Unravelling the myth around cybersecurity:

A system-of-systems analysis of the ship's ecosystem

Digital Ship
ATHENS CONFERENCE
13 & 14 November 2019

Chronis Kapalidis
Associate Fellow, Chatham House
Researcher, Cybersecurity Centre, WMG, University of Warwick
Europe Representative, Hudson Cyber, Hudson Trident UK

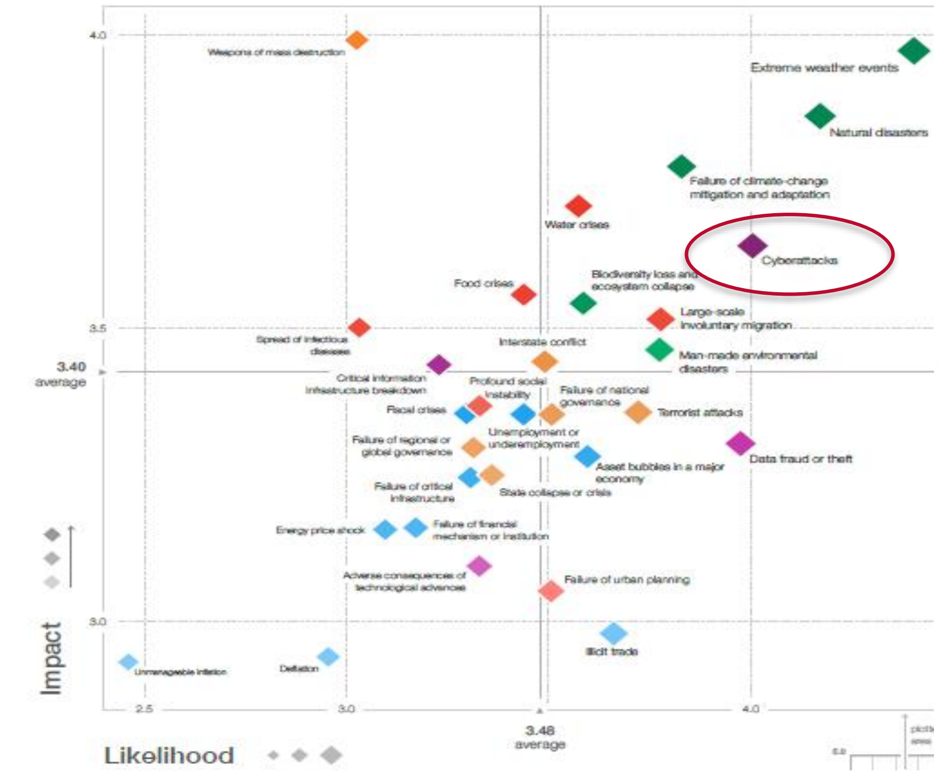
CHATHAM HOUSE
The Royal Institute of International Affairs

