Cyber Risk Management for the Maritime Sector

Chronis Kapalidis, Academy Stavros Niarchos Foundation Fellow,
International Security Department
Europe Representative, HudsonAnalytix

Thursday, November 08, 2018, Athens

HudsonAnalytix
Complexity made simple.

CHATHAM HOUSE
The Royal Institute of International Affairs

Key findings (Facts & Figures)

Date	Victim
2010-11	Greek Shipping Company
Aug 2011	Iranian Shipping Line (IRISL)
2011-13	Port of Antwerp
2012	Australian Customs and Border Protection Service agency
2012-14	Danish Port Authority
Apr 2016	South Korea
Jun 2017	AP Moller Maersk
Jun 2017	Ships in Novorossiysk
Nov 2017	Clarksons
July 2018	Cosco US
Sep 2018	Ports of Barcelona & San Diego

- **1,000,000** events/day/vessel
- **~ 11,000** cyber threats
- **80%** conducted from crew network

- ~97% of malware is designed to exploit social engineering weaknesses, not a technical flaw

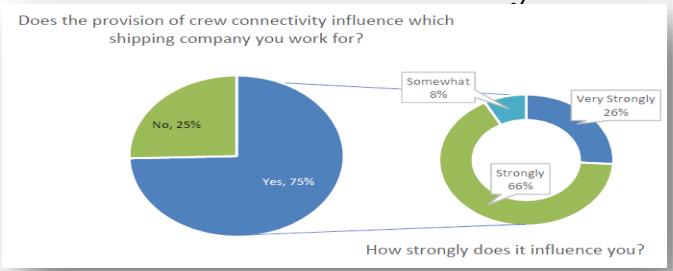
- 2 Ongoing research projects for cybersecurity at the MTS
- Expert Comments
- Global Insights Workshop
- Simulation Exercises

Key findings (Awareness)

- The urgency for action is becoming gradually understood

Why?

- No **apparent** ship-related cyber attacks
- No **mandatory** framework (Other regulations affect maritime stakeholders (GDPR, NIS))
- **Other** mandatory actions required (BWM, SC)



