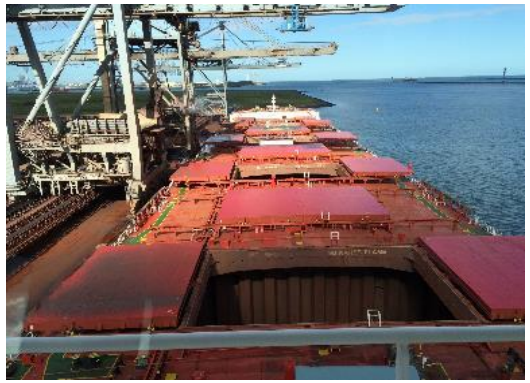
Rapid Increase in Automation and Remote Control

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Maritime Cyber Assurance℠ Research

USMRC
UNITED STATES MARITIME RESOURCE CENTER

- **Evidence-based research is a bottom-up approach** to develop a platform of verifiable facts from which to build Maritime Cyber Assurance℠ strategies
- **Maritime Cyber Assurance Team (MCAT)** comprised of highly credentialed senior mariners, terminal operations professionals, cyber security professionals – integrated with industry research sponsors
- **Support and partnerships** at the highest levels of shipping.



BIMCO

LIBERIAN REGISTRY

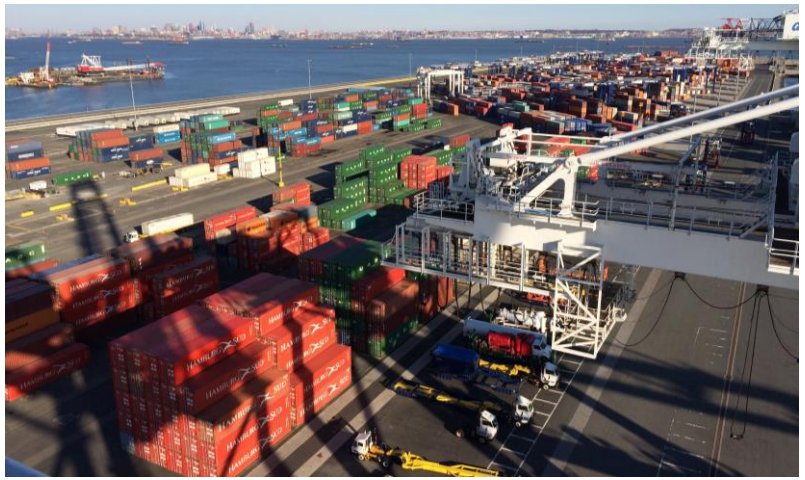
ClassNK

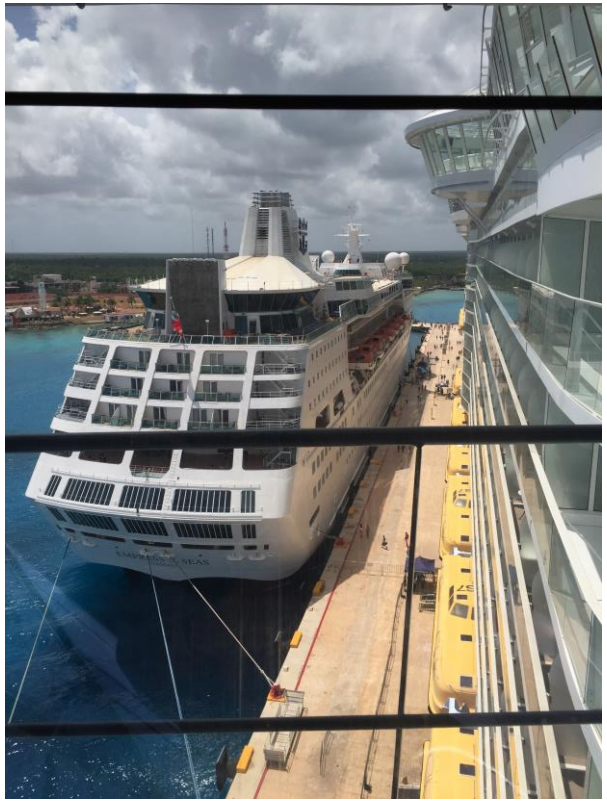
INTERDISCIPLINARY CONSORTIUM for IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (IC)³

