Securing shipping during the pandemic

Cybersecurity challenges in shipping

HudsonCyber
Managing Cyber Risk

caribbean shipping association

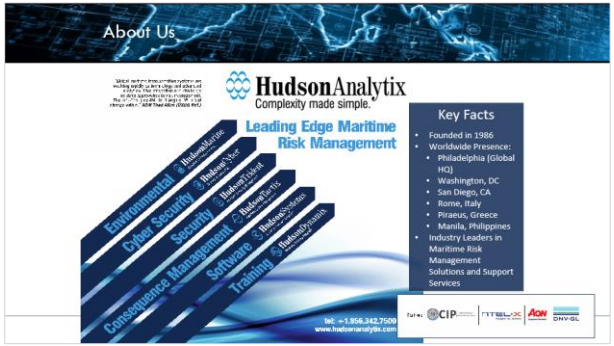
AON

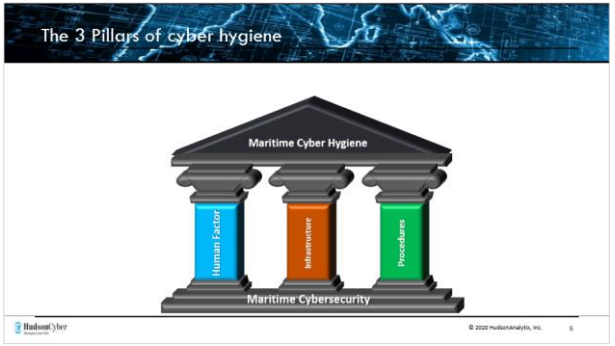
enisa European Union Agency for Network and Information Security

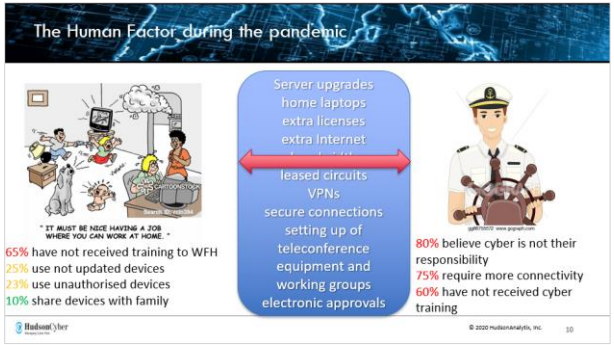
Official Service provider

Chronis Kapalidis, Hudson Analytix

London, 09 September 2020


About Us
HudsonAnalytix
Complexity made simple.
Leading Edge Maritime Risk Management
Key Facts
Founded in 1986
Worldwide Presence:
Philadelphia (Global HQ)
Washington, DC
San Diego, CA
Rome, Italy
Piraeus, Greece
Manila, Philippines
Industry Leaders in Maritime Risk Management Solutions and Support Services
Environmental
Cyber Security
Security
Consequence Management
Software
Training


The 3 Pillars of cyber hygiene
Maritime Cyber Hygiene
Human Factor
Infrastructure
Procedures
Maritime Cybersecurity


The Human Factor during the pandemic
" IT MUST BE NICE HAVING A JOB WHERE YOU CAN WORK AT HOME. "
65% have not received training to WFH
25% use not updated devices
23% use unauthorised devices
10% share devices with family
Server upgrades
home laptops
extra licenses
extra internet
leased circuits
VPNs
secure connections
setting up of teleconference equipment and working groups
electronic approvals
80% believe cyber is not their responsibility
75% require more connectivity
60% have not received cyber training


CHANGING THE CYBERSECURITY PARADIGM IN THE MARITIME DOMAIN

About Us

"Global maritime transportation systems are evolving rapidly as technology and advanced analytics drive innovation and challenge existing approaches to risk management. The art of the possible is changing. We must change with it." ***ADM Thad Allen (USCG Ret.)***

HudsonAnalytix
Complexity made simple.