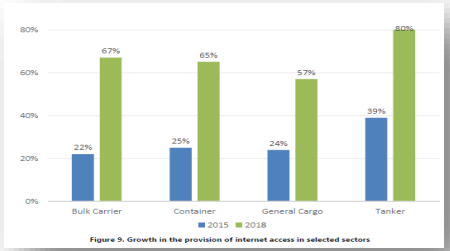


Figure 9. Growth in the provision of internet access in selected sectors

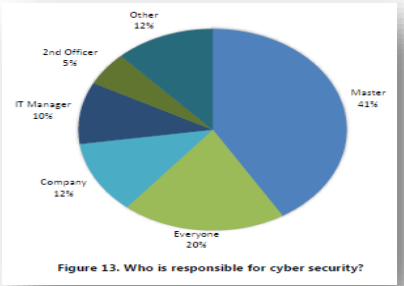
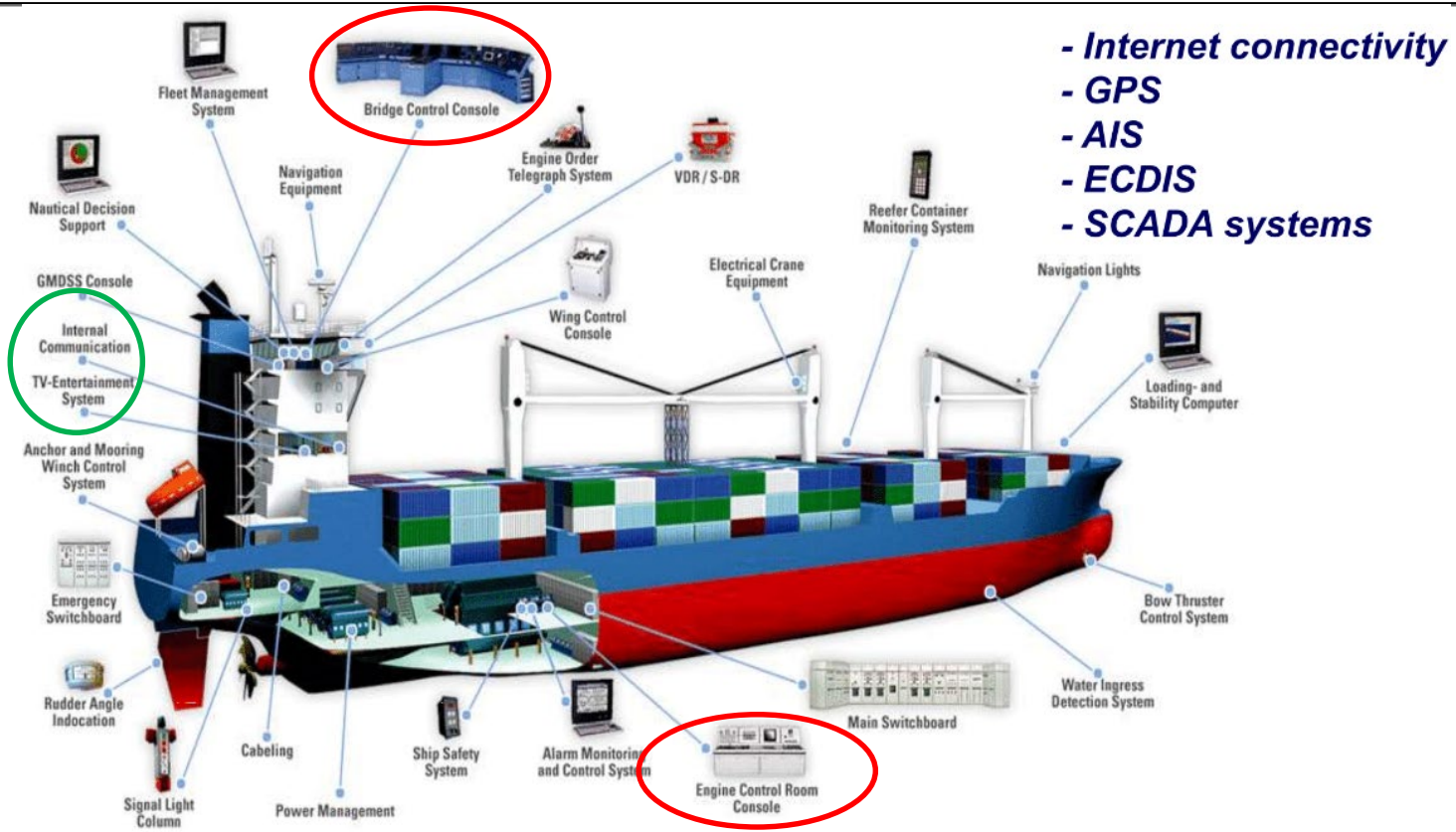
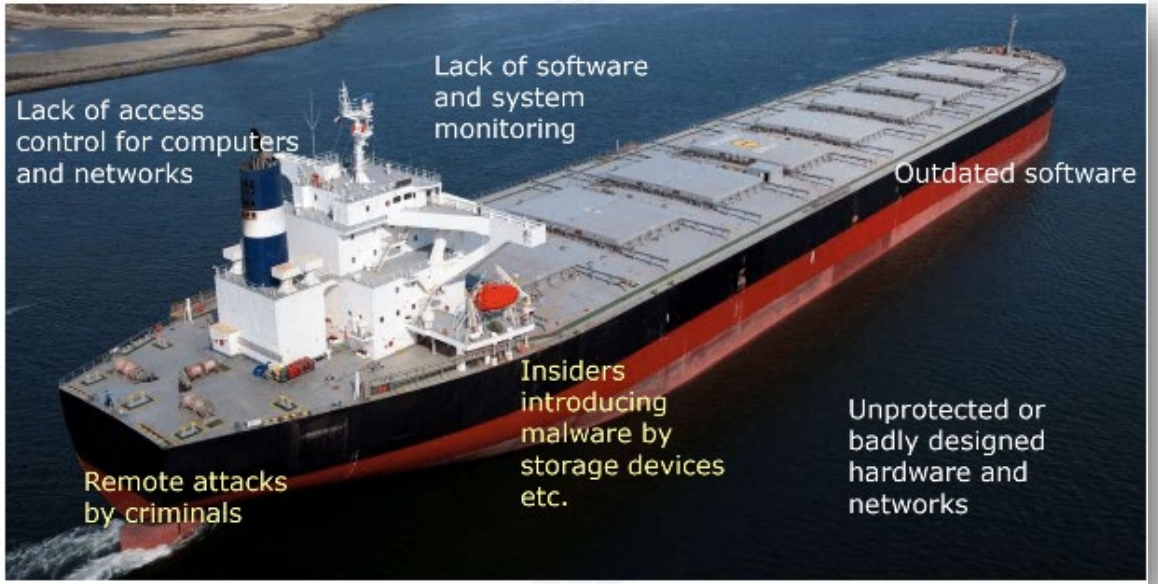


Figure 13. Who is responsible for cyber security?