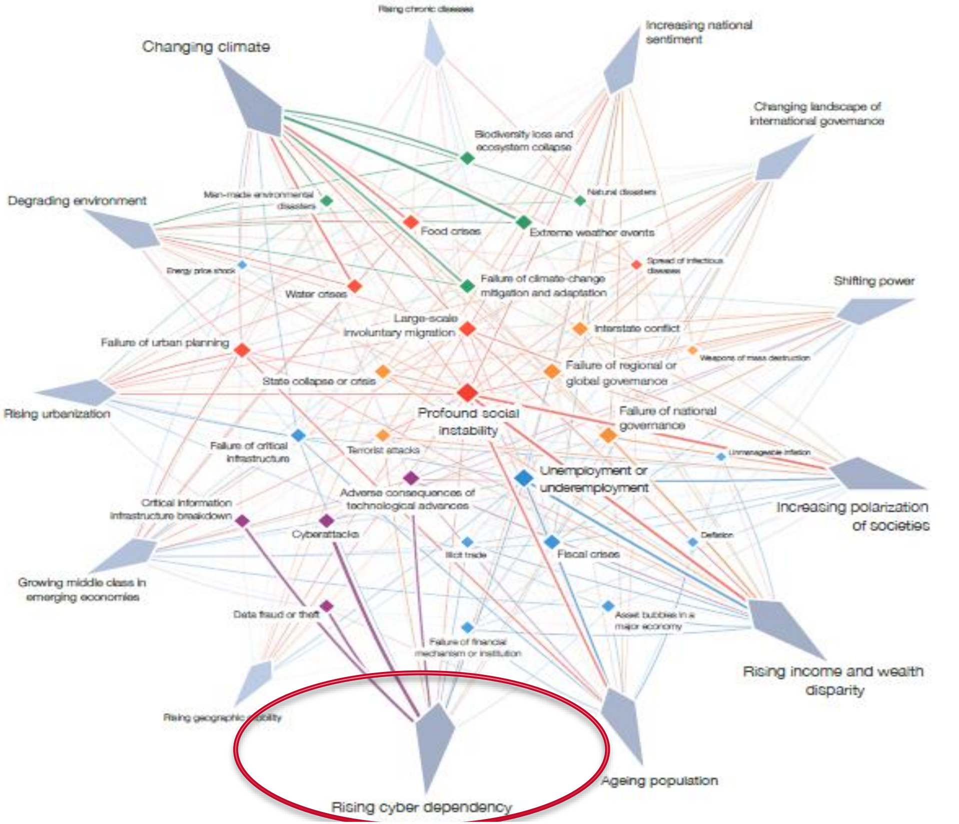
WMG
THE UNIVERSITY OF WARWICK

HudsonCyber
Managing Cyber Risk

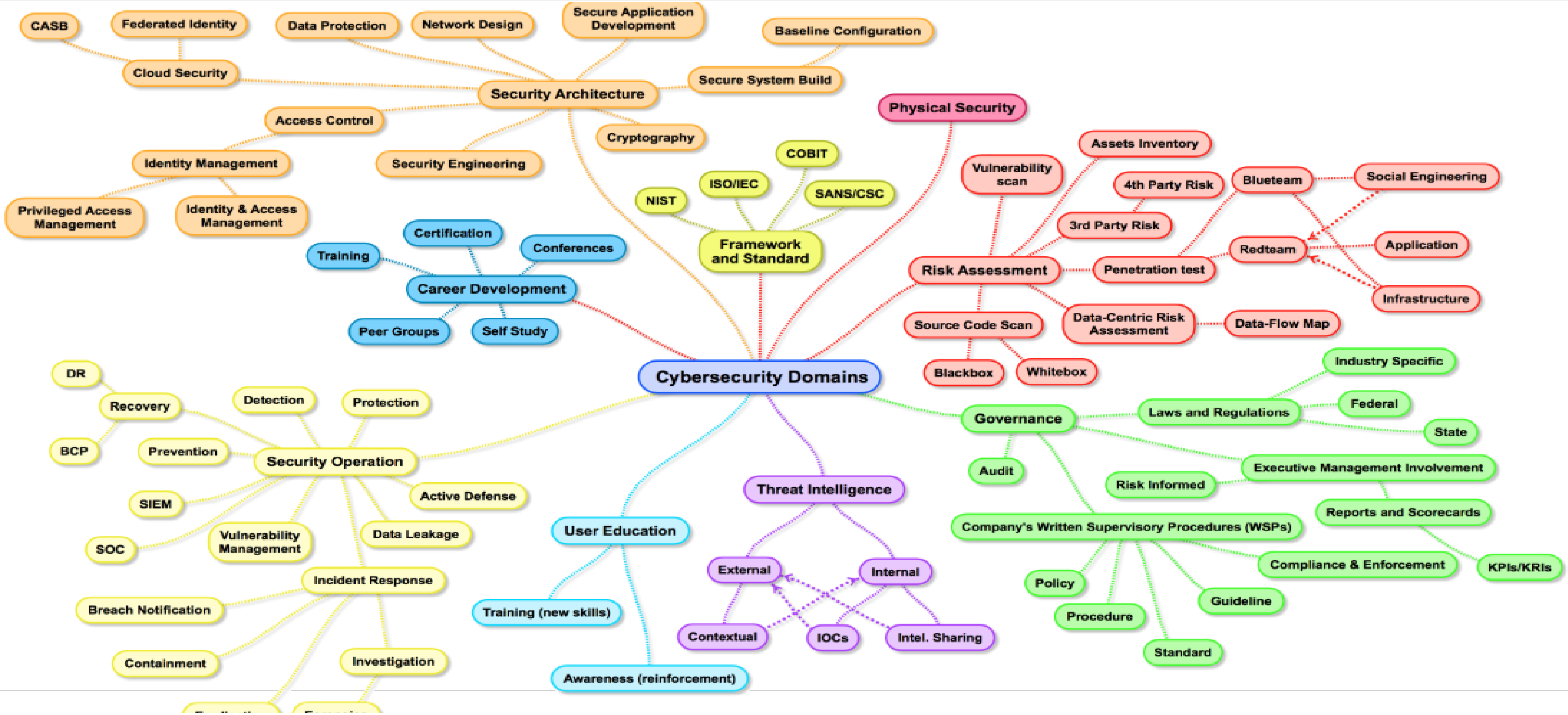
World Economic Forum Report 2018

Figure I: The Global Risks Landscape 2018




Rising chronic diseases
Increasing national sentiment
Changing climate
Changing landscape of international governance
Biodiversity loss and ecosystem collapse
Degrading environment
Man-made environmental disasters
Natural disasters
Food crises
Extreme weather events
Energy price shock
Spread of infectious diseases
Failure of climate-change mitigation and adaptation
Water crises
Shifting power
Large-scale involuntary migration
Interstate conflict
Failure of urban planning
Weapons of mass destruction
Failure of regional or global governance
State collapse or crisis
Rising urbanization
Profound social instability
Failure of national governance
Failure of critical infrastructure
Terrorist attacks
Unmanageable inflation
Unemployment or underemployment
Increasing polarization of societies
Adverse consequences of technological advances
Critical information infrastructure breakdown
Cyberattacks
Deflation
Illicit trade
Fiscal crises
Growing middle class in emerging economies
Data fraud or theft
Asset bubbles in a major economy
Failure of financial mechanism or institution
Rising income and wealth disparity
Rising geographic mobility
Ageing population
Rising cyber dependency

The cyber domains



- Cybersecurity Domains
  - Security Architecture
    - Cloud Security
      - CASB
      - Federated Identity
    - Data Protection
    - Network Design
    - Secure Application Development
    - Secure System Build
      - Baseline Configuration
    - Access Control
      - Identity Management
        - Privileged Access Management
        - Identity & Access Management
    - Cryptography
    - Security Engineering
  - Framework and Standard
    - NIST
    - ISO/IEC
    - COBIT
    - SANS/CSC
  - Physical Security
  - Risk Assessment
    - Vulnerability scan
    - Assets Inventory
    - 3rd Party Risk
      - 4th Party Risk
    - Penetration test
      - Blueteam
      - Redteam
        - Social Engineering
        - Application
        - Infrastructure
    - Source Code Scan
      - Blackbox
      - Whitebox
    - Data-Centric Risk Assessment
      - Data-Flow Map
  - Career Development
    - Training
    - Certification
    - Conferences
    - Peer Groups
    - Self Study
  - Governance
    - Laws and Regulations
      - Industry Specific
      - Federal
      - State
    - Executive Management Involvement
      - Risk Informed
      - Reports and Scorecards
        - KPIs/KRIs
    - Audit
    - Company's Written Supervisory Procedures (WSPs)
      - Policy
      - Procedure
      - Standard
      - Guideline
      - Compliance & Enforcement
  - Security Operation
    - Detection
    - Protection
    - Prevention
    - Recovery
      - DR
      - BCP
    - Active Defense
    - SIEM
    - SOC
    - Vulnerability Management
    - Data Leakage
    - Incident Response
      - Breach Notification
      - Containment
      - Investigation
  - User Education
    - Training (new skills)
    - Awareness (reinforcement)
  - Threat Intelligence
    - External
    - Internal
    - Contextual
    - IOCs
    - Intel. Sharing

CYBERSECURITY AND SHIPPING

IT vs. OT: What is the Difference?

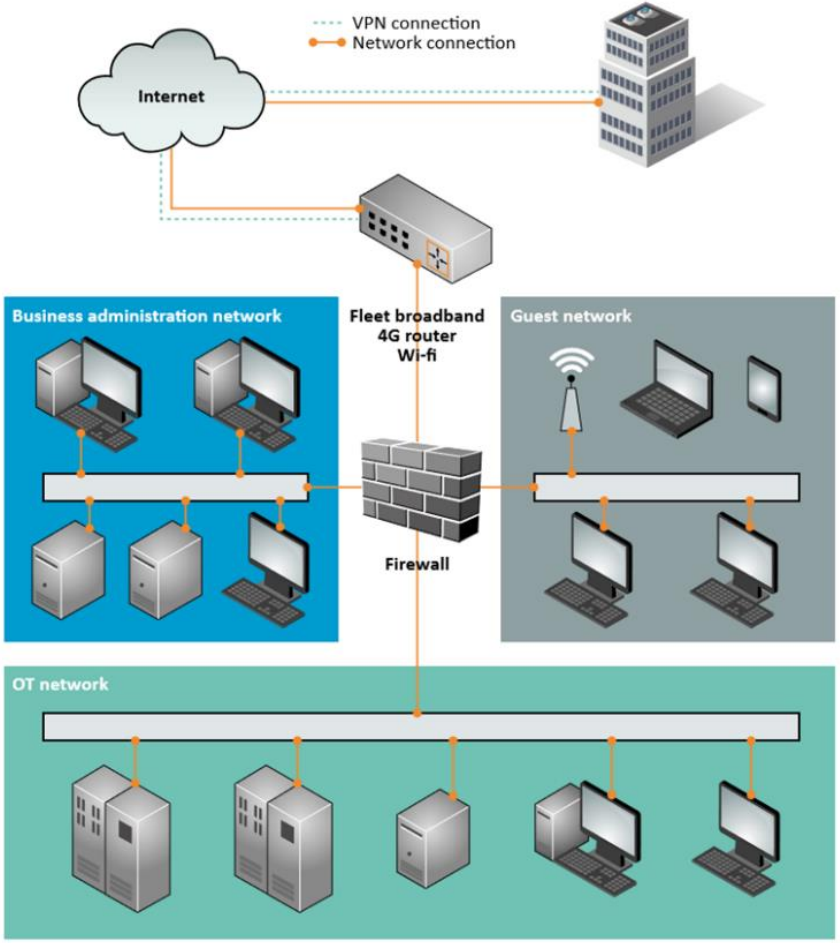
Informational Technology

- Dynamic data capture, continuous transformation of data, highly variable outcomes, and data reporting is analytical
- Potential for many variable access routes to systems
- Confidentiality, Integrity, Availability (CIA)
- Regular System Updates are the norm; they are designed for change

