Risk assessment in maritime as a driver for good cyber security governance and compliance

Julian Gaunt (CISSP)

27 April 2023

MARLINK
ABOVE AND BEYOND

IMO resolution MSC.428(98)

*MSC-FAL.1/Circ.3 "Guidelines for Maritime Cyber Risk Management"

MARLINK
ABOVE AND BEYOND

What is a risk?

The probability that a particular security threat will exploit a particular vulnerability

A potential occurrence that may cause an undesirable or unwanted outcome for an organization or a specific asset

MARLINK
ABOVE AND BEYOND

Risk Management

- Cyber security **risk management** refers to the implementation of policies, procedures and practices in order to, manage cyber security risk.
- **Risk assessment** identifies and analyses security risks posed from threats that can be damaging to: Operations, IT, OT, people, data/information etc.
- **Risk analysis** focuses on understanding the risks and determine the magnitude of damage they can cause.

MARLINK
ABOVE AND BEYOND

A business concern

2023

- **DNV:** LockBit ransomware

2020 - 2022

- **Port of Lisbon:** LockBit ransomware
- **Port of Houston:** vessel operations
- **IMO:** IT systems and website
- **CMA CGM:** “Ragnar Locker” - shipping, port operations & data breech
- **MSC:** customer website

2017

- **Saudi Petrochem:** “Triton” - OT safety systems
- **Maersk:** “Not Petya” (300m $)

2012

- **Saudi Aramco:** Shamoon (1 Billion $)

Information Technology (IT)

→ Mainly finance and reputation risks

Operational Technology (OT)

→ Life, Property & Environment + above risks

MARLINK
ABOVE AND BEYOND

How much exposure do you have to a cyberattack?

Or What's your "Risk appetite"?

MARLINK
ABOVE AND BEYOND

Start with a “Risk Assessment”

Many standards and methods as guidance:

- **ISO/IEC 27005:2018** - ‘Information technology — Information security risk management — Security techniques ’
- **NIST SP 800–30 REV.1** - ‘Guide for Conducting Risk Assessments’,
- **NIST SP 800–39** Managing information security risk’

Numerous Methodologies to choose from:

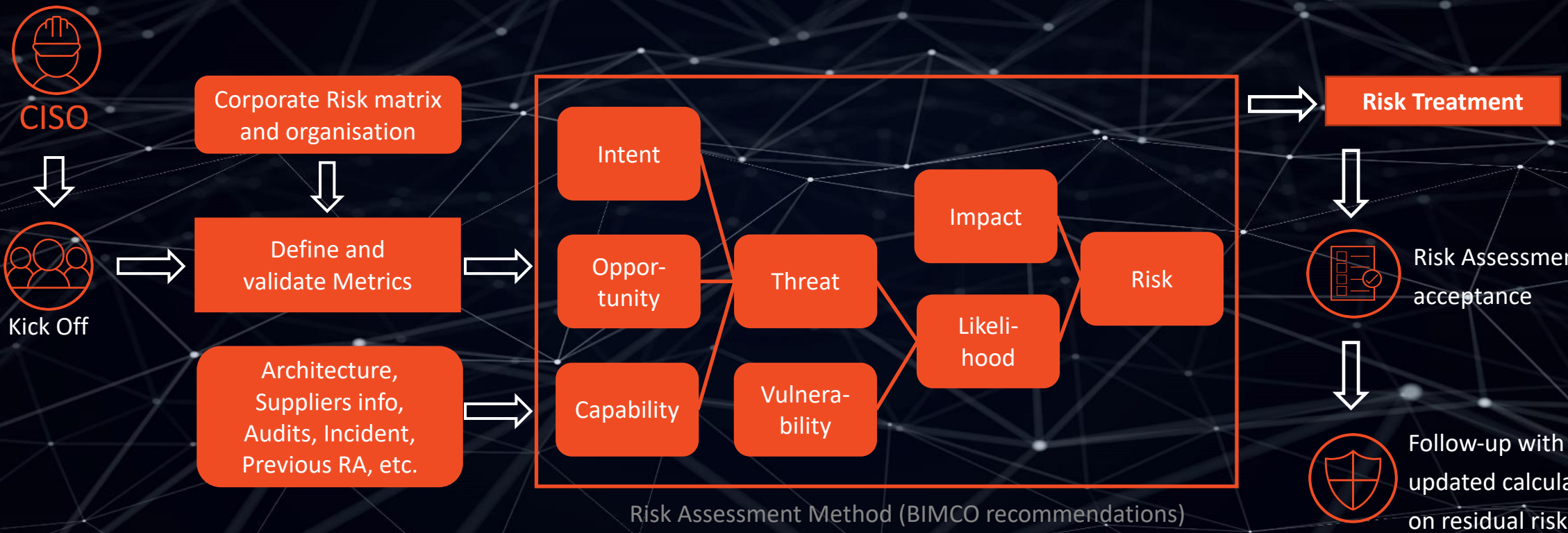
- BSI STANDARD 200-2, OCTAVE-S, ISACA, IRAM2, ETSI TS 102 165-1 (TVRA), EBIOS RISK MANAGER, EU ITSRM, MEHARI, COSO, ANSI/ISA-62443-3-2-2020, ISRAM, … and many more

