Cyber Threats in Maritime: Navigating in an Uncharted Territory
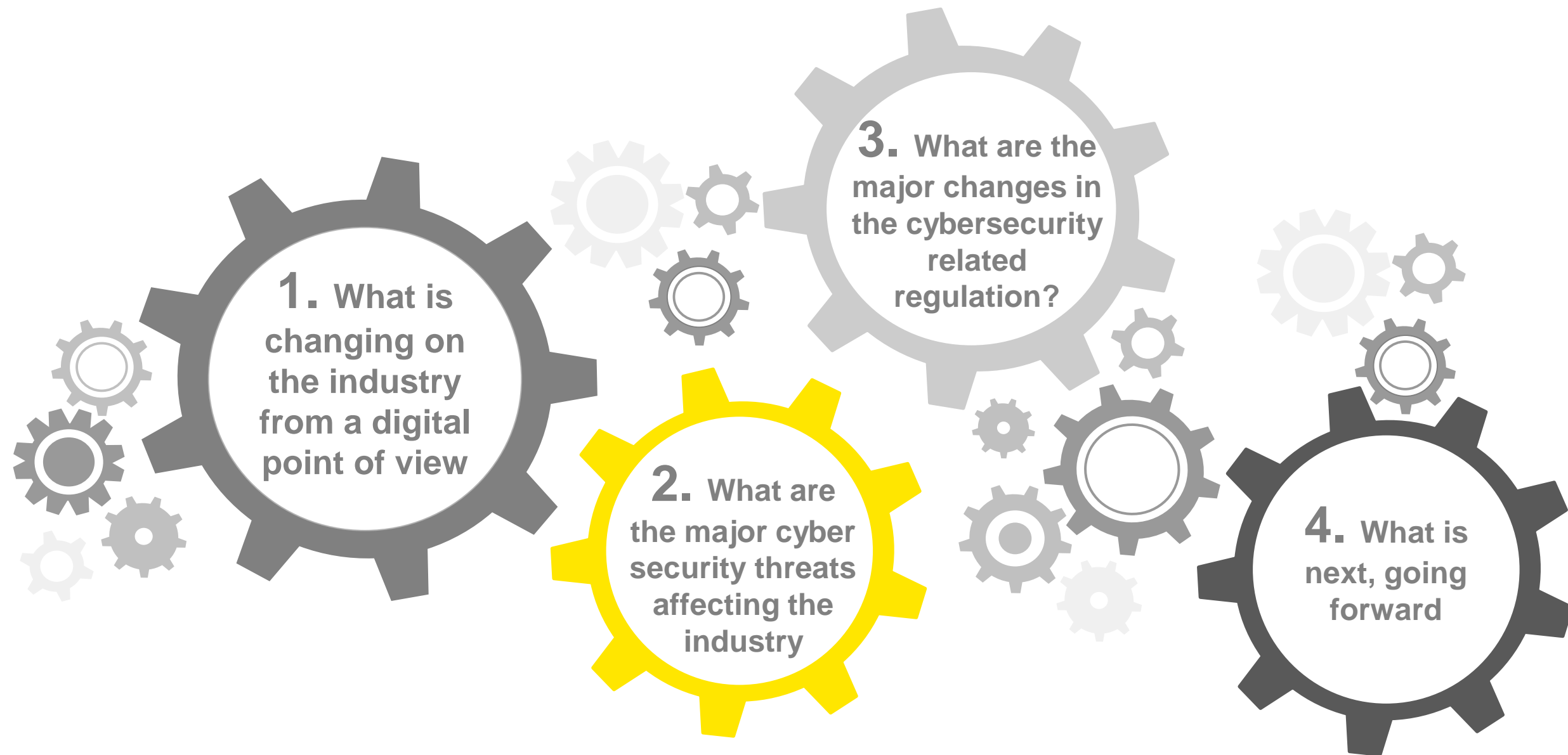
Panagiotis Papagiannakopoulos, Director,
EY Advisory Services, Head of Cybersecurity,
Data Protection & Privacy

The better the question. The better the answer.
The better the world works.