Operational Technology

- Process control, static operations, change is controlled, consistent performance, reporting is historical
- Limited highly controlled access routes to systems
- Control, Availability, Integrity, Confidentiality, Effectiveness, Trustworthiness, Safety
- Rare System Updates; availability and control are limiting factors in changes

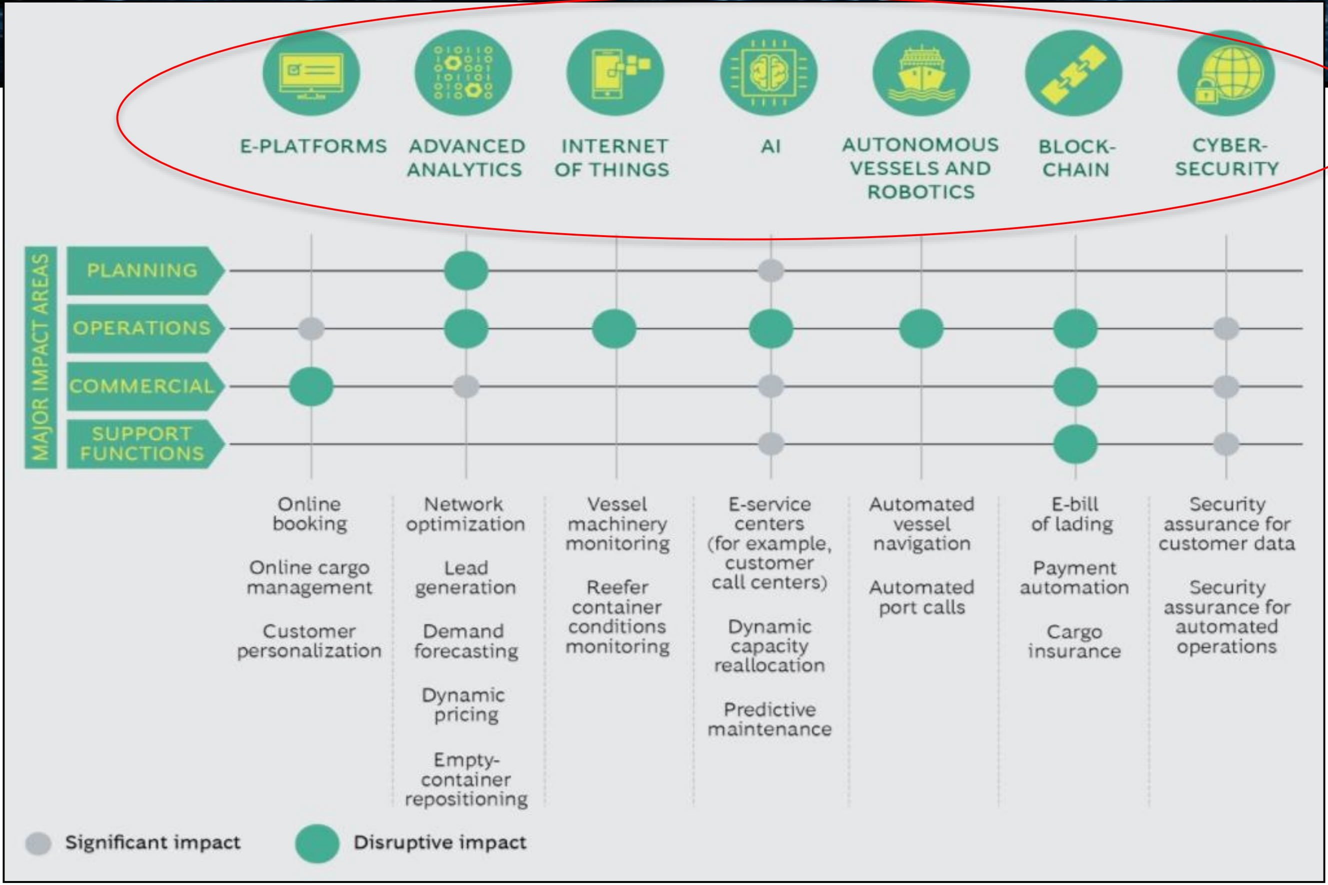
Typical shipboard network configuration



IT / OT convergence…. The unknown unknowns….

(Source BIMCO)