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Results and Achievements

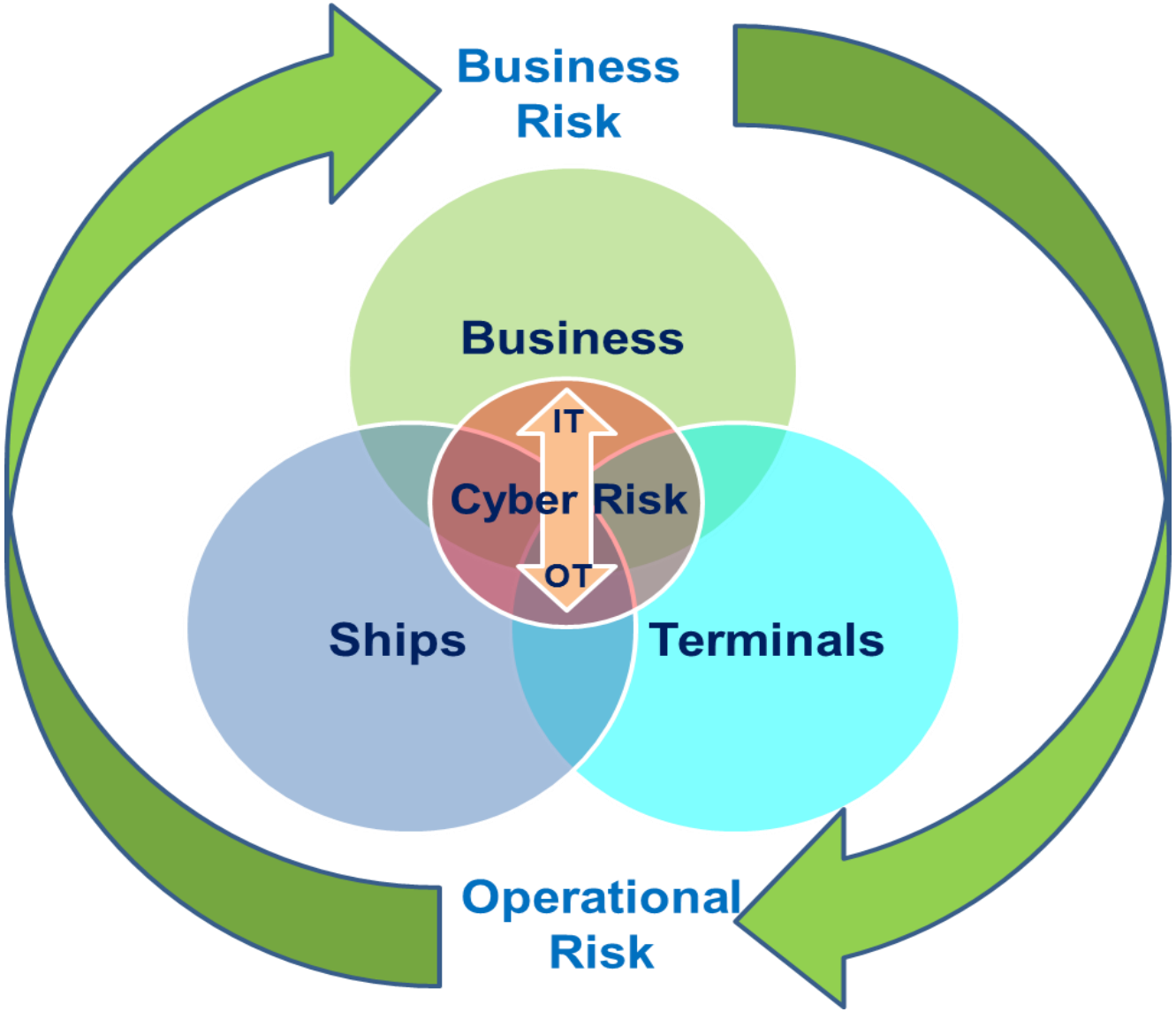
- Conducted first penetration testing of an automated container terminal
- Cruise line assessment – first for marine systems
- Advisory project supporting shipowner and critical marine systems OT vendor
- First to develop Cyber Awareness for Mariners online training course





Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

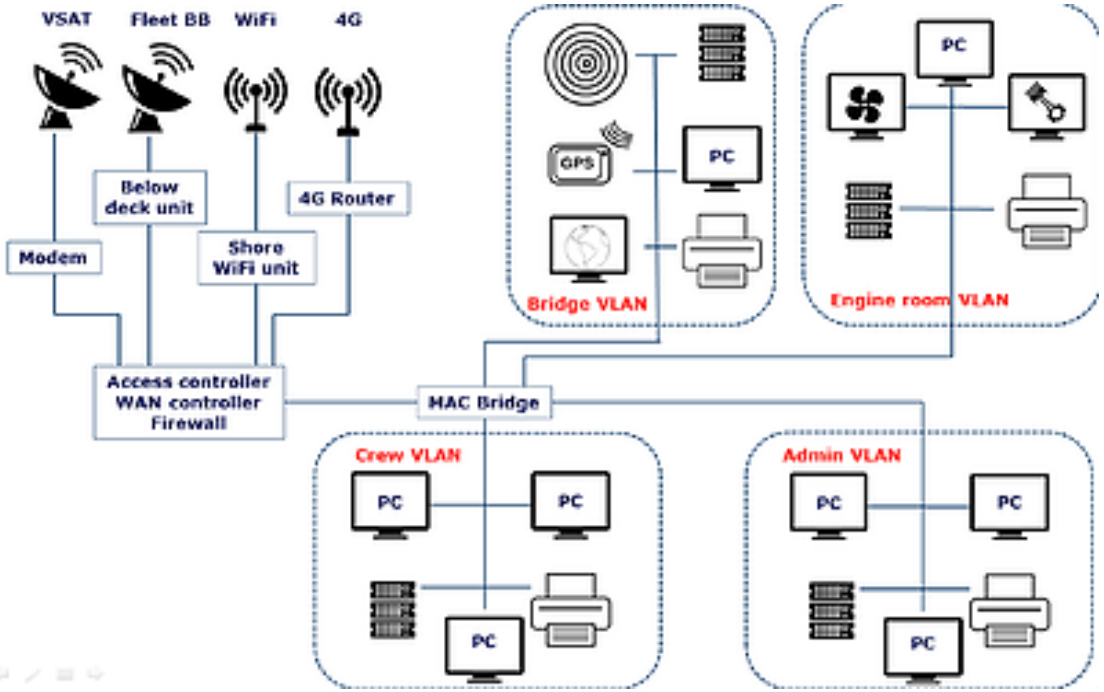
Holistic Approach



Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

The OT and the IT

- Navigation systems
- Engineering systems
- Safety systems
- Cargo management
- Administrative LAN
- Satellite provider
- Specialized systems
- Stability and load condition monitoring
- Weather routing and other applications



Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

What We Have Learned - Old News

Common Vulnerabilities

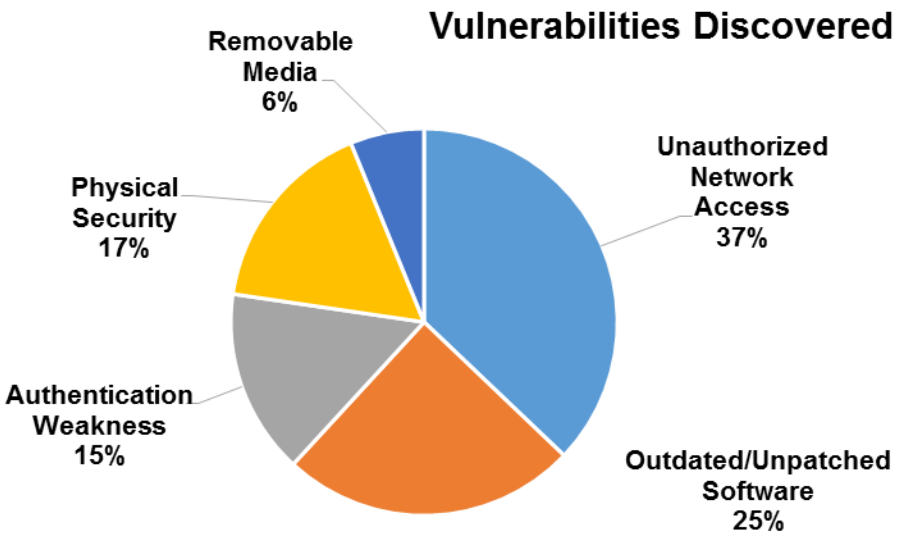
- Little evidence of cyber policy
- **Unsupported/obsolete/unpatched operating systems**
- Unauthenticated/bypassed workstation or system access
- Dangerous crew modifications
- Ad hoc and flat networks
- **Critical systems connected to the internet without boundaries or segregation**
- **Network connected Industrial Control Systems (ICS) to vendors with unknown security assurance**