On board IT and OT Systems



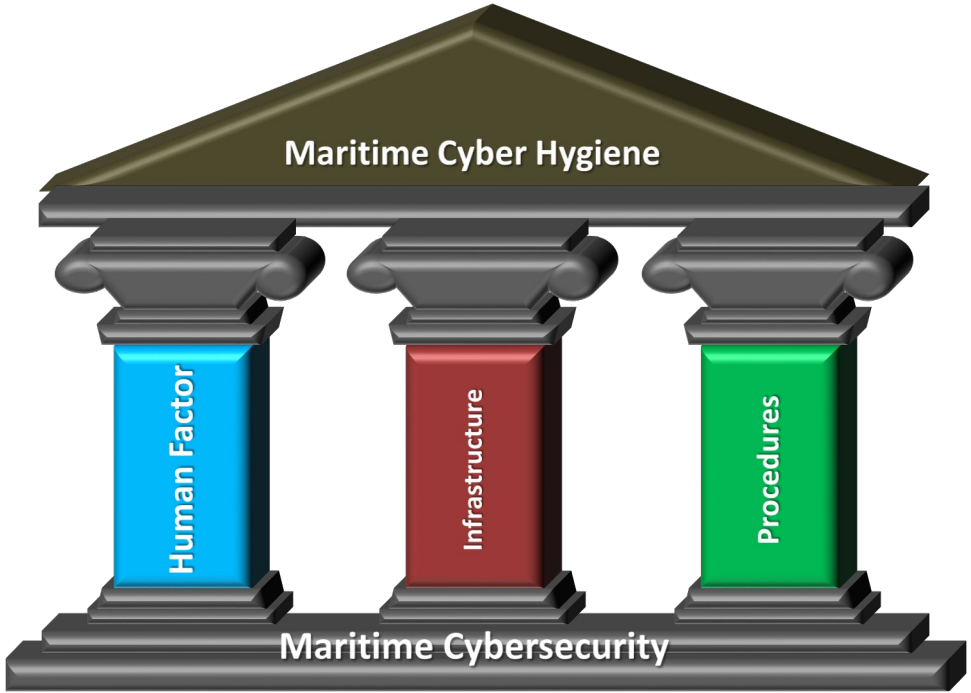
- Average ship age 10 ~ 15 years



Case Studies

- The Clarksons cyber security hack **(human factor-insider)**
- Drug trafficking via the port of Antwerp **(human factor-insider)**
- Malware on mobile offshore drilling unit incapacitated networks **(human factor-insider)**

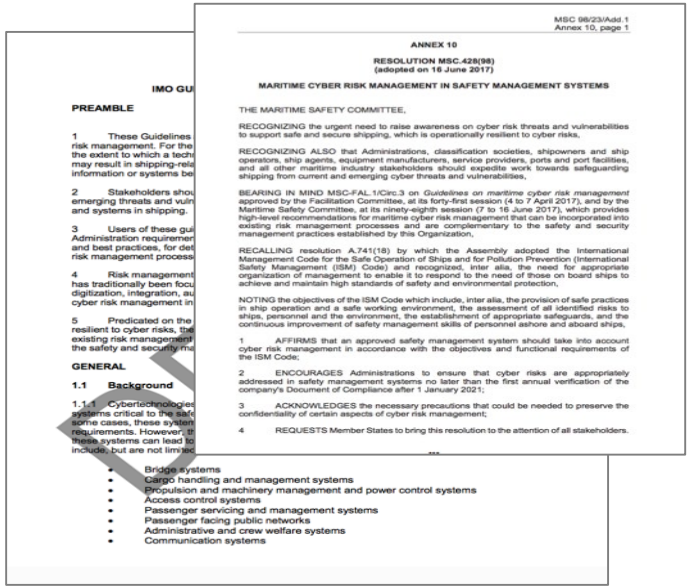
The 3 Pillars of cyber hygiene



IMO Maritime Safety Committee
Draft Guidelines on Maritime Cyber Risk Management

> 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.

IMO 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.

PREAMBLE

GENERAL

1.1 Background

- Bridge systems
- Cargo handling and management systems
- Propulsion and machinery management and power control systems
- Access control systems
- Passenger servicing and management systems
- Passenger facing public networks
- Administrative and crew welfare systems
- Communication systems

Cybersecurity is about *managing risk*

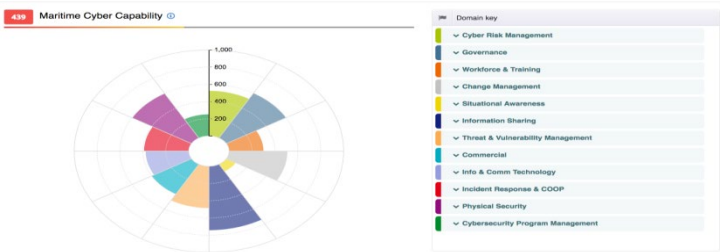
- It's about digitally identifying, informing, enabling, controlling, and describing an asset.
- *Assets* can be people, processes, tools and systems.
- It's about managing risk to the *confidentiality*, *integrity* and *availability* of the information impacting assets.