7 Digital Trends Transforming Shipping

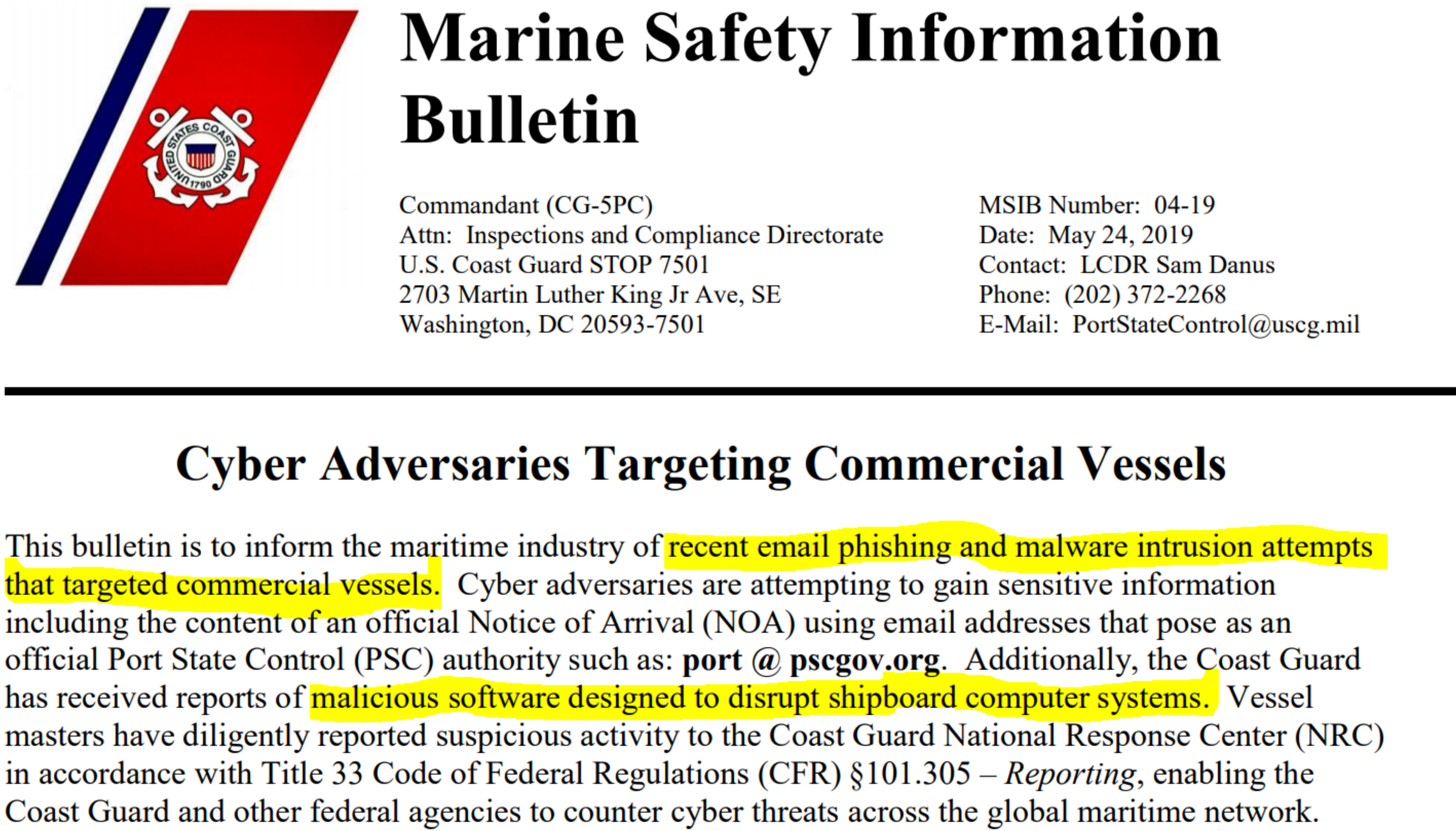


MAJOR IMPACT AREAS

	E-PLATFORMS	ADVANCED ANALYTICS	INTERNET OF THINGS	AI	AUTONOMOUS VESSELS AND ROBOTICS	BLOCK-CHAIN	CYBER-SECURITY
PLANNING		●		○			
OPERATIONS	○	●	●	●	●	●	○
COMMERCIAL	●	○		○		●	○
SUPPORT FUNCTIONS				○		●	○
	Online booking Online cargo management Customer personalization	Network optimization Lead generation Demand forecasting Dynamic pricing Empty-container repositioning	Vessel machinery monitoring Reefer container conditions monitoring	E-service centers (for example, customer call centers) Dynamic capacity reallocation Predictive maintenance	Automated vessel navigation Automated port calls	E-bill of lading Payment automation Cargo insurance	Security assurance for customer data Security assurance for automated operations

○ Significant impact ● Disruptive impact

Source: BCG Analysis



Marine Safety Information Bulletin

Commandant (CG-5PC)
Attn: Inspections and Compliance Directorate
U.S. Coast Guard STOP 7501
2703 Martin Luther King Jr Ave, SE
Washington, DC 20593-7501

MSIB Number: 04-19
Date: May 24, 2019
Contact: LCDR Sam Danus
Phone: (202) 372-2268
E-Mail: PortStateControl@uscg.mil

Cyber Adversaries Targeting Commercial Vessels

This bulletin is to inform the maritime industry of recent email phishing and malware intrusion attempts that targeted commercial vessels. Cyber adversaries are attempting to gain sensitive information including the content of an official Notice of Arrival (NOA) using email addresses that pose as an official Port State Control (PSC) authority such as: **port @ pscgov.org**. Additionally, the Coast Guard has received reports of malicious software designed to disrupt shipboard computer systems. Vessel masters have diligently reported suspicious activity to the Coast Guard National Response Center (NRC) in accordance with Title 33 Code of Federal Regulations (CFR) §101.305 – *Reporting*, enabling the Coast Guard and other federal agencies to counter cyber threats across the global maritime network.

RESEARCH FINDINGS: A SoSA OF THE SHIP'S ECOSYSTEM

CHATHAM HOUSE
The Royal Institute of International Affairs

HudsonCyber
Managing Cyber Risk

Deck Systems	Engine Systems
Signal Light Column	Engine Control Room
Anchor and Mooring Winch Control	Switchboards
Internal Comms	Bow Thruster Control
Crew Entertainment	Water Ingress Detection
GMDSS Console	Alarm and Monitoring Control
Fleet Management	Power Management
Navigation Equipment	Cabling
Bridge Control Console	
VDR/S-DR	
Electrical Crane Equipment	
Reefer Container Monitoring	
Navigation Lights	
Loading and Stability Computer	

