



CYBER RISK AND SHIPS :PRACTICAL ISSUES FOLLOWING BIMCO GUIDELINE

Yohan Le Gonidec, head of Shipowner support department, TECNITAS (subsidiary BUREAU VERITAS)

12.09.2016



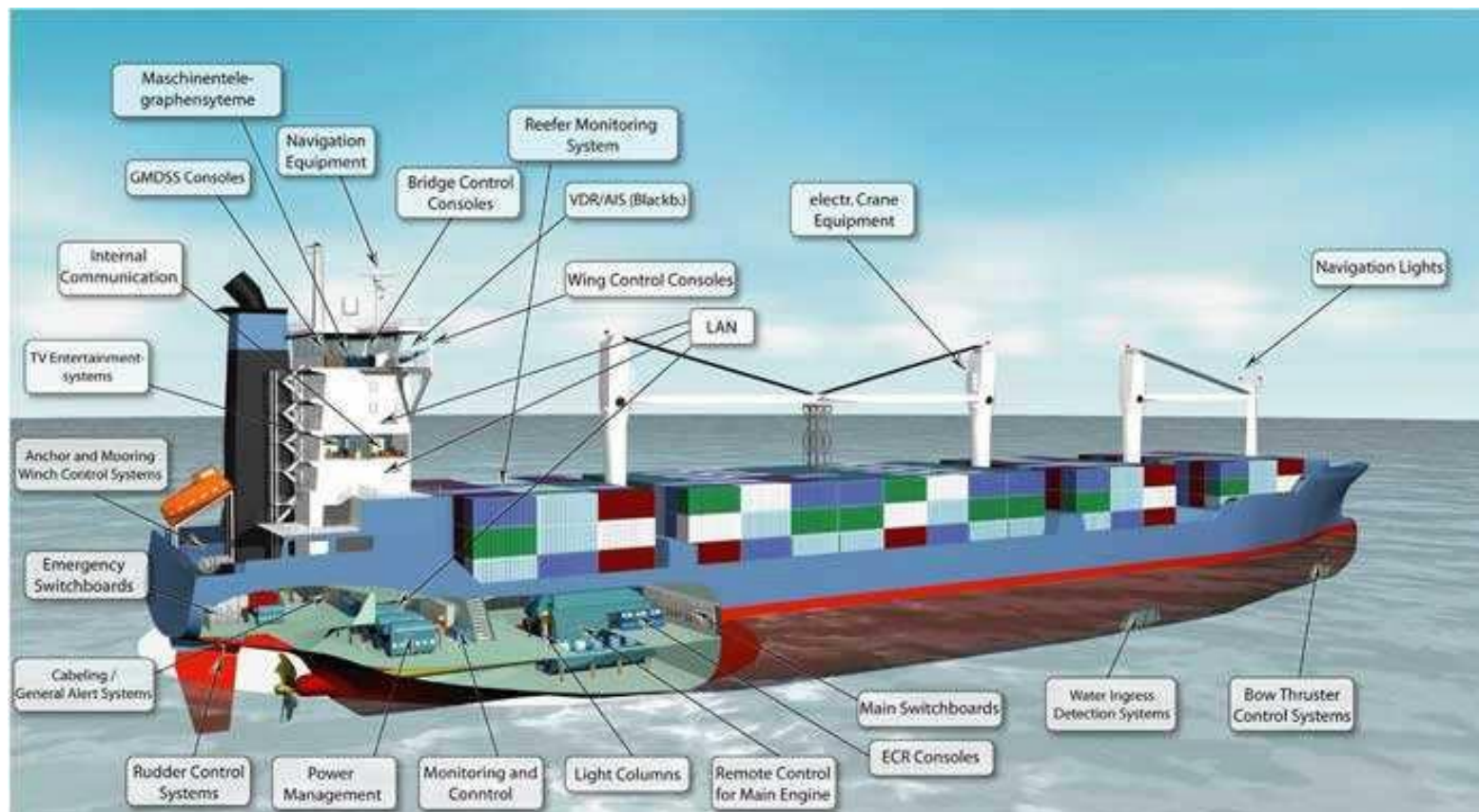
Genova
18-21 September 2016

AGENDA

- Introduction
- 1- Cyber incidents : what happened or could happen in Maritime Industry !
- 2- How to assess ship vulnerability ?
- 3 – How to improve cybersecurity ?