But modelling cyber risk is difficult….

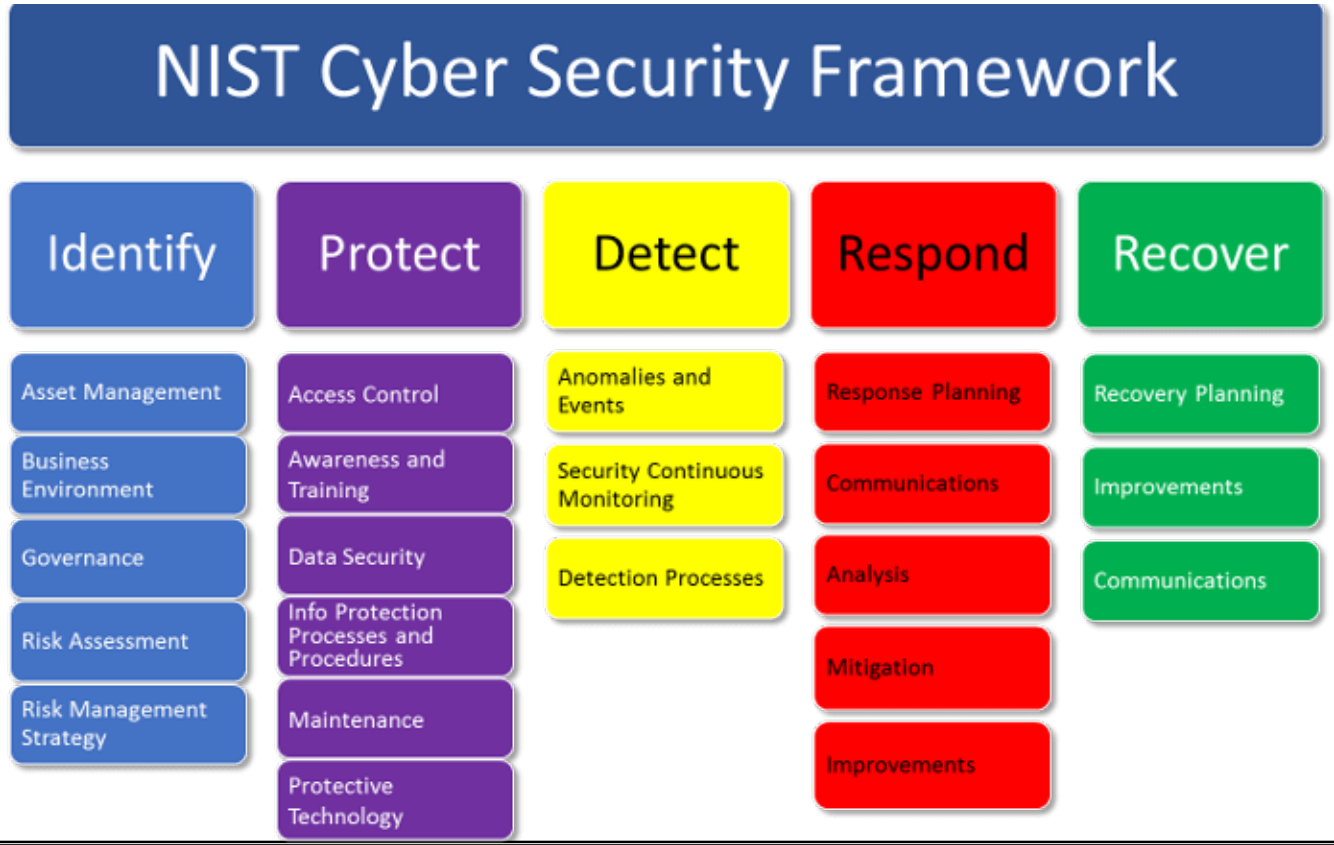
- No authoritative source of data

- A Cyber risk model requires input for people and processes in addition to technology