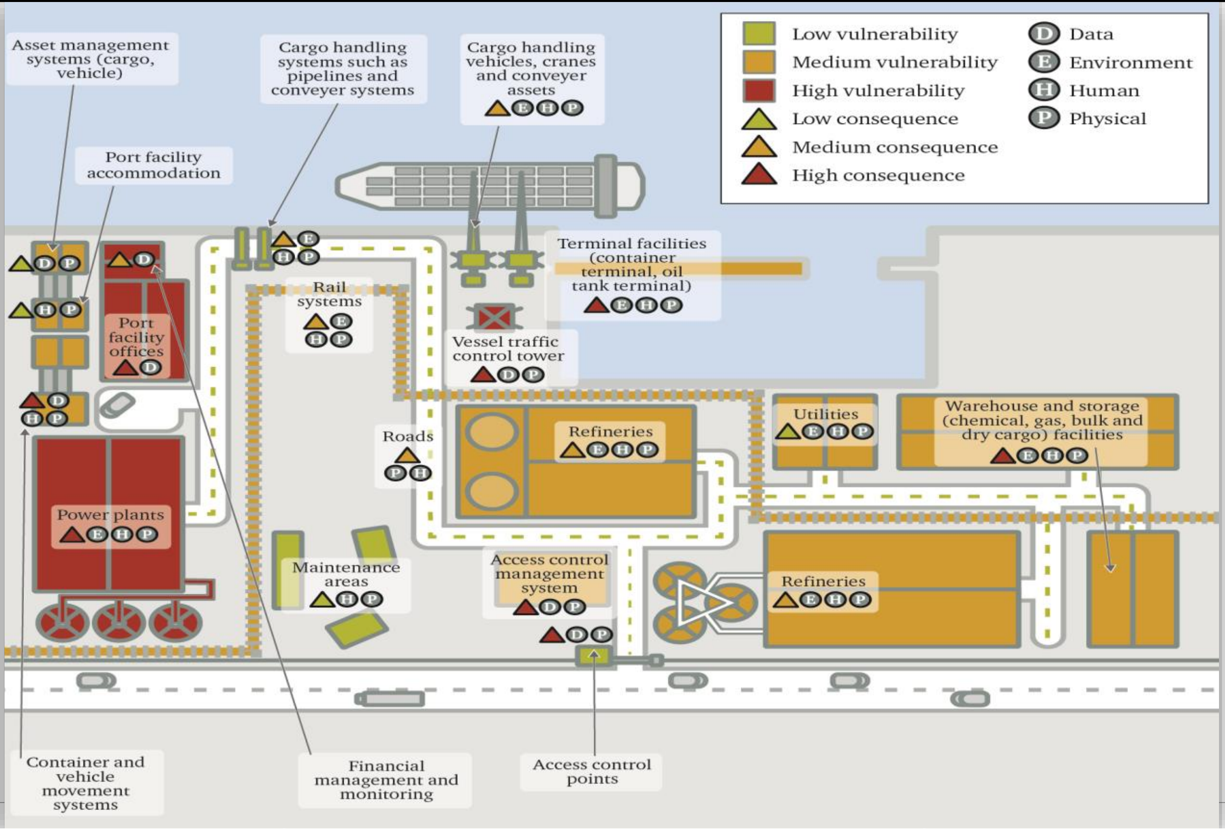
Period: Oct 17 – Feb 19

Research Method: SoSA - Interviews

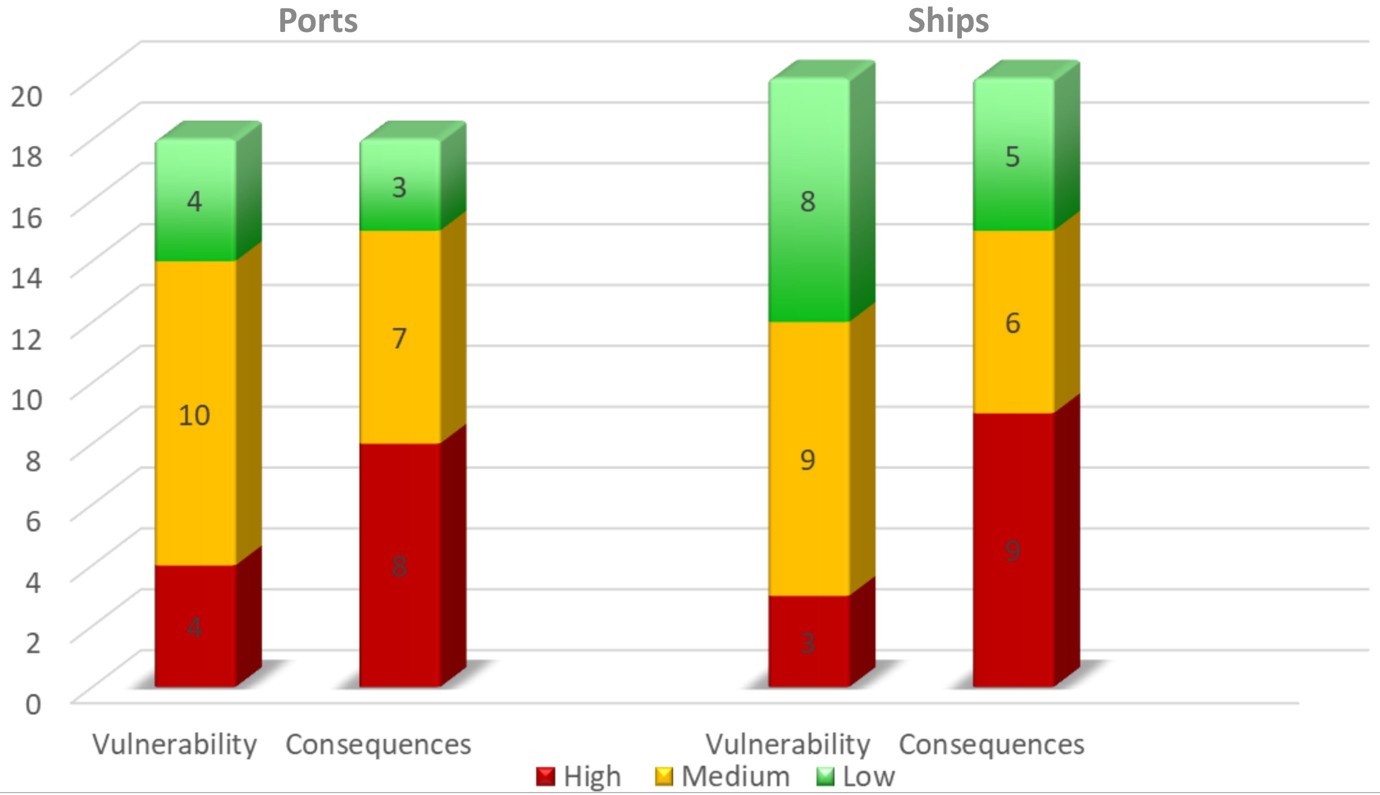
UoA: 18 port sub'nts
20 ship sub'nts

AoR: Vulnerability
Consequences
Affected Fields

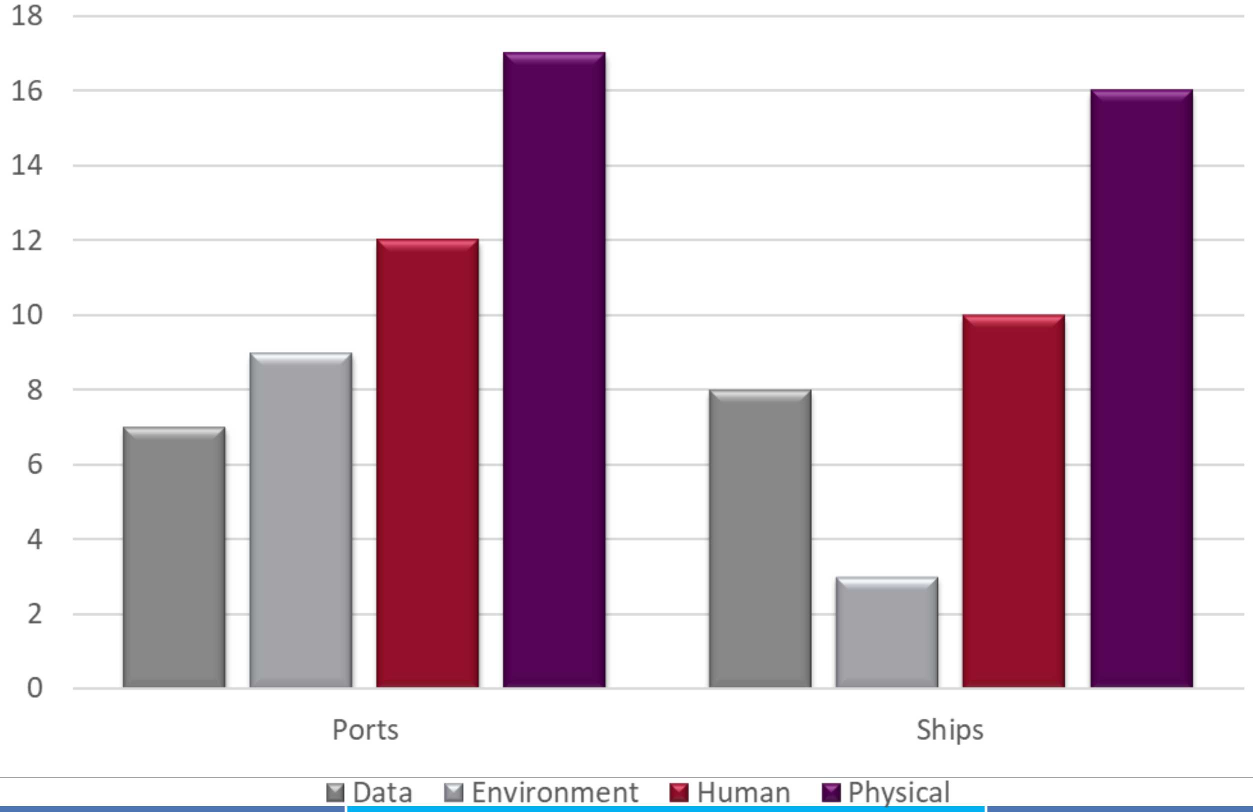
Port’s cybersecurity ecosystem


Low vulnerability
Medium vulnerability
High vulnerability
Low consequence
Medium consequence
High consequence
D Data
E Environment
H Human
P Physical
Asset management systems (cargo, vehicle)
Cargo handling systems such as pipelines and conveyer systems
Cargo handling vehicles, cranes and conveyer assets
E H P
Port facility accommodation
D P
H P
D
Port facility offices
D
D
H P
E
H P
Rail systems
E
H P
Terminal facilities (container terminal, oil tank terminal)
E H P
Vessel traffic control tower
D P
Roads
P H
Refineries
E H P
Utilities
E H P