Leading Edge Maritime Risk Management

Key Facts

- Founded in 1986
- Worldwide Presence:
  - Philadelphia (Global HQ)
  - Washington, DC
  - San Diego, CA
  - Rome, Italy
  - Piraeus, Greece
  - Manila, Philippines
- Industry Leaders in Maritime Risk Management Solutions and Support Services

tel: +1.856.342.7500
www.hudsonanalytix.com

Partners CIP Inter American Committee on Ports | NTELX Insight to Action | AON Empower Results | DNV·GL

HudsonCyber

HudsonCyber
Managing Cyber Risk

- Trusted Best-in-Class partners
- Technology agnostic
- Unique capabilities tailored to the global maritime and energy markets
- Blended, standards-based, **maturity-model assessment approach** - the *HACyberLogix* platform
- Tailored **cyber threat intelligence** - informed by "attack side"
- **Cybersecurity training**
- Facilitation of cyber risk transfer

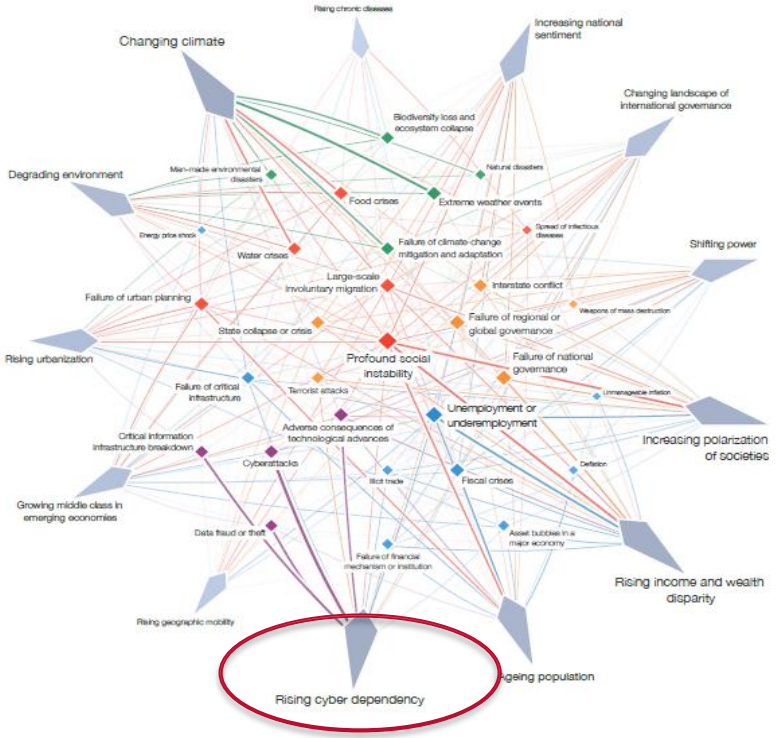
Ports & Terminal Operators

Waterside Facilities

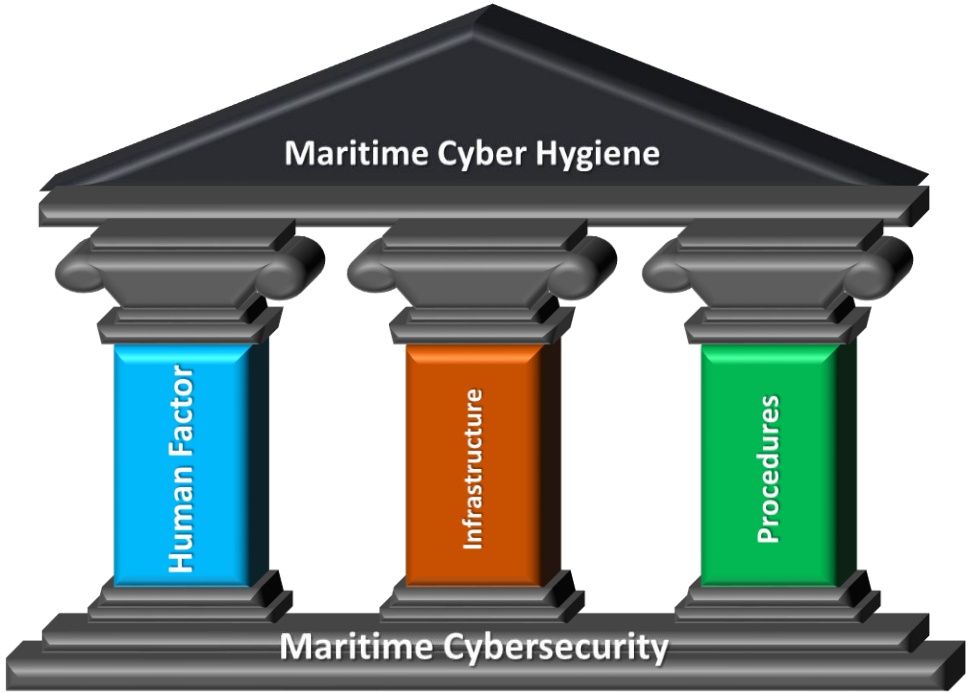