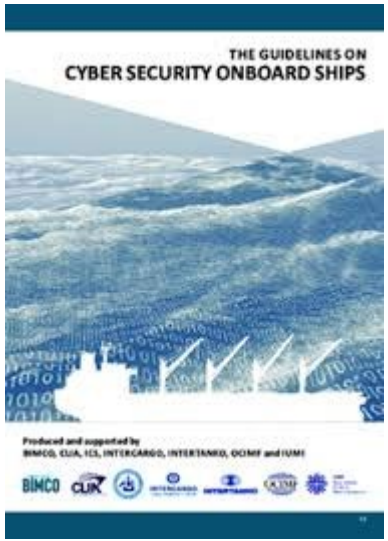
- Limited risk quantification models

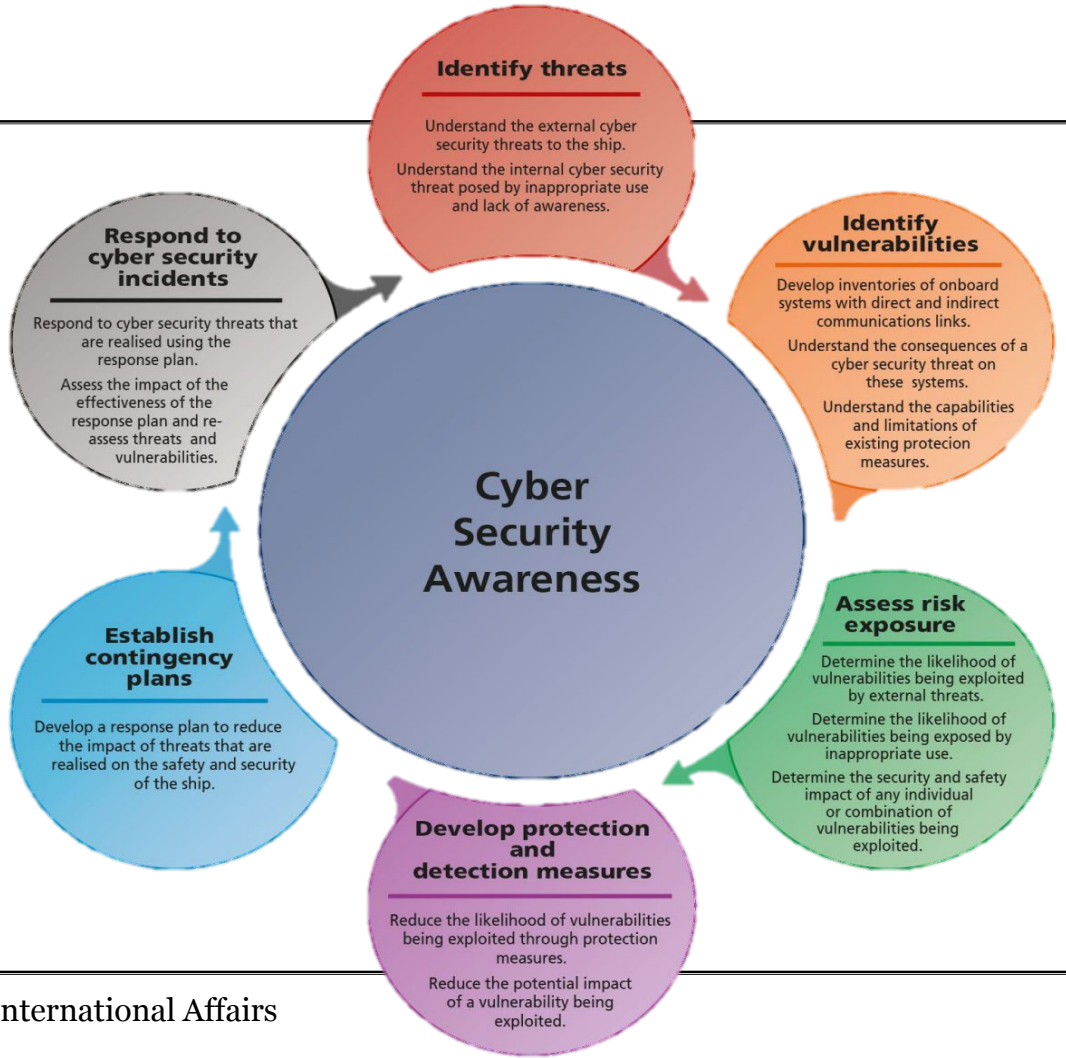


Guidelines


NIST Cyber Security Framework
Identify
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Protect
Access Control
Awareness and Training
Data Security
Info Protection Processes and Procedures
Maintenance
Protective Technology
Detect
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Respond
Response Planning
Communications
Analysis
Mitigation
Improvements
Recover
Recovery Planning
Improvements
Communications