Warehouse and storage (chemical, gas, bulk and dry cargo) facilities
E H P
Power plants
E H P
Maintenance areas
H P
Access control management system
D P
D P
Refineries
E H P
Container and vehicle movement systems
Financial management and monitoring
Access control points

Chatham House Maritime Cybersecurity Research 2019: Vulnerabilities & Consequences

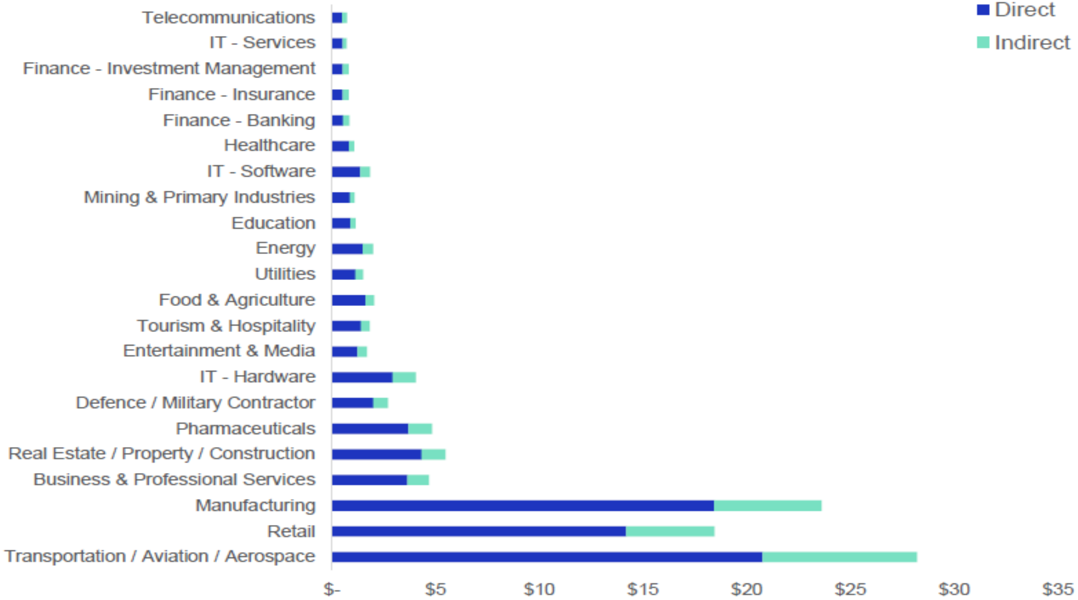


Chatham House Maritime Cybersecurity Research 2019: Affected Fields

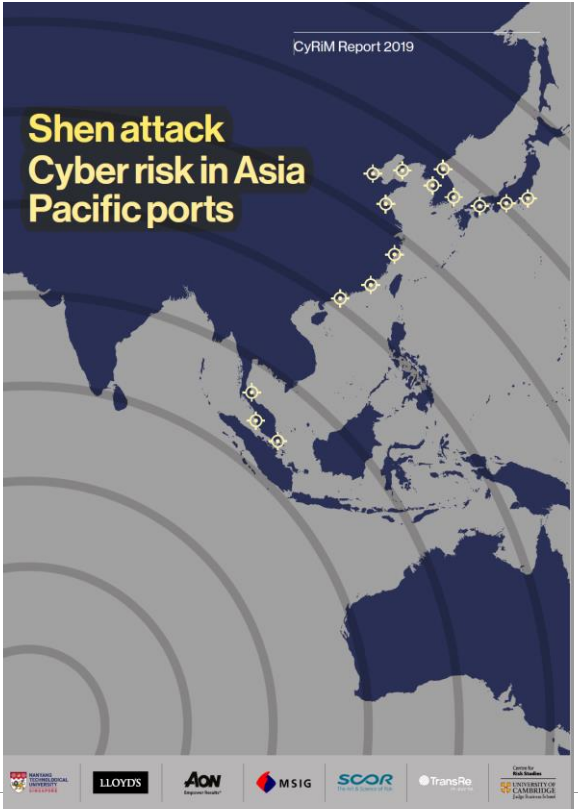


It is all about the maritime supply chain risk….

Figure 1: Total global direct and indirect economic losses by sector for scenario variant X1



Economic damage to the world economy on 15 Asian ports:
from **$40.8** to **$109.8** billion



CyRiM Report 2019

Shen attack
Cyber risk in Asia
Pacific ports

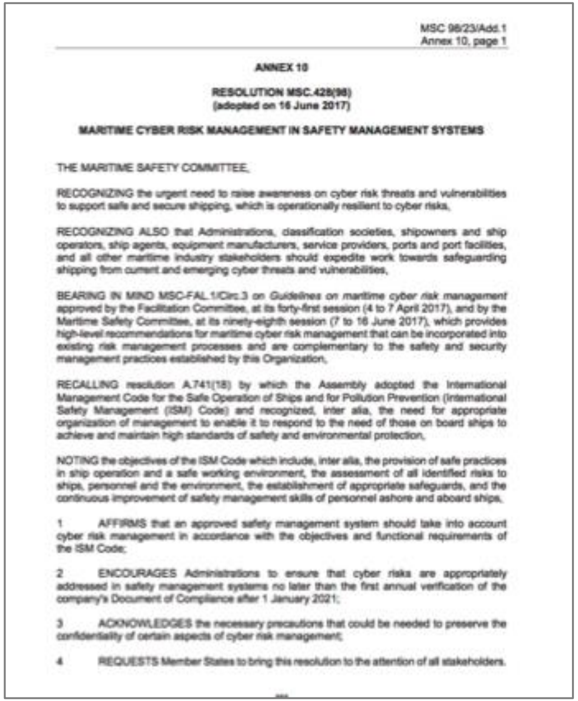
SO…. TECHNICAL OR MANAGEMENT ISSUE?