Ship-owners & Operators

Offshore

World Economic Forum Report 2019



The 3 Pillars of cyber hygiene



Cybersecurity in shipping back in 2015…

Cybersecurity in shipping today…

The urgency for action is becoming gradually understood

Why?

- No apparent ship-related cyber attacks
- No mandatory framework

(TMSA 3)

Other regulations affect maritime stakeholders (GDPR, NIS, BWM,Sulpur)

Priority

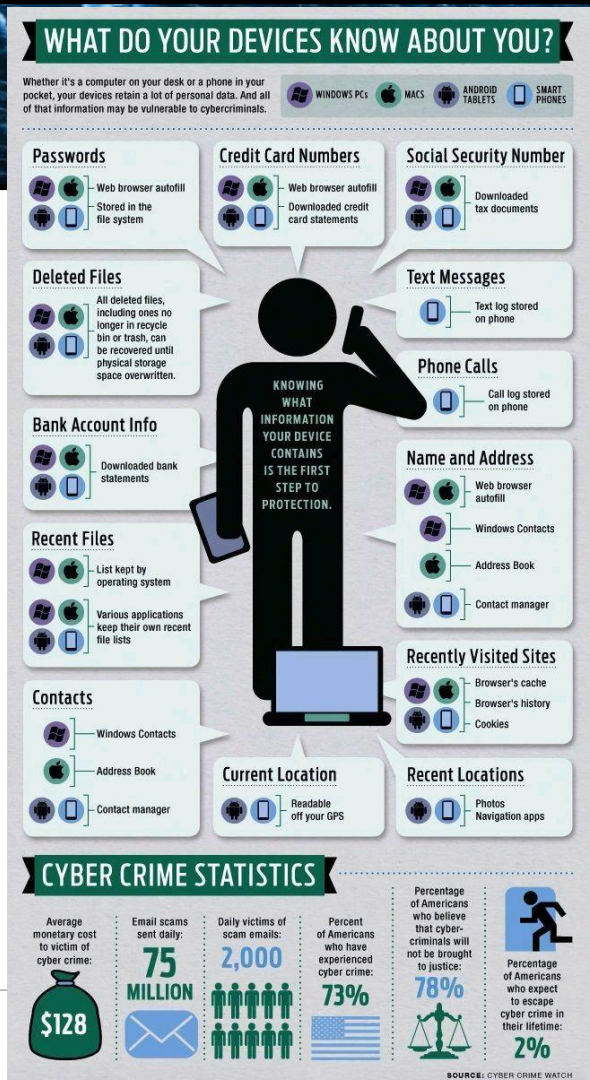
Understand how these affect our industry in order to minimize cost

'Cybersecurity as ROI'

The Human: Are we the weakest link?

	Team	Breaches
1	liverpool	280,732
2	chelsea	216,677
3	arsenal	179,095
4	manutd	59,440
5	everton	46,619
6	wolves	32,256
7	newcastle	32,143
8	tottenham	19,596
9	westham	18,801
10	brighton	15,523
11	mancity	13,796
12	crystalpalace	12,594
13	cardiff	8,118
14	leicester	7,921
15	fulham	5,984
16	watford	5,563
17	southampton	3,691
18	burnley	3,484
19	bournemouth	N/A
20	huddersfield	N/A