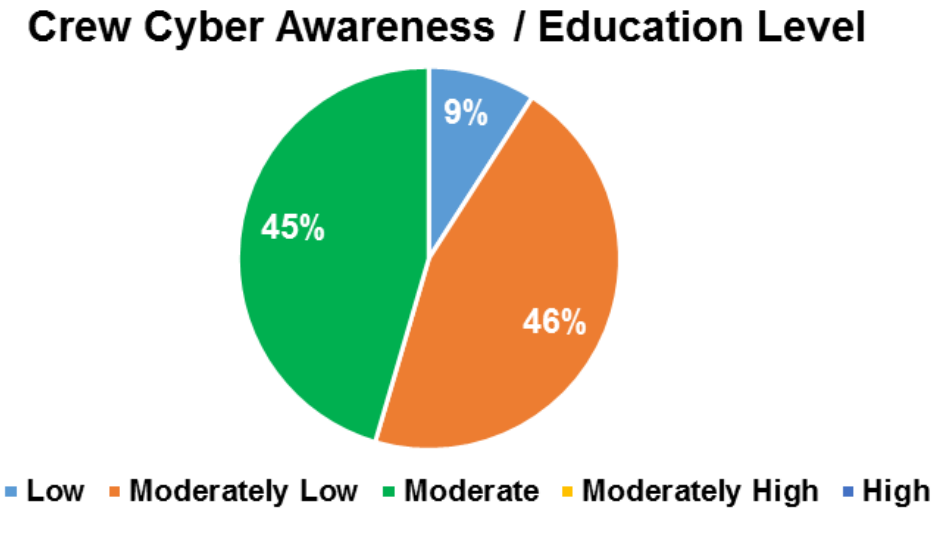
Common Vulnerable Practices

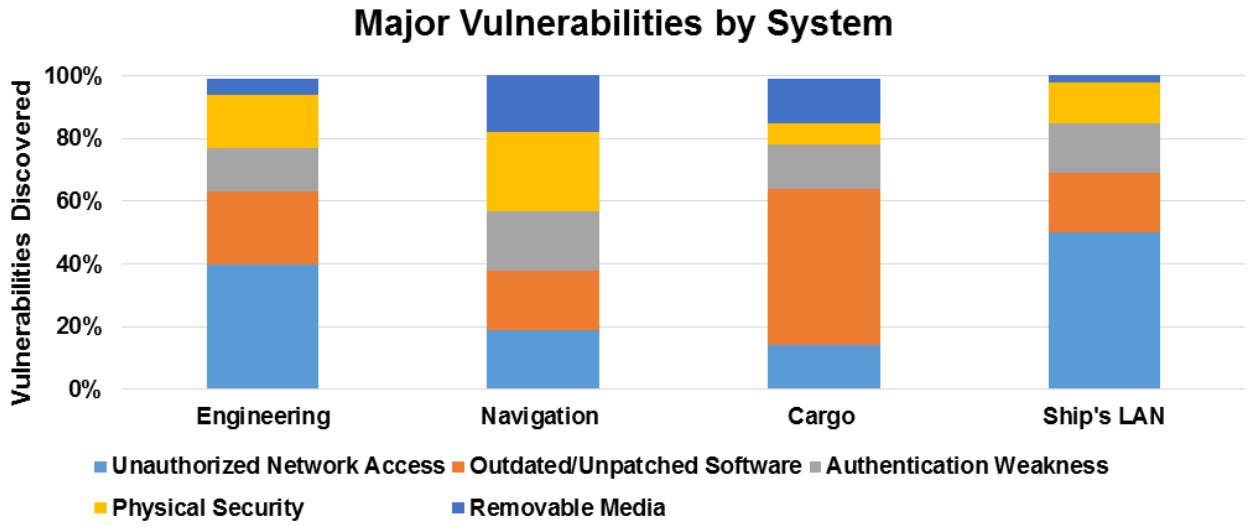
- **External vendors and third parties have access to shipboard computers**
- False belief that vessel is not connected or systems are “air gapped”
- **Poor file transfer processes, often using USB drives that have not been scanned**
- ***Acceptance*** of cyber risk is low at the C-level
- **No IT lifecycle management for IT-based systems**

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Research Data







Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Incidents – Not All Are Intentional!!!

2016 to Present

- Four reported ransomware attacks on US-flag vessels; numerous malware and ransomware across maritime businesses internationally
- Three reported cases of navigation system crashes due to obsolete operating systems – I was present for one of them
- Two cases in which malware infected ECDIS on ships with “paperless” navigation – resulted in costly delays
- Very recent case where the owner’s cyber team discovered a dormant worm in a critical marine system that was to be connected for remote access – vigilance and investment in security saved them between $5M and $10M in a reportable marine loss, and unknown secondary and tertiary costs.

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

NIST Framework Core

What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?

Function	Category	Category Unique ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory
ID.BE-1: The organization's role in the supply chain is identified and communicated
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
ID.BE-4: Dependencies and critical functions for delivery of critical services are established
ID.BE-5: Resilience requirements to support delivery of critical services are established

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Scenario 1 - Hackers take control

- **Crew operates Main engineering consoles with ADMIN account permissions**
  - Ability to install software and reconfigure the systems at will
- **3rd party remote control software was installed**
  - Likely to enable remote maintenance
  - Connection to ship's mess where seating was more comfortable
  - Potential for uncoordinated or malicious remote access
- **Persistent unauthorized internet connection to Engineering Control Console (ECC)**
  - Engineering controls are accessible to global malicious actors and incidental automated attacks.
  - Crew could browse internet websites on the ECC

Cascading effects of multiple system vulnerabilities on a modern vessel

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Scenario 1

- **Operational Impact -** Degraded/denied engineering functions. Loss of engine control on the ship. Engine casualties could be induced from a remote actor. Could threaten the vessels safe operation if the engineering casualty induced occurred in a restricted maneuvering environment.
- **Business Impact -** Engines and auxiliary systems could be damaged resulting in significant financial loss from repairs and vessel layup.

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Scenario 2 - Data Access

- **Widespread Exposure of Critical Data and Systems -** Rudimentary IT infrastructure leads to widely shared risk across operations. Malware spreads faster and has more effect when there are no network segregation boundaries or security barriers. Lack of crew cyber awareness enables access to an entire ship's network and data.
  - **Ad-hoc networks -** Evidence of ad-hoc networks on the ship's LAN. No network or baseline documentation exists to justify existence of these multiple networks.