IMO recommendation:

- **IMO MSC-FAL.1/CIRC.3 GUIDELINES ON MARITIME CYBER RISK MANAGEMENT.**

MARLINK
ABOVE AND BEYOND

Risk Assessment in the organisation



Risk Assessment Method (BIMCO recommendations)

MARLINK
ABOVE AND BEYOND

Threat analysis

State-sponsored actors, **cybercriminals (54%)** and hacktivists were the **main threat actors** in 2021/2022

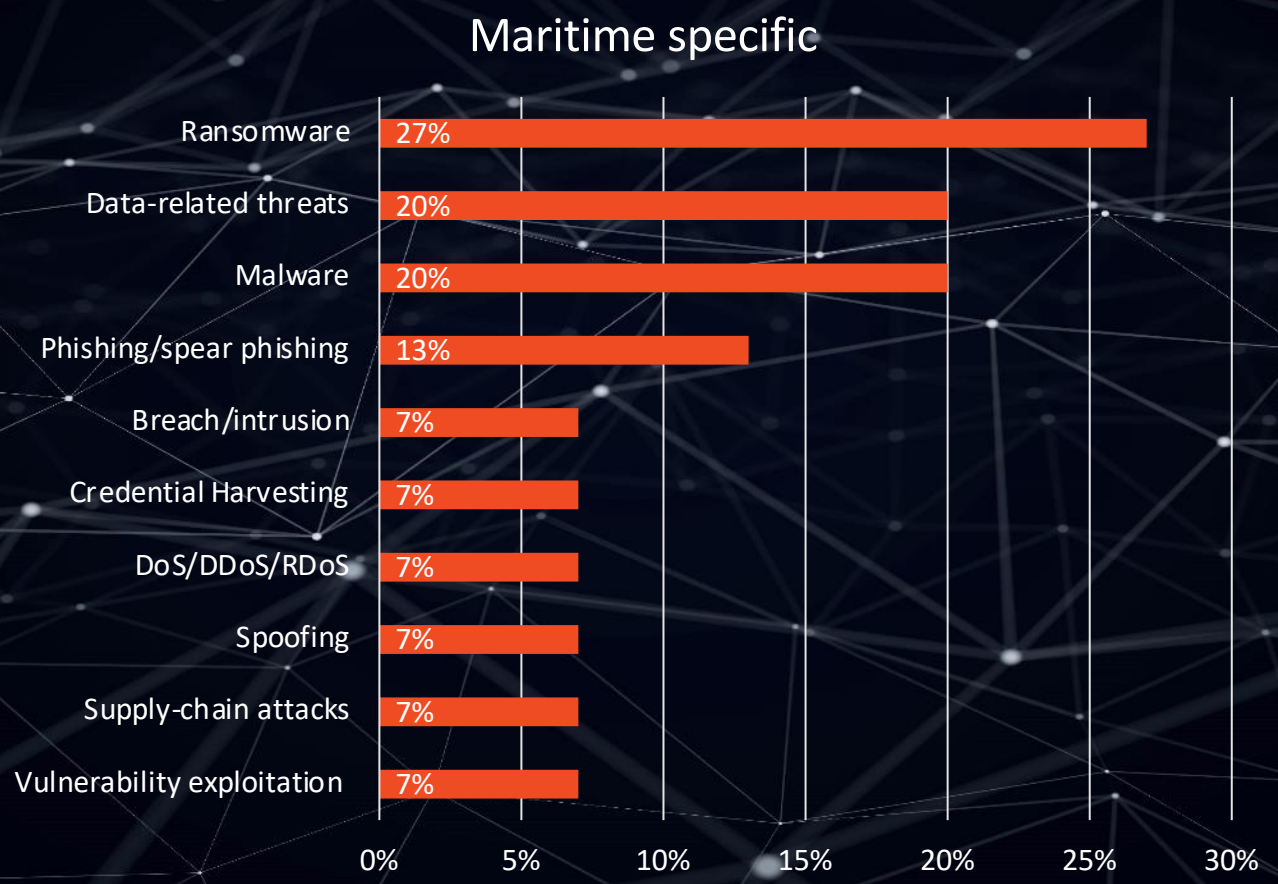
- Ransomware attacks main threat against the sector in 2022 (38%)
- Majority of attacks target **IT**. > Operational disruptions
- No reliable information on a cyberattack affecting the safety of transport
- **OT** were rarely targeted.