HudsonCyber
Managing Cyber Risk



The Human Factor during the pandemic

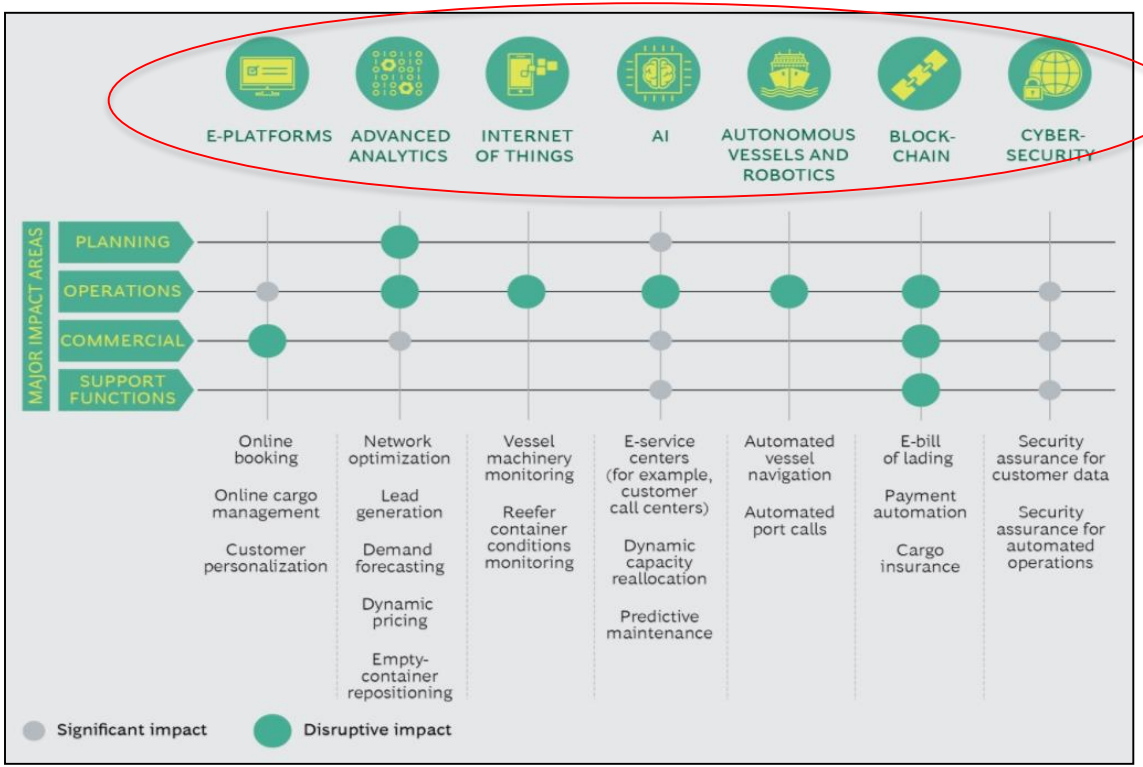
" IT MUST BE NICE HAVING A JOB WHERE YOU CAN WORK AT HOME. "

65% have not received training to WFH
25% use not updated devices
23% use unauthorised devices
10% share devices with family

Server upgrades
home laptops
extra licenses
extra Internet
leased circuits
VPNs
secure connections
setting up of
teleconference
equipment and
working groups
electronic approvals