INTRODUCTION

- Ship onboard systems offer vulnerabilities:



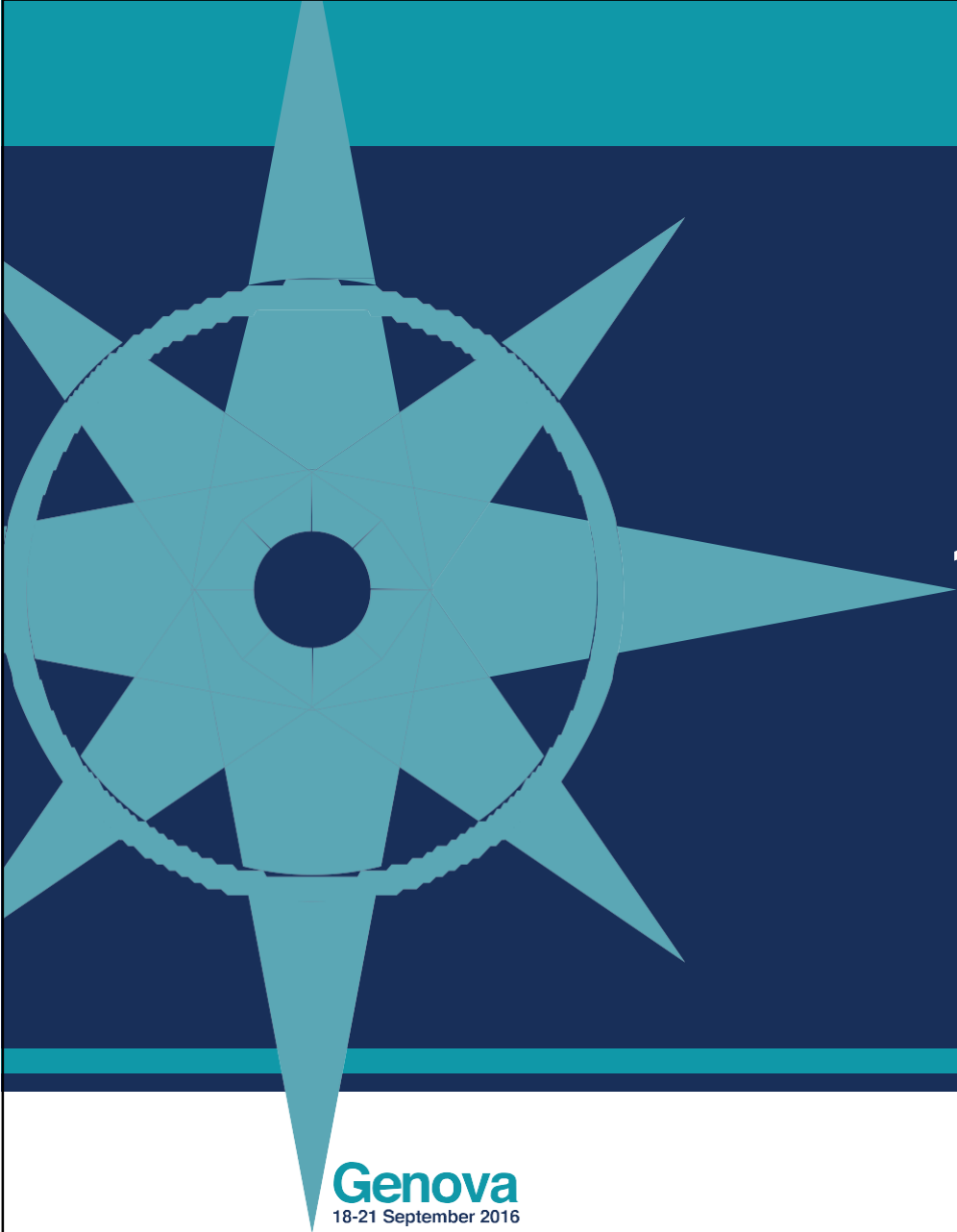
CYBER THREATS

- Cyber risk is specific to:
 - The company
 - The ship
 - The operation and / or trade