Forecast for 2023

- Hacktivist activity and DDoS attacks likely to continue
- Ransomware groups will likely target and disrupt OT operations

Ref: ENISA THREAT LANDSCAPE: TRANSPORT SECTOR (March 2023)

Threat analysis



Ref: ENISA THREAT LANDSCAPE: TRANSPORT SECTOR (March 2023)

MARLINK
ABOVE AND BEYOND

Vulnerability analysis

IACS UR E26 **requirements**

- Asset Inventory of all Hardware/Software/IT/OT/Networks …
- Clarify and document the processes and Organisation
- Analyse the vulnerabilities in the architecture, processes and people

Weight		2	2	1	1	1	1	
Supporting assets		Physical access	Logical Access	Patching	Malware protection	Documented procedures & staff training	Contingency plans	Vulnerability Level
Physical	Entry to Ship	3						3
	Entry to Ship telco room	2						2
	Entry to ship network room	1						1
Network	Satlink	1	3	2	3	1	3	3
	4G/5G	1	2	2	2	1	2	2
	Wired (switch 1)	1	2	1	2	1	2	2
	Wired (Router 1)	1	2		2	1	2	2
	Internal wifi 1	1	1	3	1	1	1	3
	Internal wifi 2	2	1	2	1	2	1	2
Systems	IT Server 1	3	3	1	3	3	3	3
	IT Server 2	1	2	1	2	1	2	2
	IT Server 3	1	2	1	2	1	2	2

MARLINK
ABOVE AND BEYOND

Impacts to operations / business

- Know what your trying to protect and what level you need to protect it
  - Safety of Crew
  - Maintain the Integrity of the vessel and the equipment aboard
  - Protect the Environment
  - Timely Navigation into and out of Port
  - Timely unloading and loading of ship
  - Maintaining integrity of Cargo
  - Wellbeing of Crew
  - …

Primary business functions	Description	Responsible	Impacts from failure of function				Severity
			Operations	Image	Financial	Regulation	
Timely navigation between ports delays (Low 1 day, High 2 days)	The captain navigates the ship using the instruments on the bridge to steer and propel the ship on the correct course and at the correct speed to meet the crossing plan.	**Ship Captain CEO**	2	2	1	1	**2**

MARLINK
ABOVE AND BEYOND

Risk Map

Major (5)	R2	R6			
Material (4)	R1				
Moderate (3)					
Minor (2)	R3	R4, R5, R9, R10, R11, R12			
Insignificant (1)		R7, R8			
Impact / likelihood	Rare (1)	Unlikely (2)	Neutral (3)	Likely (4)	Certain (5)

Some example of Risks:

R2 : Captain bringing malware infected USB into ship PC -> entry external threat via remote trojan.

Attacker (*APT) exploits lack of effective segregation to OT network --> compromises vessel safety to cause catastrophic disaster.

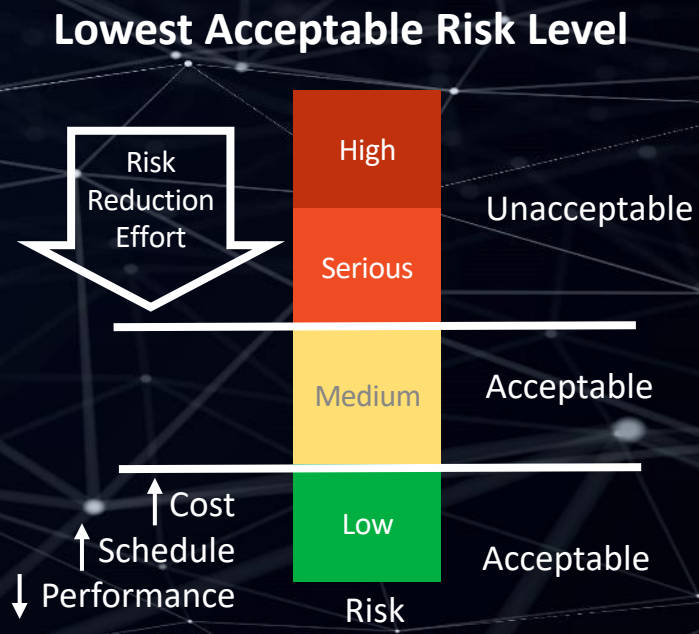
R1 : Crew member using admin network for personal internet access, infection on personal device introduces malware --> spreads inside networks causing DDOS
--> impacts to operational application.