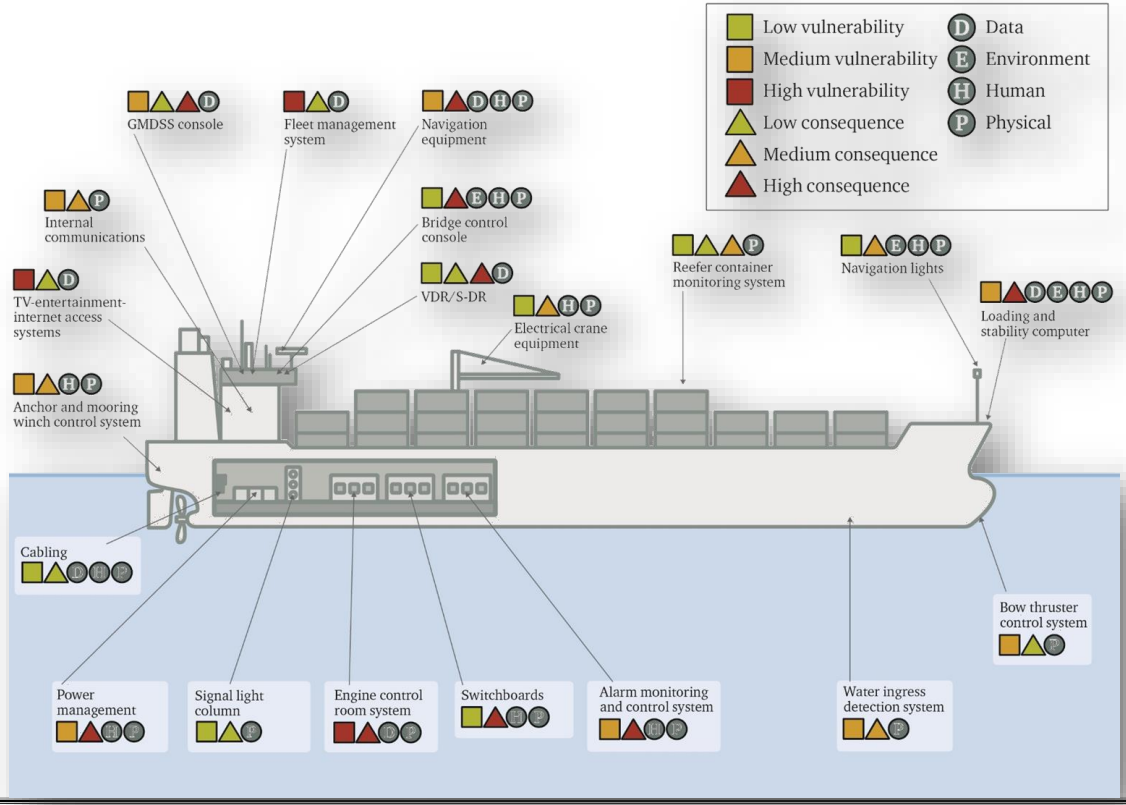
80% believe cyber is not their responsibility
75% require more connectivity
60% have not received cyber training

7 Digital Trends Transforming Shipping



Source: BCG Analysis

Chatham House Maritime Cybersecurity Research 2019: Ship's cybersecurity ecosystem



Period:
Oct 17 – Feb 19
Research Method: SoSA
UoA: 18 port sub'nts
20 ship sub'nts
AoR: Vulnerability
Consequences
Affected Fields

CHATHAM HOUSE
The Royal Institute of International Affairs

Is the industry a target?

Date	Victim	Date	Victim
2010-11	Greek Shipping Company	Jun 2017	Ships in Novorossiysk
Aug 2011	Iranian Shipping Line (IRISL)	Nov 2017	Clarksons
2011-13	Port of Antwerp	July 2018	Cosco US
2012	Australian Customs and Border Protection Service Agency	Sep 2018	Ports of Barcelona & San Diego
2012-14	Danish Port Authority	Jan 2018- September 2019	GPS and AIS interference in Eastern Mediterranean
Apr 2016	South Korea	June – August 2019	GPS and communications interference in the Strait of Hormuz
Jun 2017	AP Moller Maersk	May 2020	Shahid Rajaee port, Iran
		Q1 and Q2 2020	Cyber attacks on shipping companies MSC, Toll Group (twice) and Carnival Cruises

CHANGING THE CYBERSECURITY PARADIGM IN THE MARITIME DOMAIN

IMO Maritime Safety Committee
Draft Guidelines on Maritime Cyber Risk Management

INTERNATIONAL MARITIME ORGANIZATION

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.

...

One accepted approach is to comprehensively **assess and compare an organization's current, and desired, cyber risk management postures**.

