
The Cyber Risk and its management in the Marine Industry

How to identify threats, manage vulnerabilities and protect the Shipping business

Naples Shipping Week
27th of September 2018



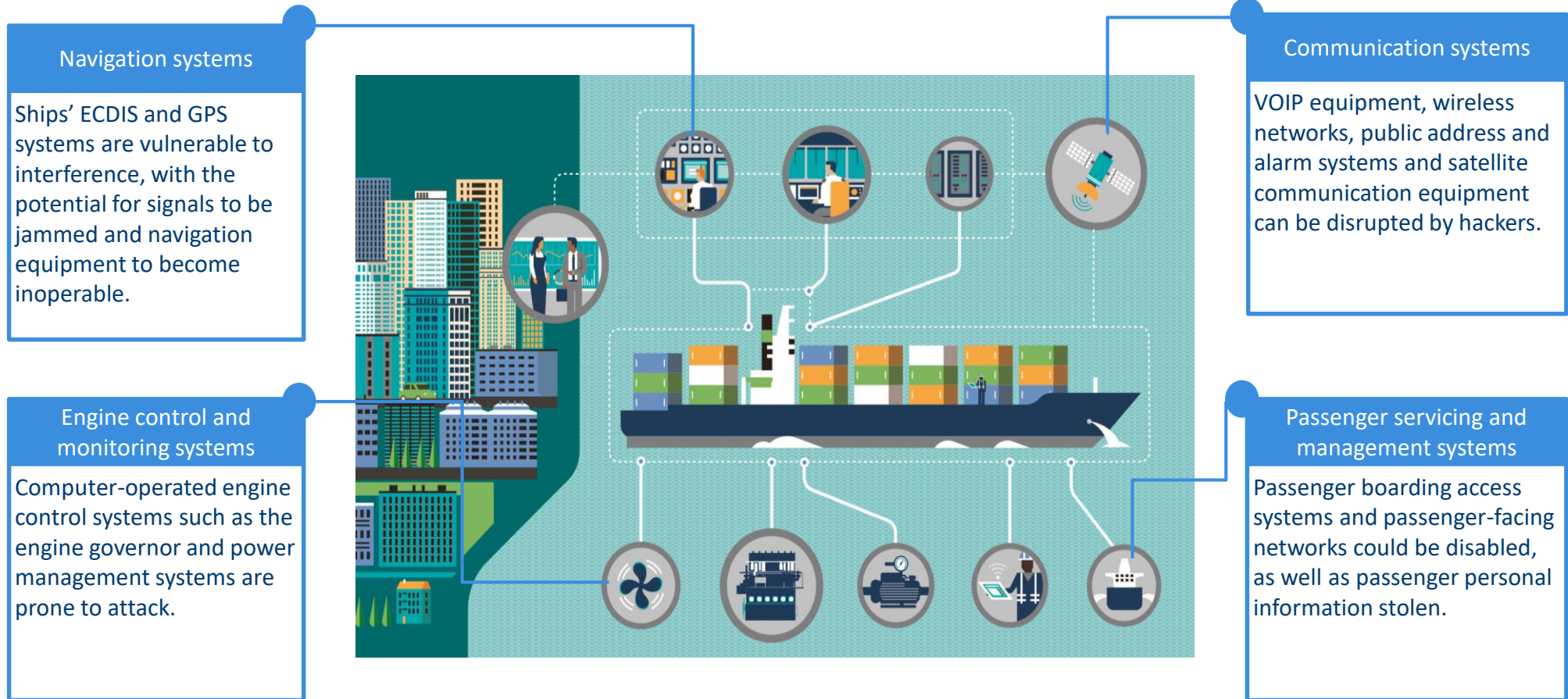
JohnPaul CAVANNA

Paolo SCIALLA

Lloyd's Register



Increased complexity brings increased RISKS



International and European framework



- International Maritime Organisation (IMO)
 - MSC-FAL.1/Circ.3 Guidance on maritime cyber risk management (in place after 1 Jan 2021)

- International Safety Management (ISM) Code
 - ISM Code 2018, (MSC.42/98)



- General Data Protection Regulation (GDPR) apply from May 2018- includes ships



- EU Directive 2016/1148 concerning security of Network and Information Systems (NIS Directive)

- BIMCO, CLIA, ICS, Intercargo and Intertanko Guidelines

- US NIST Critical Infrastructure Cyber Security Framework

- Tanker Management Self-Assessment (TMSA)

- TMSA No. 3, published in April 2017, met by 1st Jan 2018



HOW to manage the Cyber RISK

To improve cyber security?