**APT (Advanced persistent threat) by State based hacker or terrorist*

MARLINK
ABOVE AND BEYOND

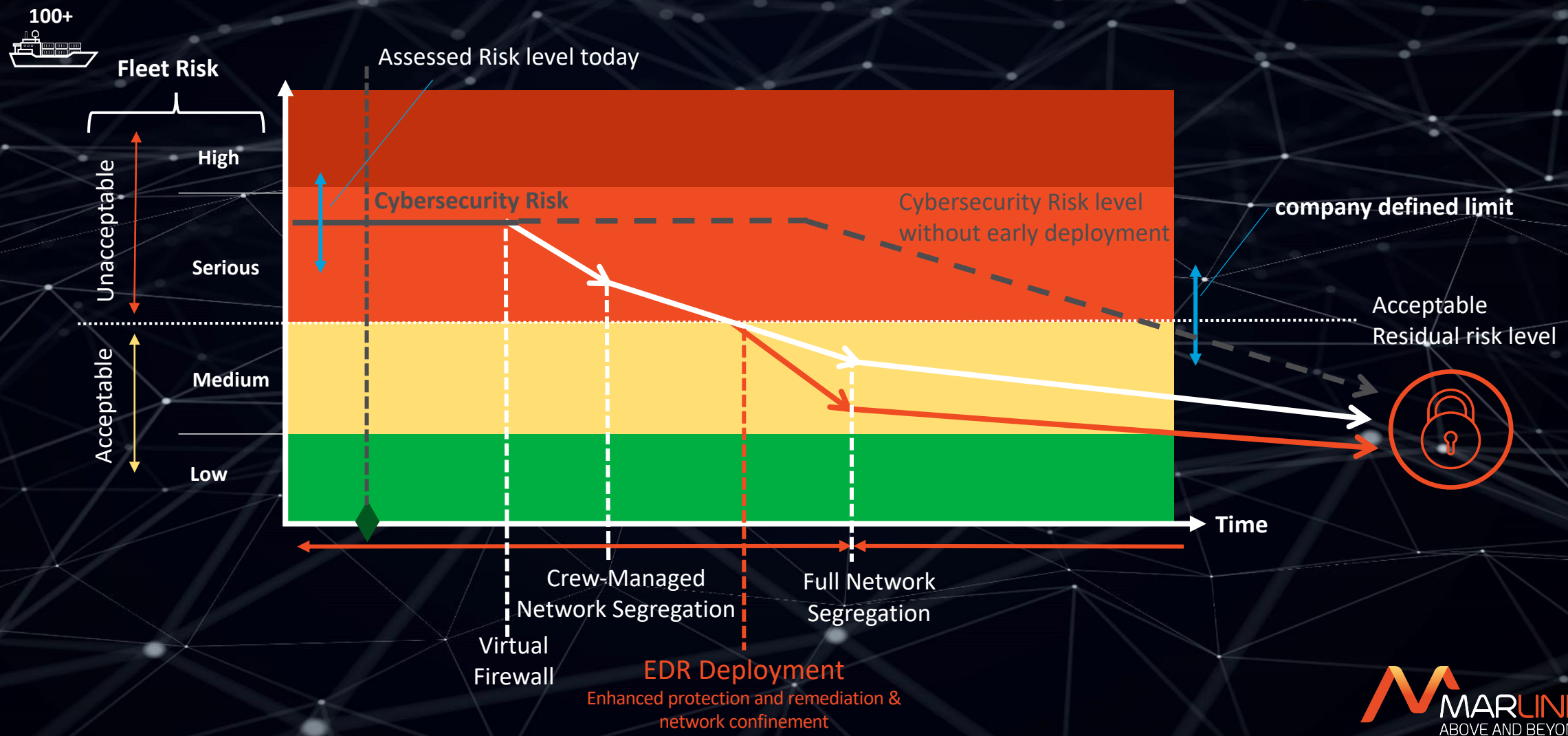
Risk Treatment

Major (5)	R2	R6			
Material (4)	R1	Risk to Treat			
Moderate (3)					
Minor (2)	R3	R4, R5, R9, R10, R11, R12			
Insignificant (1)		R7, R8			
Impact / likelihood	Rare (1)	Unlikely (2)	Neutral (3)	Likely (4)	Certain (5)



MARLINK
ABOVE AND BEYOND

Risk Management to drive a better security posture



MARLINK
ABOVE AND BEYOND

Benefits of Risk Management

- Increased Safety
- Reputation
- Cost Savings
- Continuous Improvement
- Compliance
- Resilience

Business can make better informed decisions on ways to prevent and mitigate cyber security risks based on their probability and outcome.