Group	Motivation	Objective
Activists (including disgruntled employees)	<ul style="list-style-type: none"> • Reputational damage • Disruption of operations 	<ul style="list-style-type: none"> • Destruction of data • Publication of sensitive data • Media attention
Criminals	<ul style="list-style-type: none"> • Financial gain • Commercial espionage • Industrial espionage 	<ul style="list-style-type: none"> • Selling stolen data • Ransoming stolen data • Ransoming system operability • Arranging fraudulent transportation of cargo
Opportunists	<ul style="list-style-type: none"> • The challenge 	<ul style="list-style-type: none"> • Getting through cyber security defences • Financial gain
States State sponsored organisations Terrorists	<ul style="list-style-type: none"> • Political gain • Espionage 	<ul style="list-style-type: none"> • Gaining knowledge • Disruption to economies and critical national infrastructure.





1 - CYBER INCIDENTS : WHAT HAPPENED OR COULD HAPPEN IN MARITIME INDUSTRY ?

Genova
18-21 September 2016

IUMI

CYBER INCIDENTS : ALREADY A REALITY IN MARITIME INDUSTRY

- Number of known cases is low (Only following 5 facts could be found on the web)
- There are however few reports that hackers have compromised maritime cyber security.
- Significant holes were found in the three key technologies sailors use to navigate
 - GPS
 - Marine Automatic Identification System (AIS),
 - Electronic Chart Display and Information System (ECDIS)

FACT N°01 : HACKING AIS* DATA IS POSSIBLE

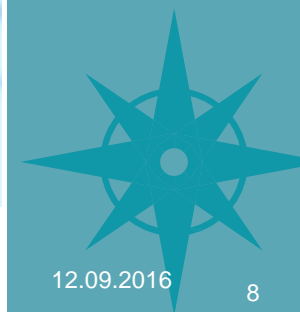
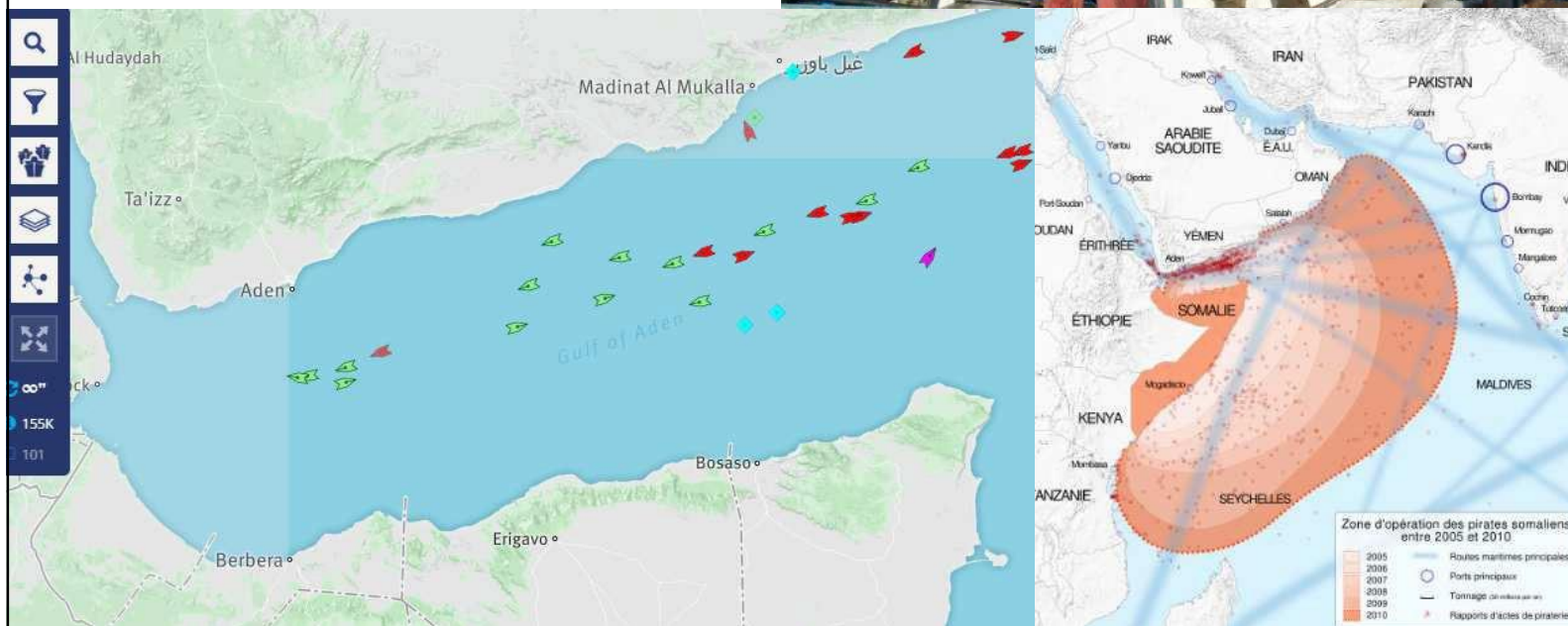
Installed in an estimated 400,000 vessels, AIS is currently the best system for collision avoidance, maritime security, aids to navigation and accident investigations.