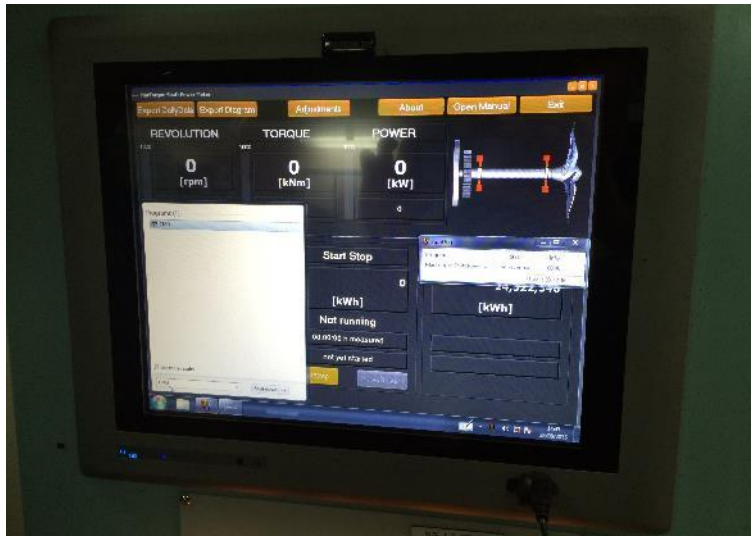
- This issue was prevalent throughout the assessments
- Can proliferate from IT to OT.

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Scenario 2

- **Operational Impact -** Deliberate or unintentional release of operational information (navigation, cargo, bunkering, stability, etc.), could lead to onboard disruption. An increasing number of opportunities for malware insertion to a network exist which could lead to loss of all ship's administrative data.

- **Business Impact -** Unauthorized access to network. This type of access can be a key factor in the exploitation of information via social engineering of crew members and use of their network access.



Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Completing the Digital Transformation

Sea Traffic Management, e-Navigation, and the Maritime Cloud

- Voyage planning, route exchange, and voyage optimization
- Harmonized information and data exchange
- ***Driven by safety – to reduce accidents***
- ***"Collaborative decision-making"***

These are regional initiatives – what about the US?

Changes in maritime training? When?

How will global cyber networks prove resilience and security?

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Approaching Regulation?

IMO Interim Guidelines on Maritime Cybersecurity Risk Management

- MSC 98 June 2017 – will be ratified – no longer “interim”
- Voluntary guidelines? If this is new compliance, what are the consequences?

Cyber to be included in the ISM Code?

- US Letter to the IMO, 3 APR 2017
- IMO MSC 98 discussions

Cyber and the Maritime Transportation Security Act (MTSA)

- EO 13636 – Improving Critical Infrastructure Cybersecurity
- Pending USCG NVIC – to be released soon
- **Facilities and marine terminals subject to MTSA**

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Advice for the Shipowner/Insureds

Commit to understanding the problem – prioritize cyber

- Beyond corporate responsibility – its about doing the right thing!
- Unify your senior management around cyber – it can be done!
- Conduct baseline cyber assessments and periodic follow-on assessments
- Talk to your technology vendors and obtain assurance
- Identify your resources and build strategies and governance.
- Due diligence: seek outside help, hire staff, partner with others
- Talk to your charterers, insurance, P&I, crewing companies, flag state, class society, associations, etc.

The value of investing in cyber is obvious

- Life, property, and the environment
- **Don’t wait for an incident or regulation!!!**

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Summary

Cyber is inherently vulnerable

- *The risk is real and tangible – Clause 380 is problematic for the shipowner who has invested in cyber risk management*
- Cybersecurity and resilience likely to be in the accident error chain
- Greater need for an intellectual commitment to understanding cyber
- C-level acceptance critical across industry and dependent businesses

Dependency on technology and the changing Human-Machine Interface

- Over-reliance and weaknesses in “trust but verify” likely to be in the accident error chain (complacency already is…)
- Automated, remote, and digitally assisted decisions
- **Rapid advancements in innovation (through government partnerships) don’t include the same partnerships with government for security – e-Navigation/STM as examples.**

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.

Thank you!

Contact:

Captain Alex Soukhanov

www.usmrc.org

alex.soukhanov@usmrc.org

Office: +1 401 849 0222

Copyright © 2016 United States Maritime Resource Center, Inc. All Rights Reserved.