Take a holistic approach involving:

1. **People** – *focus on knowledge, behavior and mind-set*

- Raise awareness, provide training and communicate the risks at all levels of the organization.

2. **Processes** – *focus on policies, procedures and risk assessments*

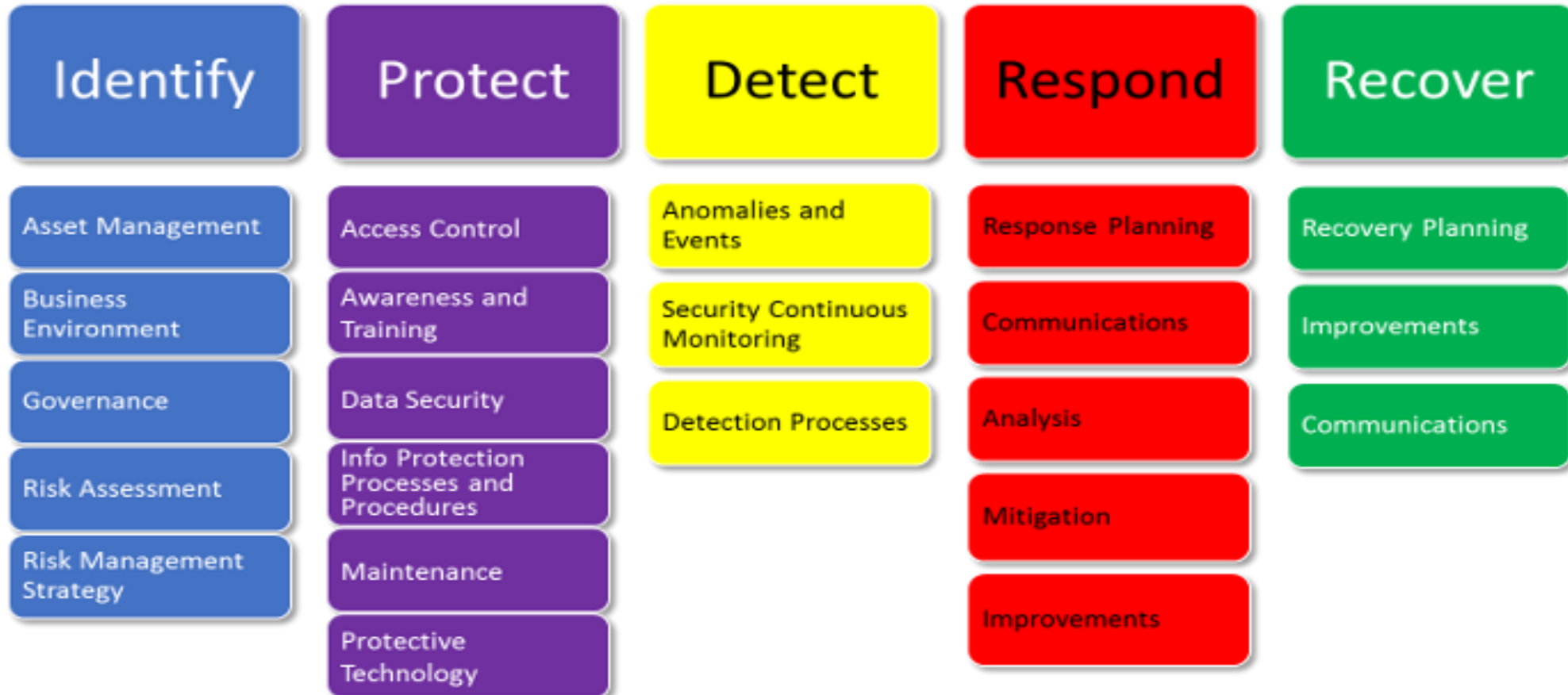
- Align cyber risks with existing security and safety risk management requirements contained in the ISPS and ISM Codes as included in company policies.
- Include requirements relating to training, operations and maintenance of critical cyber systems in relevant documentation on-board.