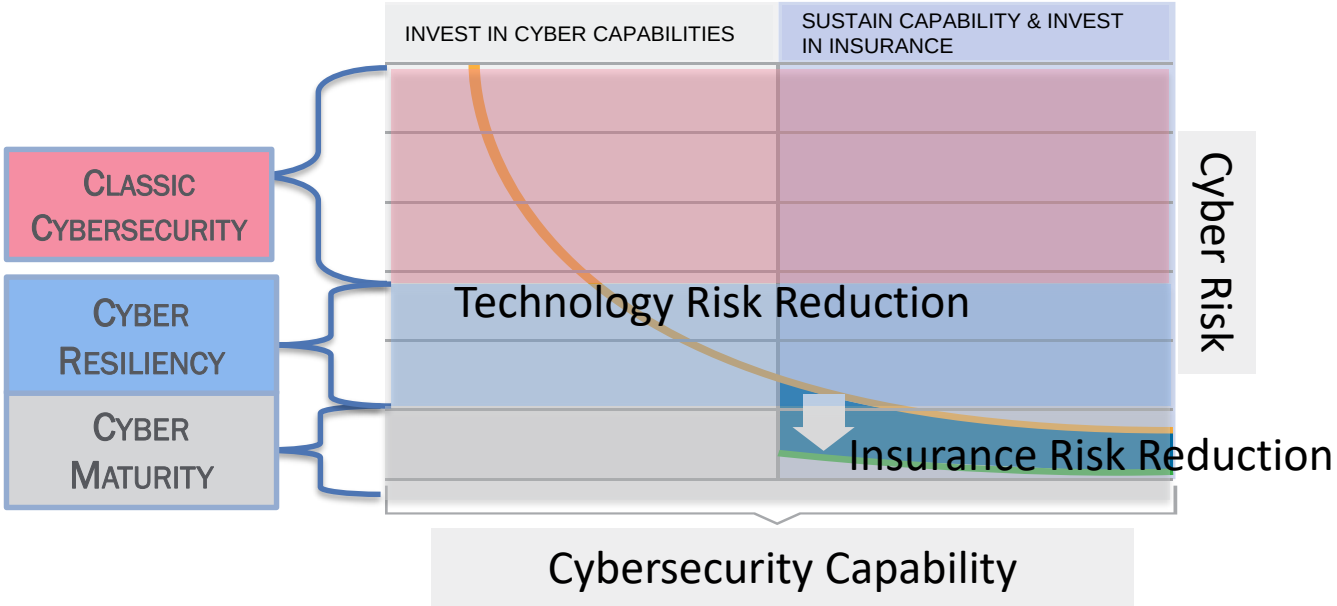
Such a comparison may reveal gaps that can be addressed to achieve risk management objectives through a prioritized cyber risk management plan.

This **risk-based approach** will enable an organization to best apply its resources in the most effective manner.

Gaining Perspective: Understanding Referenced Standards - NIST CSF and IMO (MSC.1/Circ.1526)

NIST CSF Functional Category	CSF Category	IMO Clause (Category)	IMO Clause Description
Identify	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy	**Identify (3.5.1)**	***Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data, and capabilities that, when disrupted, pose risks to ship operations***
Protect	• Access Control • Awareness & Training • Data Security • Information Protection Processes & Procedures • Maintenance • Protective Technology	**Protect (3.5.2)**	***Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber event and ensure continuity of shipping operations***
Detect	• Anomalies & Events • Security Continuous Monitoring • Detection Processes	**Detect (3.5.3)**	***Detect: Develop and implement activities necessary to detect a cyber event in a timely manner.***
Respond	• Response Planning • Communications • Analysis • Mitigation • Improvements	**Respond (3.5.4)**	***Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber event.***
Recovery	• Recovery Planning • Improvements • Communications	**Recover (3.5.5)**	***Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber event.***