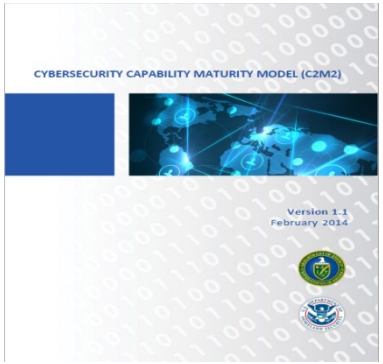
Guidelines

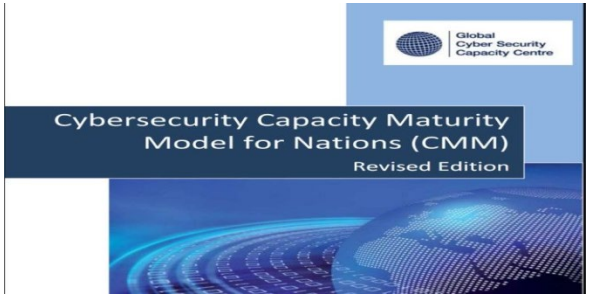

THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS
Produced and supported by
BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI


Identify threats
Understand the external cyber security threats to the ship.
Understand the internal cyber security threat posed by inappropriate use and lack of awareness.
Identify vulnerabilities
Develop inventories of onboard systems with direct and indirect communications links.
Understand the consequences of a cyber security threat on these systems.
Understand the capabilities and limitations of existing protecion measures.
Assess risk exposure
Determine the likelihood of vulnerabilities being exploited by external threats.
Determine the likelihood of vulnerabilities being exposed by inappropriate use.
Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.
Develop protection and detection measures
Reduce the likelihood of vulnerabilities being exploited through protection measures.
Reduce the potential impact of a vulnerability being exploited.
Establish contingency plans
Develop a response plan to reduce the impact of threats that are realised on the safety and security of the ship.
Respond to cyber security incidents
Respond to cyber security threats that are realised using the response plan.
Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.
Cyber Security Awareness