*AIS : Automatic Identification System



FACT N°02 : SOMALI PIRATES USED AIS DATA

As a shopping list...

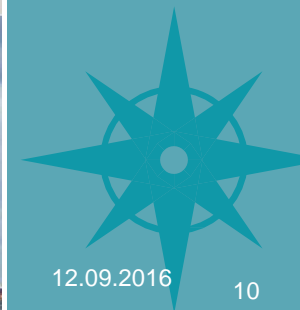


FACT N°03 : TILTING OF AN OIL RIG

In 2014, forced to shut down...



FACT N°04 : ONSHORE SYSTEMS WERE HACKED TO TRANSPORT DRUG ANVERS

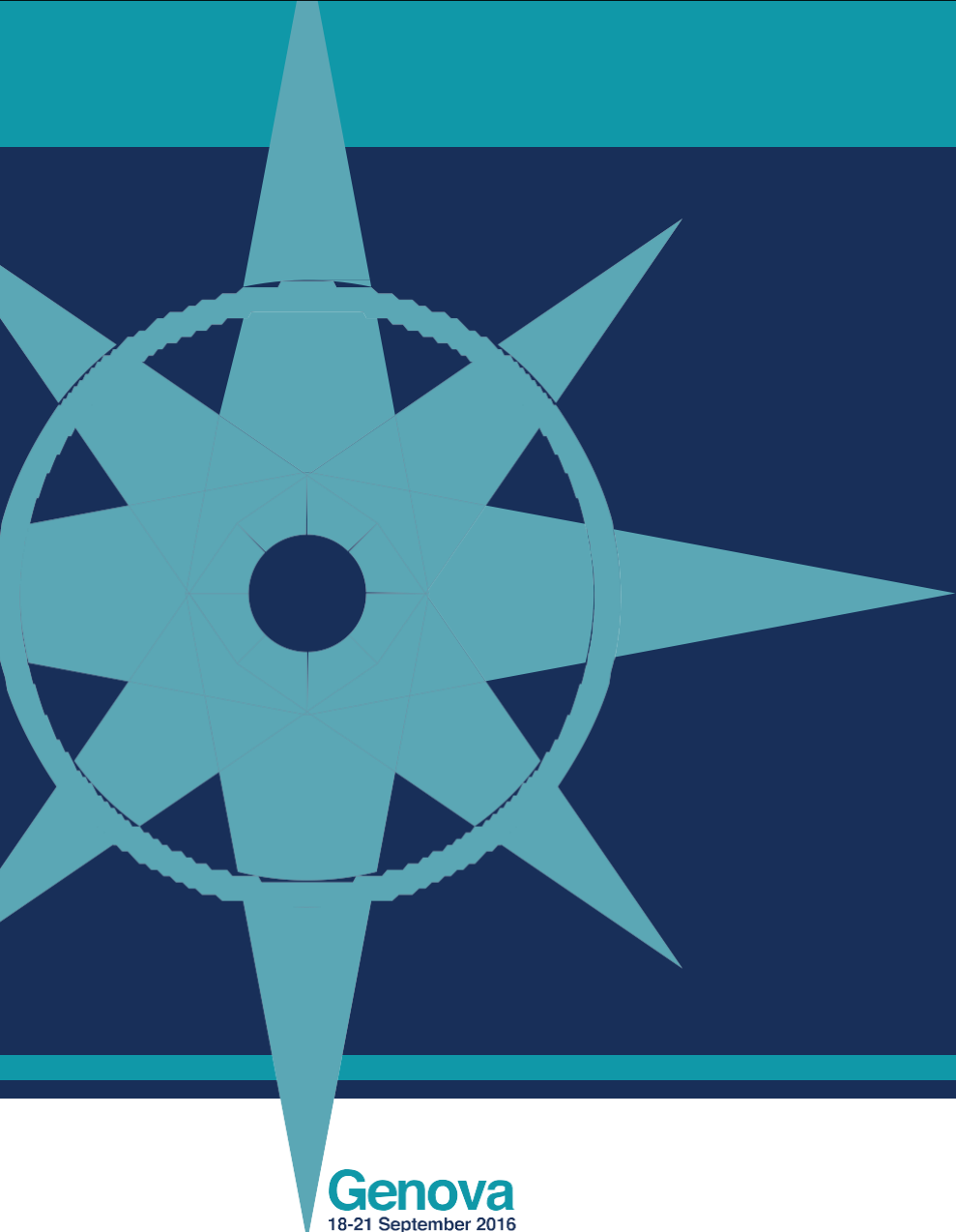


FACT N°05 : A YACHT CHANGED HIS WAY, BECAUSE OF GPS HACKED SIGNAL

Fake GPS

© Texas University, Cockrell School of Engineering





2- HOW TO ASSESS SHIP VULNERABILITY ? (METHODOLOGY)

Genova
18-21 September 2016

IUMI

BIMCO GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

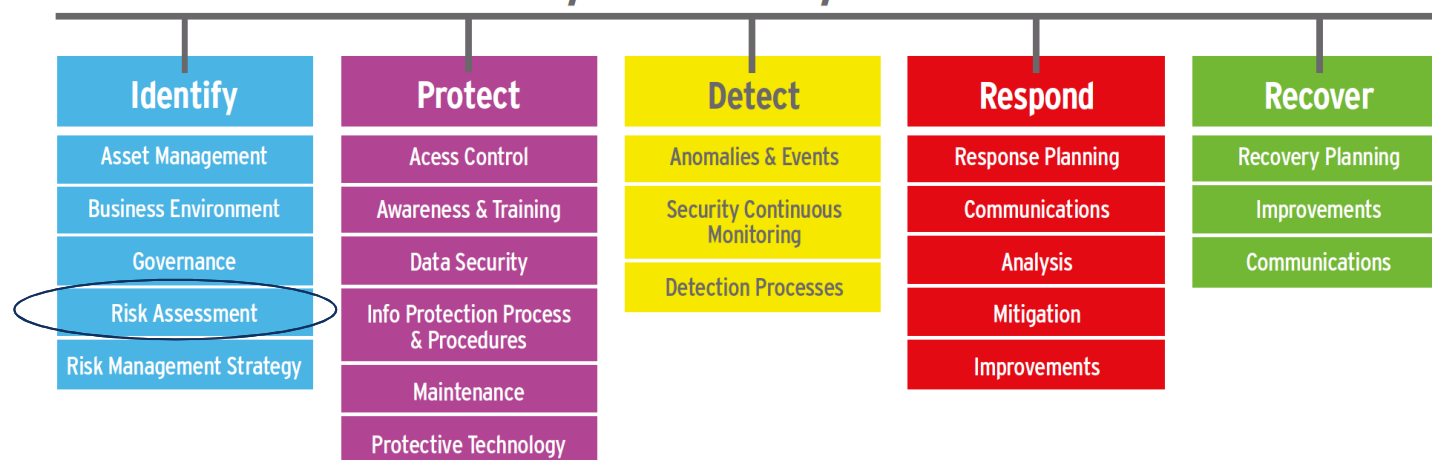
- Provides measures to lower cyber security risks on how to:
 - **Raise awareness** of the safety, security and commercial risks for shipping companies if no cyber security measures are in place;
 - **Protect shipboard OT and IT infrastructure** and connected equipment;
 - **Manage users**, ensuring appropriate access to necessary information;
 - **Protect data used onboard** ships, according to its level of sensitivity;
 - **Authorize administrator privileges** for users, including during maintenance and support on board or via remote link; and
 - **Protect data being communicated** between the ship and the shore side.