3. **IT systems** – *focus on firewalls, antivirus and encryption*

- Ensure there is adequate protection at all levels of the company - from senior management ashore to the crew on-board so that it becomes an inherent part of the safety and security culture on-board each vessel

The Cyber Risk management process in Marine Industry

NIST Cyber Security Framework

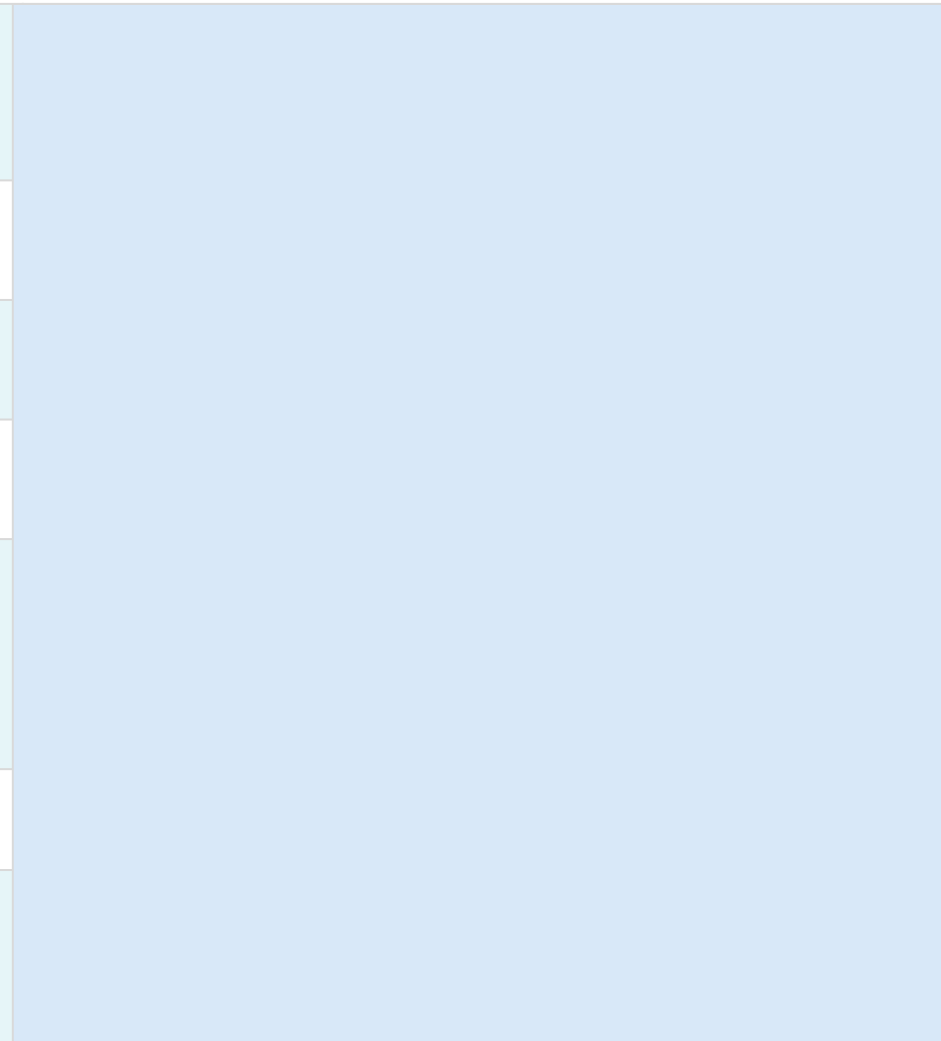


Today's Enterprise Needs A New Style Of Security

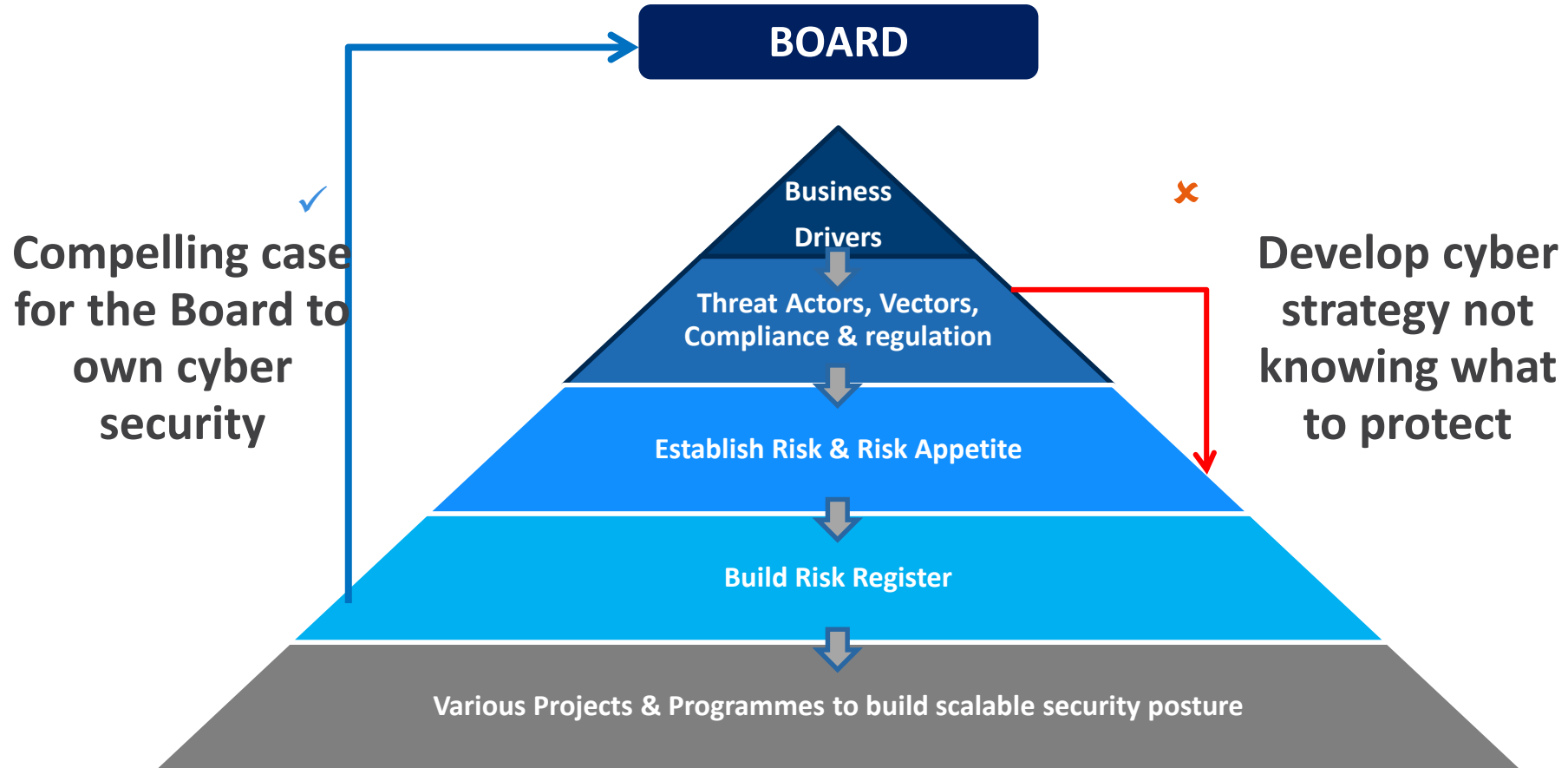
OLD

NEW

Ultimate State	<ul style="list-style-type: none">▪ Impregnable
Messaging	<ul style="list-style-type: none">▪ Fear, Uncertainty, Doubt
Business Proximity	<ul style="list-style-type: none">▪ None
Accountability & Leadership	<ul style="list-style-type: none">▪ IT / Risk department
Focus	<ul style="list-style-type: none">▪ Perimeter & Information
Approach	<ul style="list-style-type: none">▪ Complicate, obstruct, say no
SOC Focus	<ul style="list-style-type: none">▪ Regional. Isolated. Servers, network & security devices



Governance Risk and Compliance



Thank you

JohnPaul CAVANNA

Paolo SCIALLA

Lloyd's Register