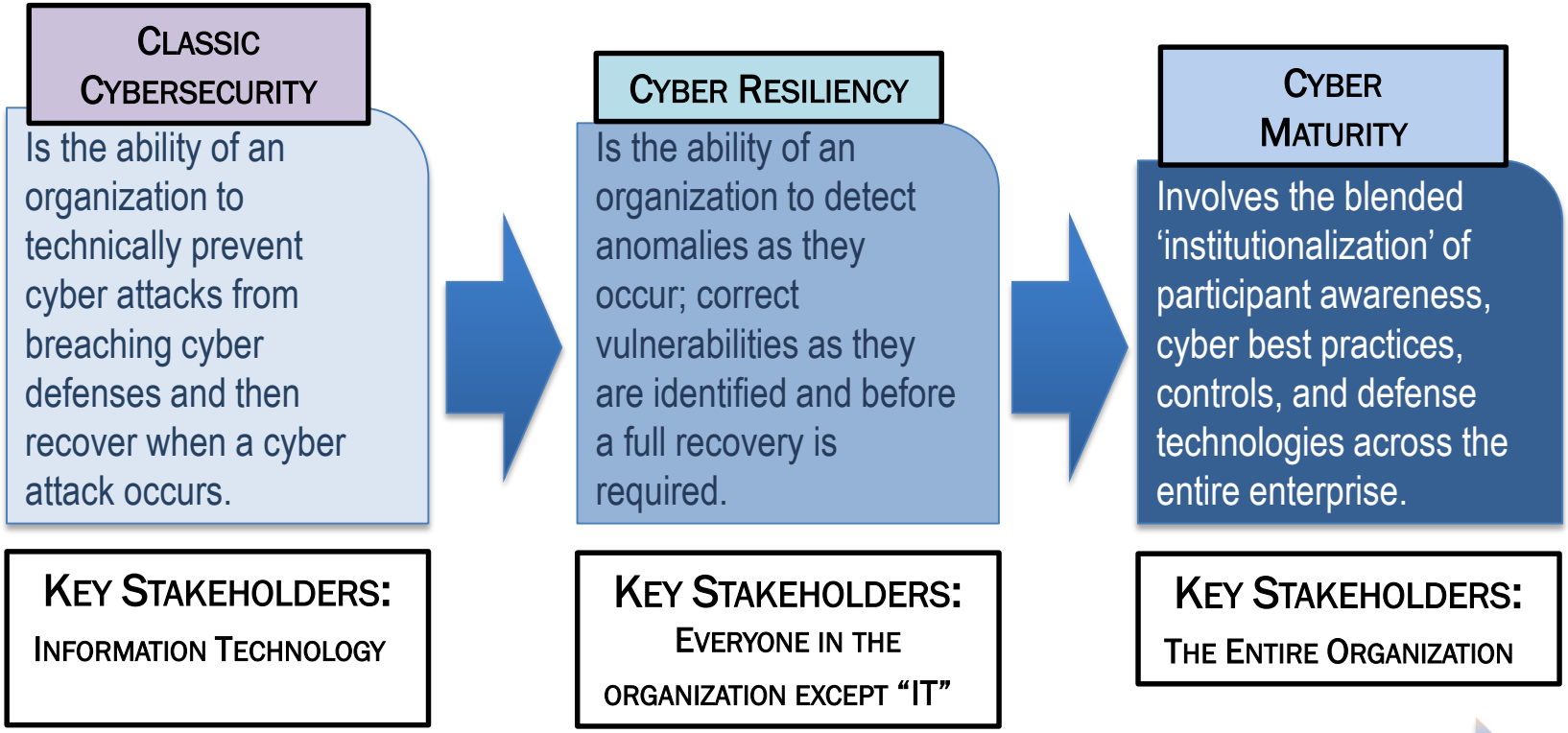
Cybersecurity Capability Maturity

…defines an organization's *cyber ecosystem*, identifies the depth and breadth of deployed capabilities, establishes benchmarks to support long-term measurement and continuous improvement, and serves as the primary mechanism for sustaining the organization's cybersecurity strategy and investments.

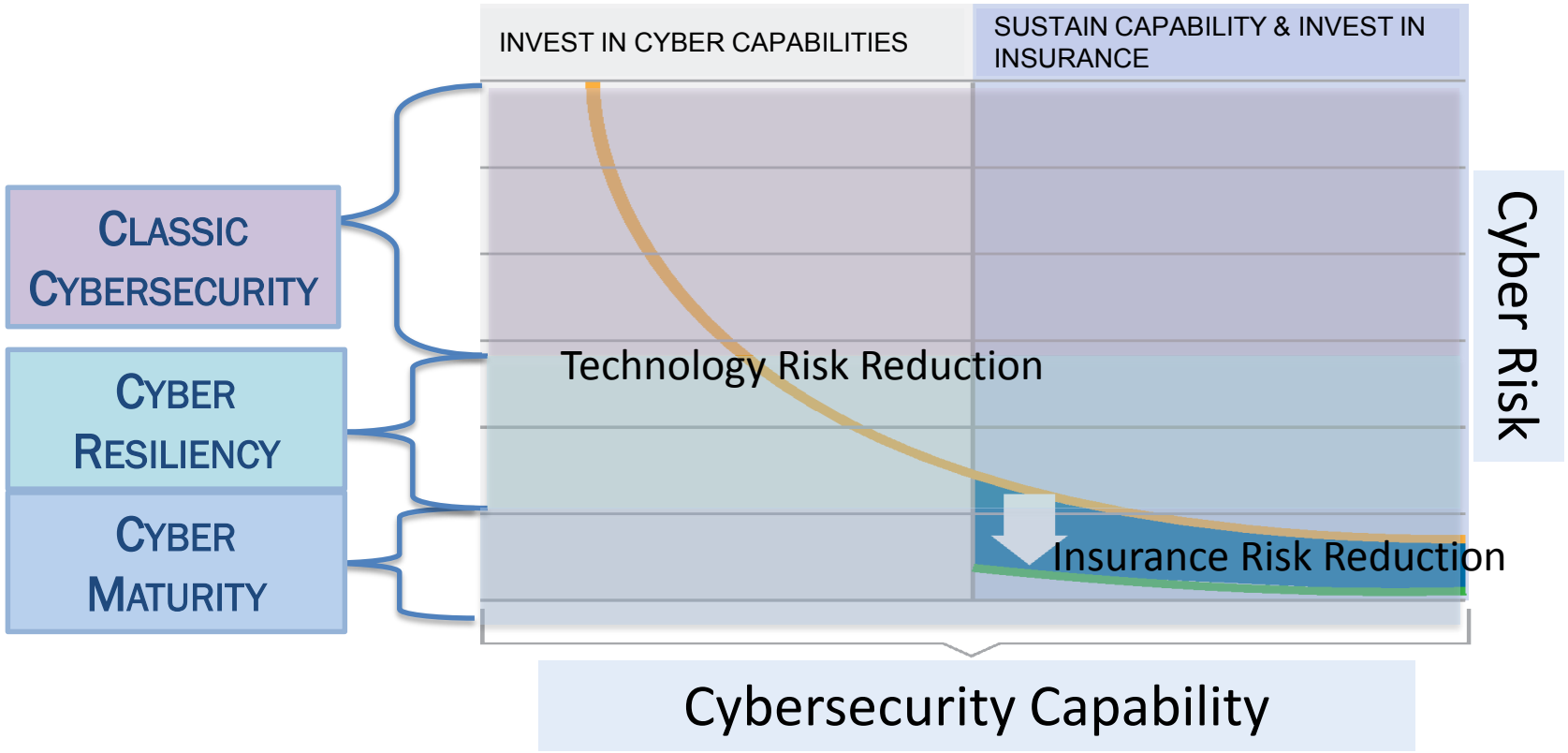




Evolving from Cybersecurity to Cyber Maturity



The Cyber Risk Reduction Curve



The HACyberLogix Structure

The Maritime Transportation Cybersecurity Capability Assessment Approach

The *HACyberLogix* application provides maritime organizational leadership with the sustained ability to analyze, benchmark, measure, and facilitate cybersecurity capability evolution across all the areas of a company's business.