Cyber Risk Management and the IMO

Maritime Safety Committee (MSC), 98th session, 7-16 June – Media information

Resolution MSC.428 (98) Maritime Cyber Risk Management in Safety Management Systems affirms that:

- *Approved Safety Management Systems should take **cyber risk management** into account in accordance with the objectives and requirements of the ISM Code.*
- ***Existing risk management practices** should be used to address the operational risks associated with the growing dependence on cyber enabled systems.*



MSC 98/23/Add.1
Annex 10, page 1

ANNEX 10

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

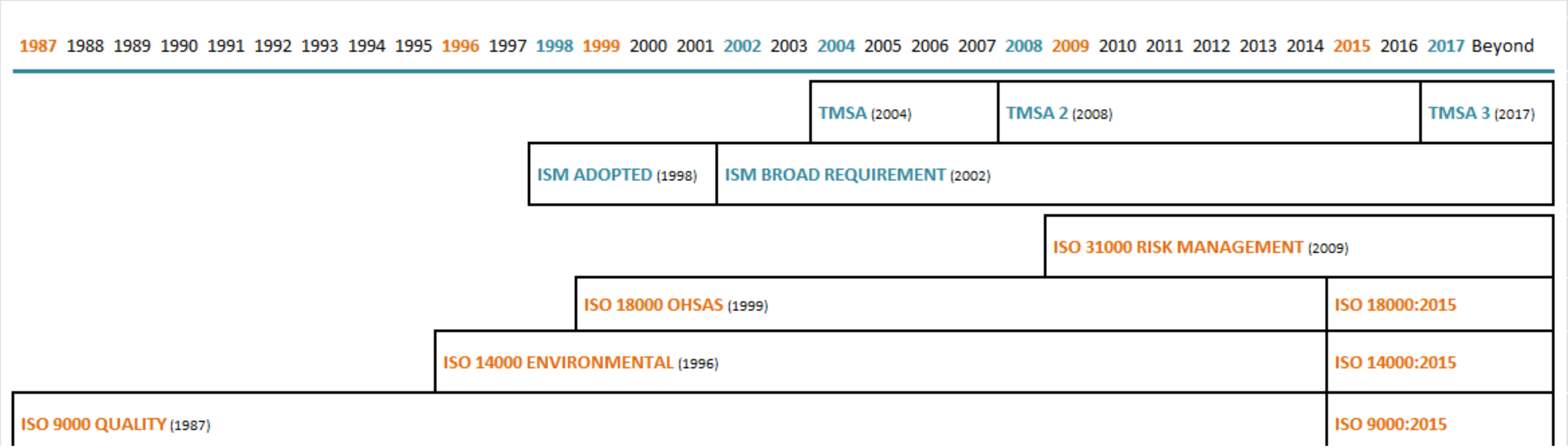
2 ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.

Regulation Drives Changes but so Does Risk

- **ISO** adopted the *Plan-Do-Check-Act* process for all standards in 2015; focusing on *continual improvement*.
- **ISM** uses risk identification and audit based prevention to ensure the focus is on *continual improvement*.
- **TMSA** introduced the *Plan-Act-Measure-Improve* cycle with relevant KPIs to



1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 Beyond

TMSA (2004) | TMSA 2 (2008) | TMSA 3 (2017)

ISM ADOPTED (1998) | ISM BROAD REQUIREMENT (2002)

ISO 31000 RISK MANAGEMENT (2009)

ISO 18000 OHSAS (1999) | ISO 18000:2015

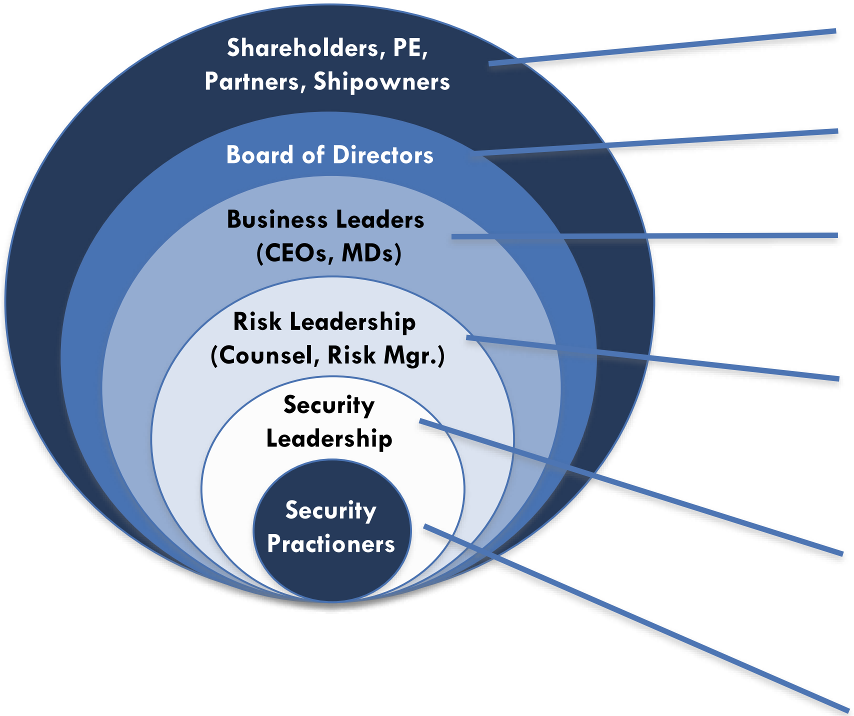
ISO 14000 ENVIRONMENTAL (1996) | ISO 14000:2015

ISO 9000 QUALITY (1987) | ISO 9000:2015

Re-Thinking Cyber Risk Management

- ✓ Consider cyber risk in terms of *money*
- ✓ *The cyber-risk-to-money intersection offers measurable value to inform resource prioritization*
- ✓ Financial grounding translates cyber risk into common language
- ✓ Empowers decision-makers with relevant context and inputs so as to make informed decisions on cyber risk

Who Owns Cyber Risk?



Shareholders, PE, Partners, Shipowners
Board of Directors
Business Leaders (CEOs, MDs)
Risk Leadership (Counsel, Risk Mgr.)
Security Leadership
Security Practioners

Evaluate and Fund Risk

(In terms of Investment decisions)

Evaluate and Fund Risk

(Minimize losses; support/protect shareholder equity)

Manage Risk

(Profit and Loss / Balance Sheet)

Identify, Prevent, Accept, and Transfer Risk

(Insurance; Agreements and Contracts *in terms of and risk to* Profit and Loss and Balance Sheet)