The Cyber Risk Reduction Curve

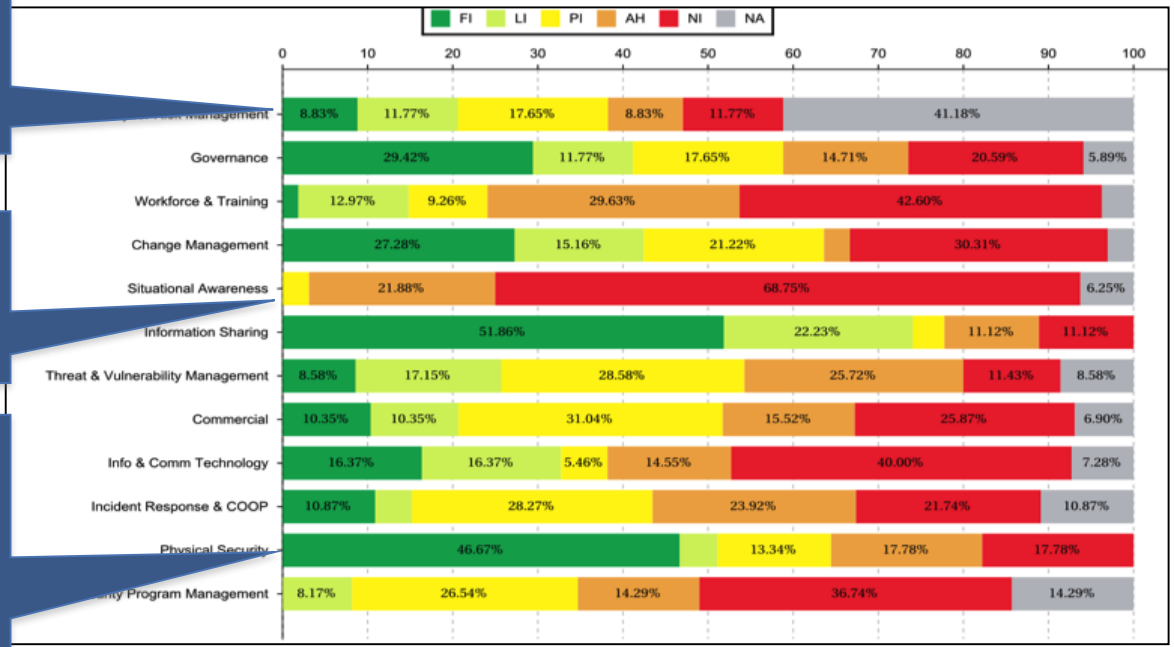


Designed for "Balance Sheet Owners"

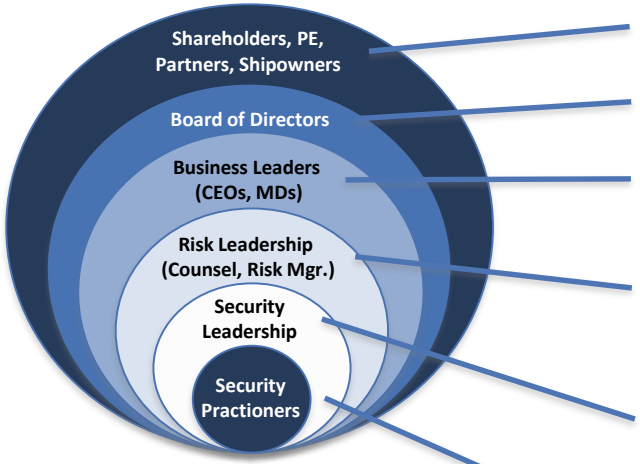
Risks are not well understood

Risks are recognized but not well managed

Risks are well understood and managed



Who *Owns* Responsibility for Cyber Risk?



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 supports cash flow and profit and loss)

Key Considerations for Empowering Leaders and Institutionalizing Cybersecurity Capability

ORGANIZE!
Establish multi-disciplined cyber working group that meets regularly. Grant authorities!

ENTERPRISE ASSESSMENT
Perform an enterprise level cybersecurity capability assessment.

CYBER THREAT ANALYSIS
Assume you're already compromised. Discover who's targeting you; emergent exploits.