BIMCO GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

- In application to BIMCO guidelines, we have to refer to concrete standards to know how to perform the checkings:
 - NIST CYBER SECURITY FRAMEWORK (which is also mentioned in BIMCO guidelines);

NIST Cyber Security Framework



NIST : [National Institute of Standards and Technology](http://www.nist.gov) 5US
Department of Commerce)



DETERMINATION OF VULNERABILITY

■ Risk assessment

2 axis !

- Identification of **existing technical and procedural controls** to protect the onboard IT and OT systems.
- Identification of **IT and OT systems** that are **vulnerable**, the specific vulnerabilities identified, including human factors, and the policies and procedures governing the use of these systems
- Identification and evaluation of **key ship board operations** that are vulnerable to cyber attacks.
- These key operations should be protected in order to avoid disruption to commercial operations and ensure the safety of the crew, ship and the marine environment

IT :Information technology

OT : Operational technology

DETERMINATION OF VULNERABILITY

Identification of **possible cyber incidents** and their **impact** on key ship board operations, and the likelihood of their occurrence in order to establish and prioritize mitigating measures.

- Risk-priority matrix, L = low risk; M moderate risk; H = high risk; V =very high risk

Frequency of Occurrence (or Likelihood)	Consequences (Severity of Accident)				
	Incidental (1)	Minor (2)	Serious (3)	Major (4)	Catastrophic (5)
Frequent (5)	M	H	VH	VH	VH
Occasional (4)	M	M	H	Risk without measure	VH
Seldom (3)	L	M	H	H	VH
Remote (2)	L	L	Risk after measure	H	H
Unlikely (1)	L	L	M	M	H

DETERMINATION OF VULNERABILITY

- The high risk and very high consequences could be:
 - Commercial operations of the ship is stopped;
 - Cargo is lost
 - Ship is lost (grounding, etc.) ;
 - Dead passengers;

- Main efforts are to identify which weakness could lead to such catastrophic scenarios.

- Less protection (lower level) could be accepted for limited risk

- Has to be discussed at top management of company

DETERMINATION OF VULNERABILITY

For each cyberincident, the risk is evaluated considering the impact about Confidentiality, Integrity and Availability (CIA)