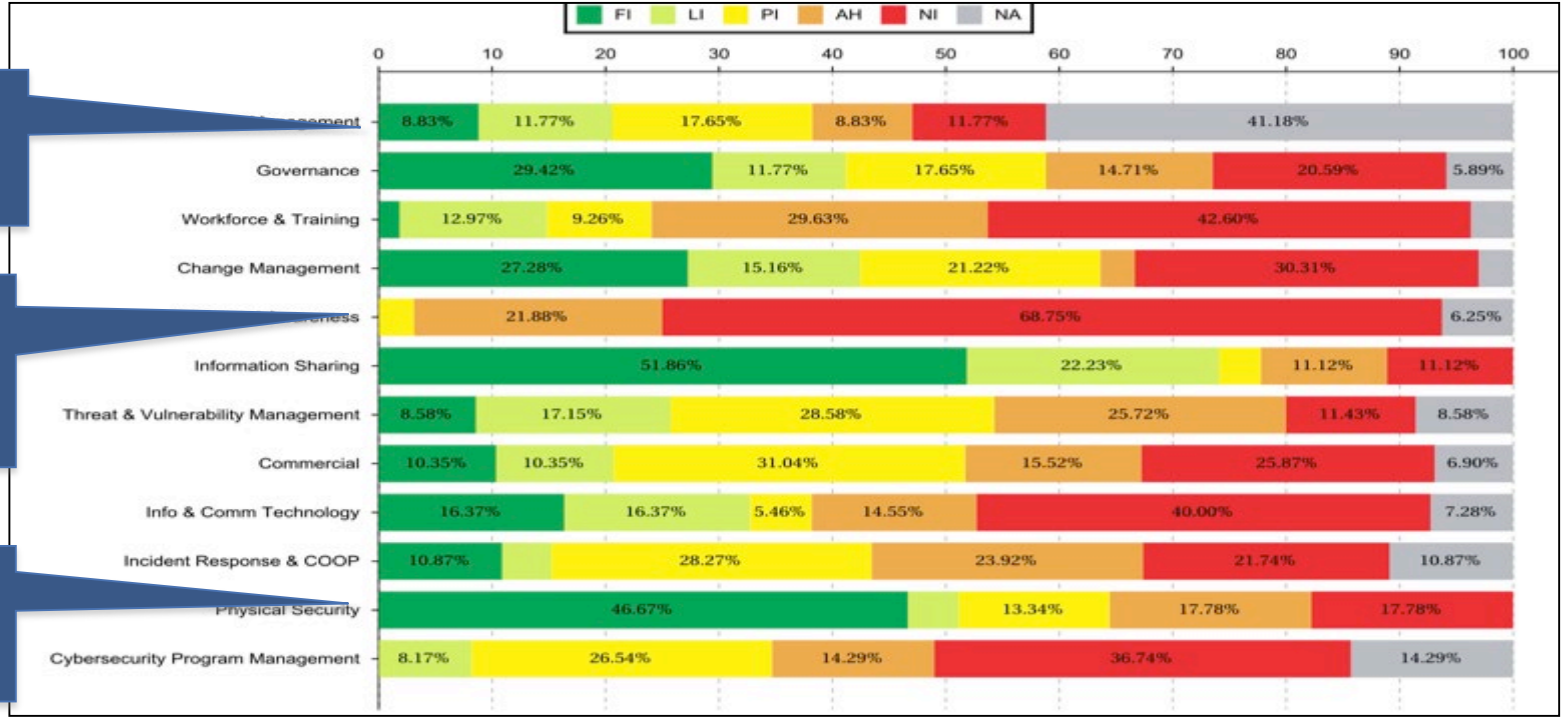
Risk Management	Governance	Workforce & Training	Change Management
Situational Awareness	Information Sharing	Threat & Vulnerability Management	Commercial
ICT	Event & Incident Response	Physical	Cyber Program Management

Understanding the approach

Risks are not well understood

Risks are recognized but not well managed

Risks are well understood and managed



Cyber as ROI

Two aspects in increasing ROI from investing in cybersecurity

User	*Corporate*
Invest in user awareness training	*Use the knowledge and best practises of other industries*
Educate staff on new measures, technologies and tools	*Cyber security by design*

Thank you

We have land and a home
as long as we have ships at sea..

Themistocles 480 B.C.