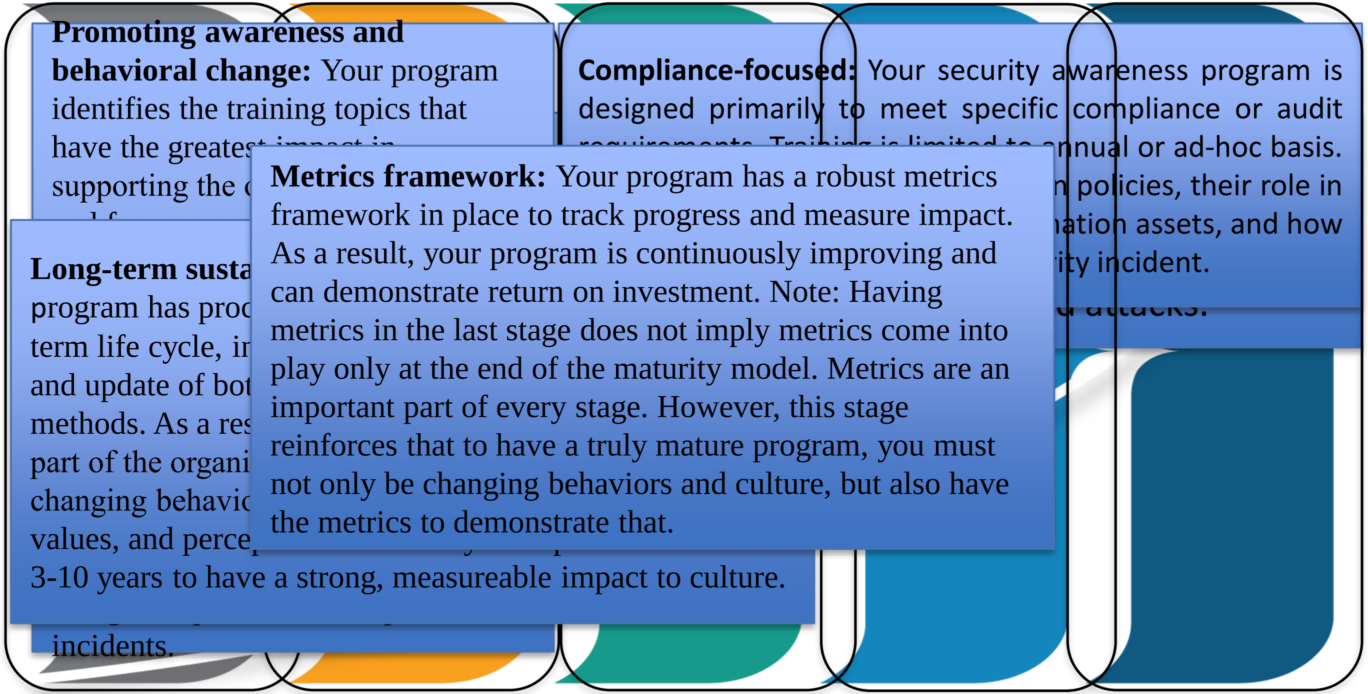
Validate Risk, Allocate Resources

(In terms of cyber risk to operations and Profit and Loss)

Communicate Needs, Solutions

(In terms of cyber *risk to* operations that

The Security Awareness Maturity Model™

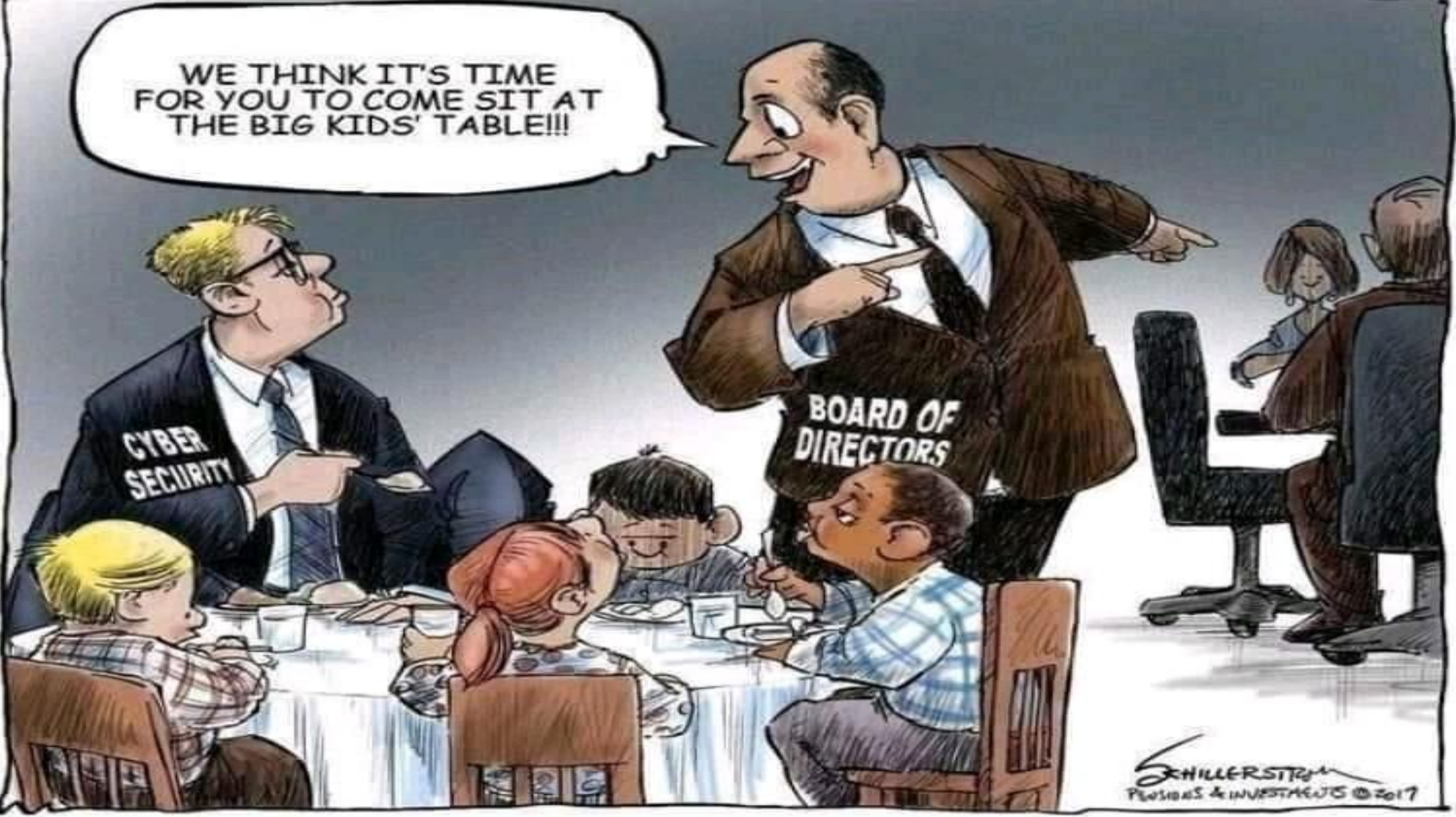


Promoting awareness and behavioral change: Your program identifies the training topics that
have the greatest impact in
supporting the o
incidents.

Compliance-focused: Your security awareness program is designed primarily to meet specific compliance or audit requirements. Training is limited to annual or ad-hoc basis.
n policies, their role in
ation assets, and how
ity incident.
d attacks.

Long-term susta
program has proc
term life cycle, i
and update of bot
methods. As a res
part of the organi
changing behavio
values, and perce
3-10 years to have a strong, measureable impact to culture.

Metrics framework: Your program has a robust metrics framework in place to track progress and measure impact. As a result, your program is continuously improving and can demonstrate return on investment. Note: Having metrics in the last stage does not imply metrics come into play only at the end of the maturity model. Metrics are an important part of every stage. However, this stage reinforces that to have a truly mature program, you must not only be changing behaviors and culture, but also have the metrics to demonstrate that.


WE THINK IT'S TIME FOR YOU TO COME SIT AT THE BIG KIDS' TABLE!!!
CYBER SECURITY
BOARD OF DIRECTORS
SCHILLERSTROM
PENSIONS & INVESTMENTS © 2017