MARLINK
ABOVE AND BEYOND

Conclusion

Step 1: Identify

- Know your Risk level
  → Do a Risk Assessment

Step 2: Confront the threat

- Implement governance (Risk management)
  → Update and manage the risk!

MARLINK
ABOVE AND BEYOND

Marlink´s Digital Portfolio

Cyber Security solutions & Services

Hybrid Connectivity & Cloud

IoT solution & Analytics

Network & IT Management

Crew Welfare

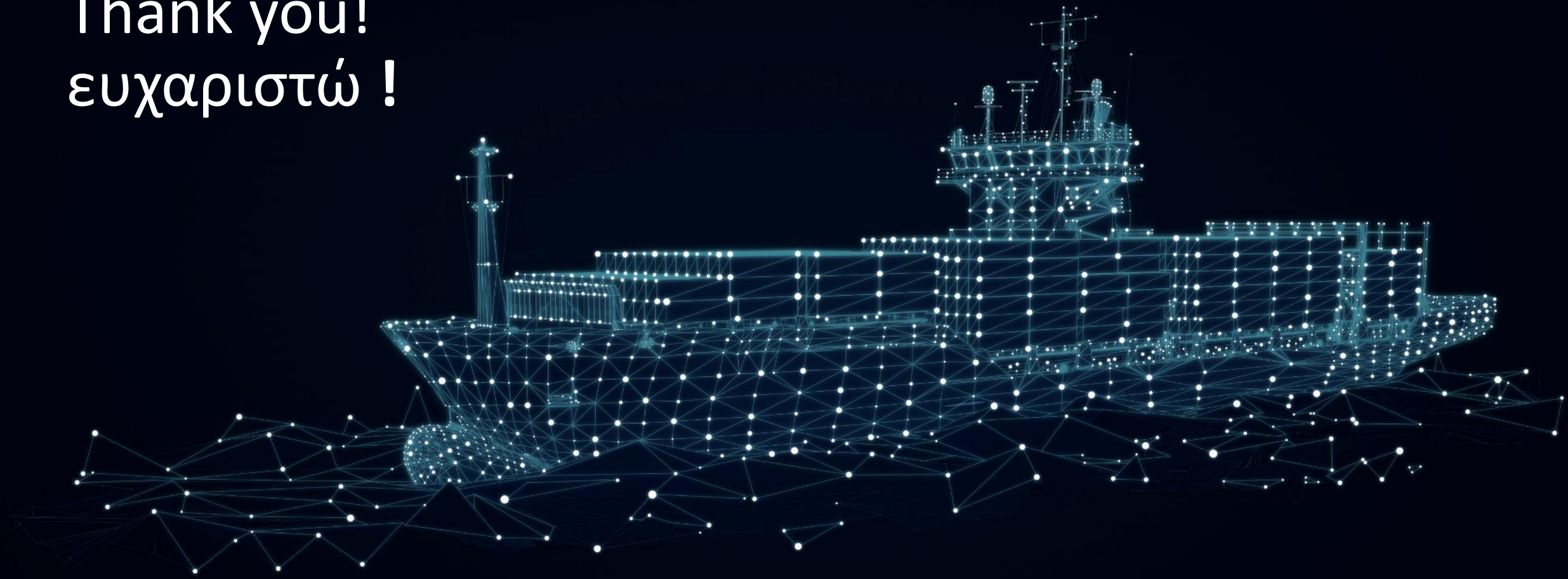
Managed Services

Telemedicine

Marlink's Digital Portfolio is build around providing Problem Solving solutions , services and Creating Value to our customers.

MARLINK
ABOVE AND BEYOND

Thank you!
ευχαριστώ !



Julian Gaunt Julian.Gaunt@marlink.com Cybersecurity Expert
Dimitris Moros Dimitris.Moros@marlink.com Commercial Director Greece and Cyprus
Nabil Azar Nabil.Azar@marlink.com Sales Director Digital, Europe

MARLINK
ABOVE AND BEYOND