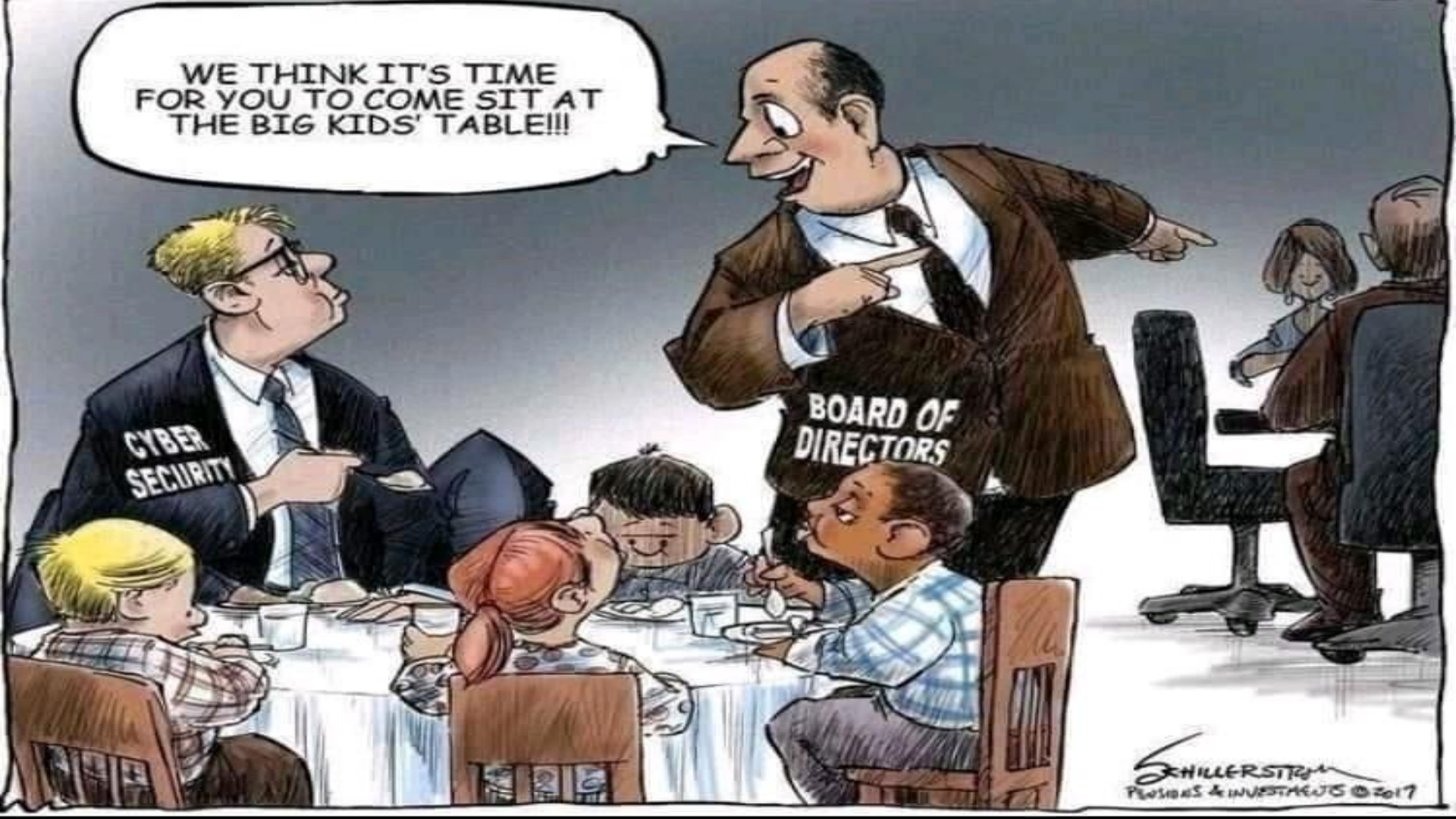
QUANTIFY YOUR EXPOSURE
Identify your most valuable assets, determine values and develop loss scenarios. Prioritize.

STRESS TEST YOUR INSURANCE
Review all policies for gaps/exclusions. How do they perform against the loss scenarios?

PREPARE
Establish a Cyber Incident Response (IR) plan. Update Data Loss Prevention (DLP), Disaster Recovery (DR) and Business Continuity (BC) Plans.

TRAIN
Train! Deliver awareness training to executives (first) then staff and crews. Incorporate cyber risk factors into drills and exercises.

SUSTAIN RESOURCES
Develop and sustain resources (people, processes, tools) with a budget.


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