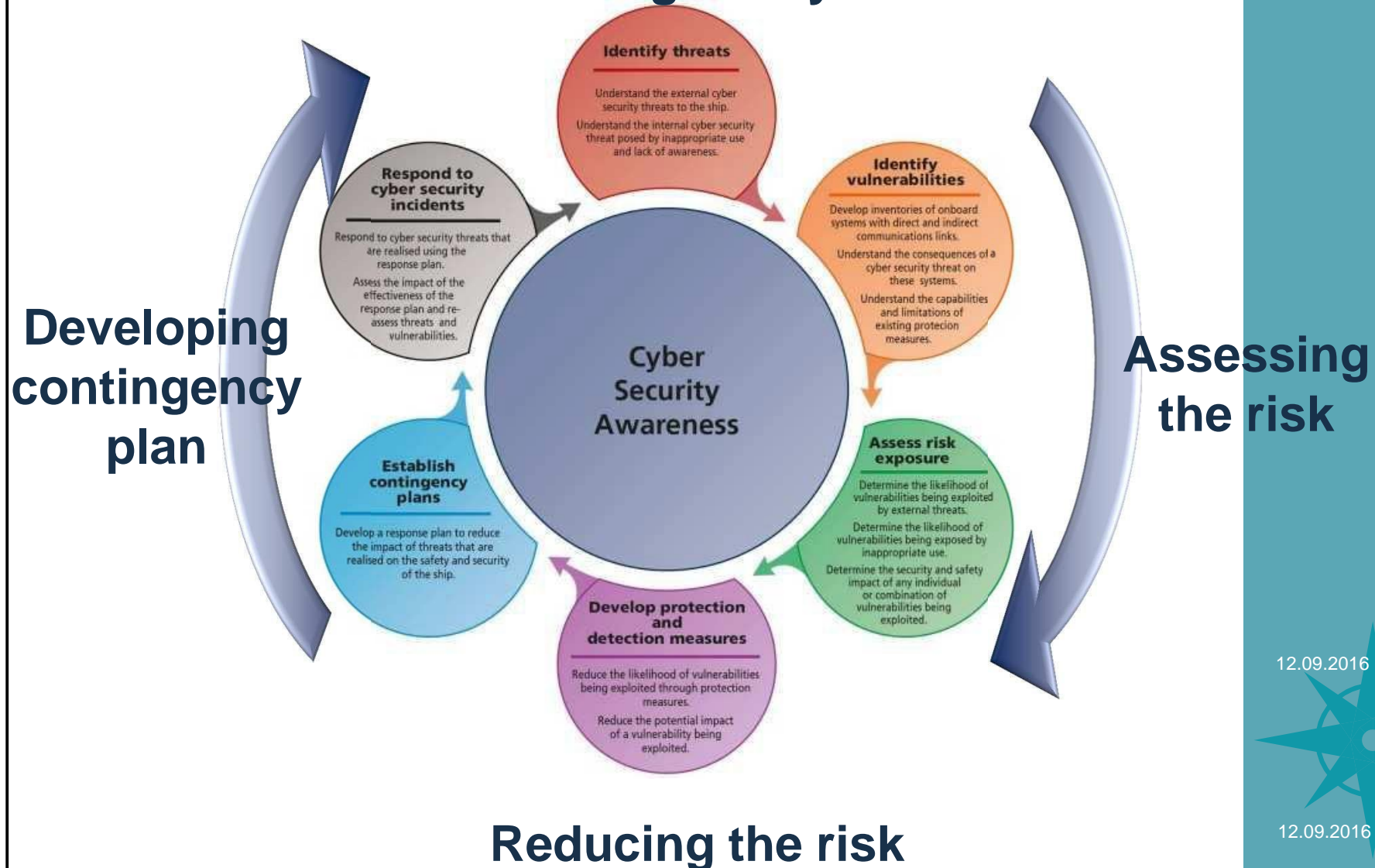
Exemple: Scada (Supervisory Control And Data Acquisition system controlling the distribution of onboard electric power)

SCADA system	Confidentiality	Integrity	Availability	Overall impact
Sensor data	Low	High	High	High
Statistical data	Low	Low	Low	Low



VIRTUOUS CYCLE FOR MITIGATING RISKS

Understanding the cyber threat



12.09.2016



12.09.2016



HOW TO IMPROVE CYBERSECURITY IN MARITIME INDUSTRY ?

Genova
18-21 September 2016

IUMI

- Performing risk assessments studies
 - At design level (builder),
 - For existing vessels (shipowner)
 - Use of assessment softwares

- Class societies are building their solutions to increase the safety of ships
 - Specific second Party audit (for the account of the Builder/Shipowner)
 - Defining rules to comply to obtain a Cybersecurity additional notation (voluntary basis today)

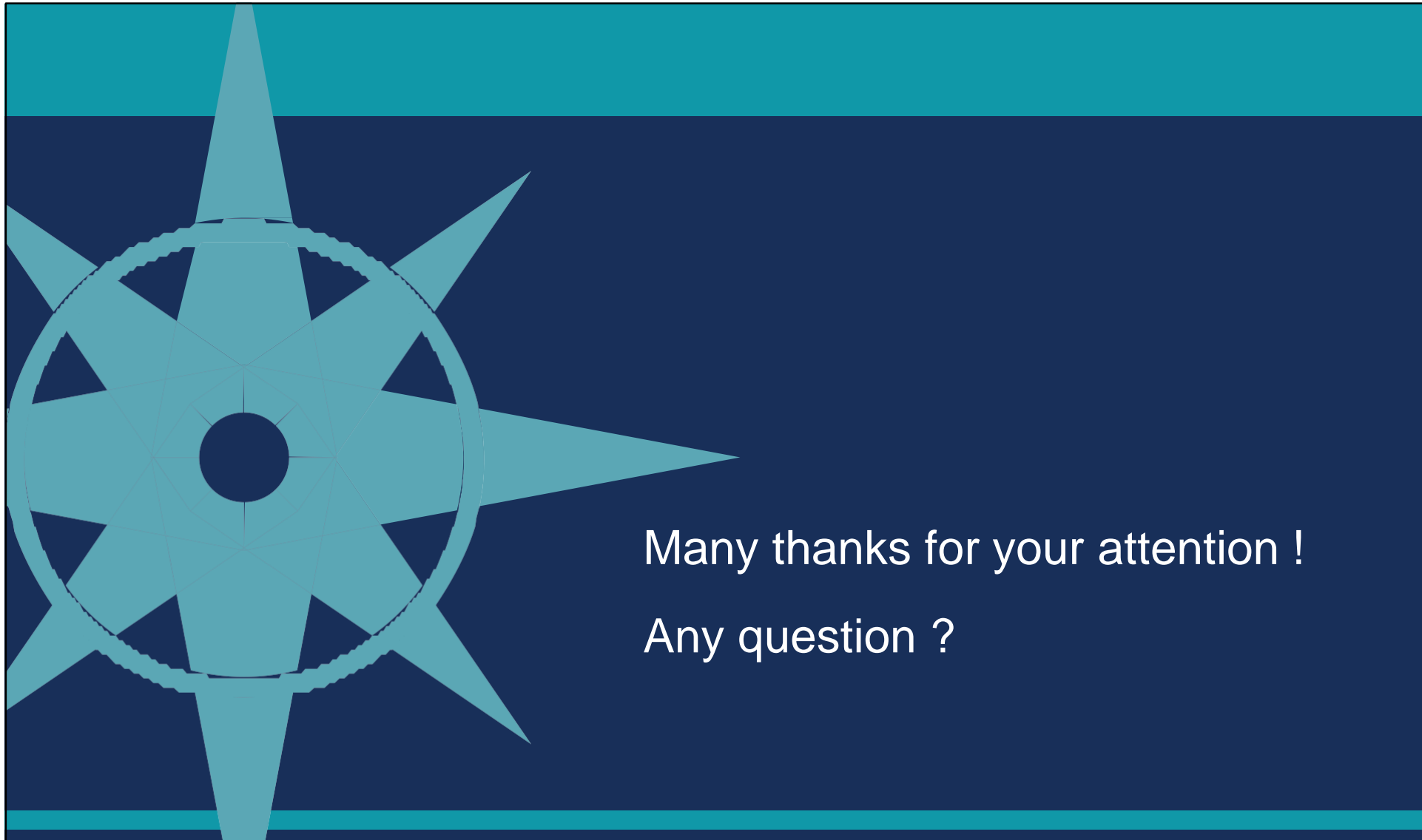
 - Idea is to perform checkings/approval for all the system, including the whole chain of suppliers.





CONCLUSIONS

- Cyber incidents are already a reality in maritime industry
- Application of BIMCO guidelines would enable to decrease vulnerability in maritime world by assessing and mitigating risks
- Some shipowners show low concern about cybersecurity, but the awareness increases during last years
- Ships and shipping companies are highly vulnerable today and will be more and more vulnerable if cybersecurity risks are not properly adressed !



Many thanks for your attention !

Any question ?

Genova
18-21 September 2016

IUMI



Yohan LE GONIDEC
Naval Architect/ Shipowner support
TECNITAS /BV SERVICES DEPT
FRANCE
yohan.le-gonidec@tecnitas.com