EY
Building a better
working world

Agenda

1. What is changing on the industry from a digital point of view

2. What are the major cyber security threats affecting the industry

3. What are the major changes in the cybersecurity related regulation?

4. What is next, going forward

EY

Things are only just starting to get interesting … and the growth has just begun

Connected IoT Devices

50
Billion
By 2020
Source: Intel
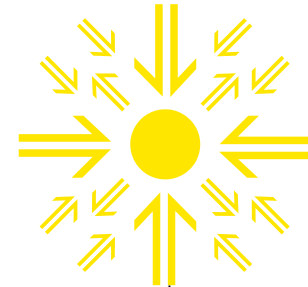
Smart Phones

1.9
Billion
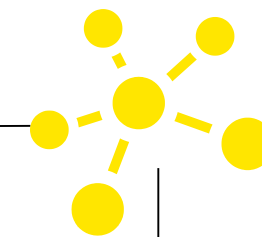By 2020
Source: IDC

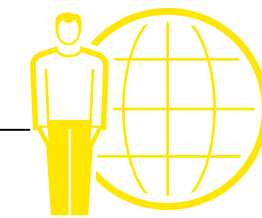Transformation

Data Universe

44
ZettaBytes
By 2020
Source: IDC
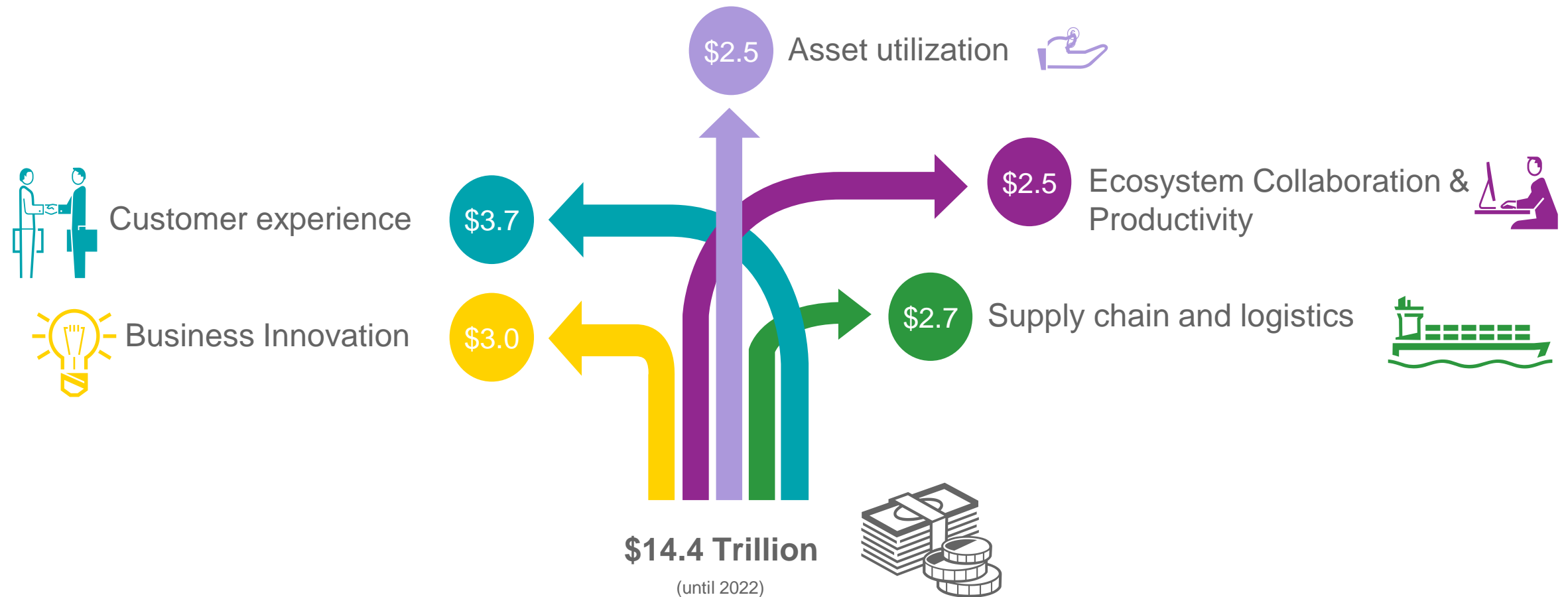
Internet Population

4
Billion
By 2020
Source: ITU/UNESCO

We have reached critical inflection points in many colliding **physical**, biological and **digital** technologies

EY

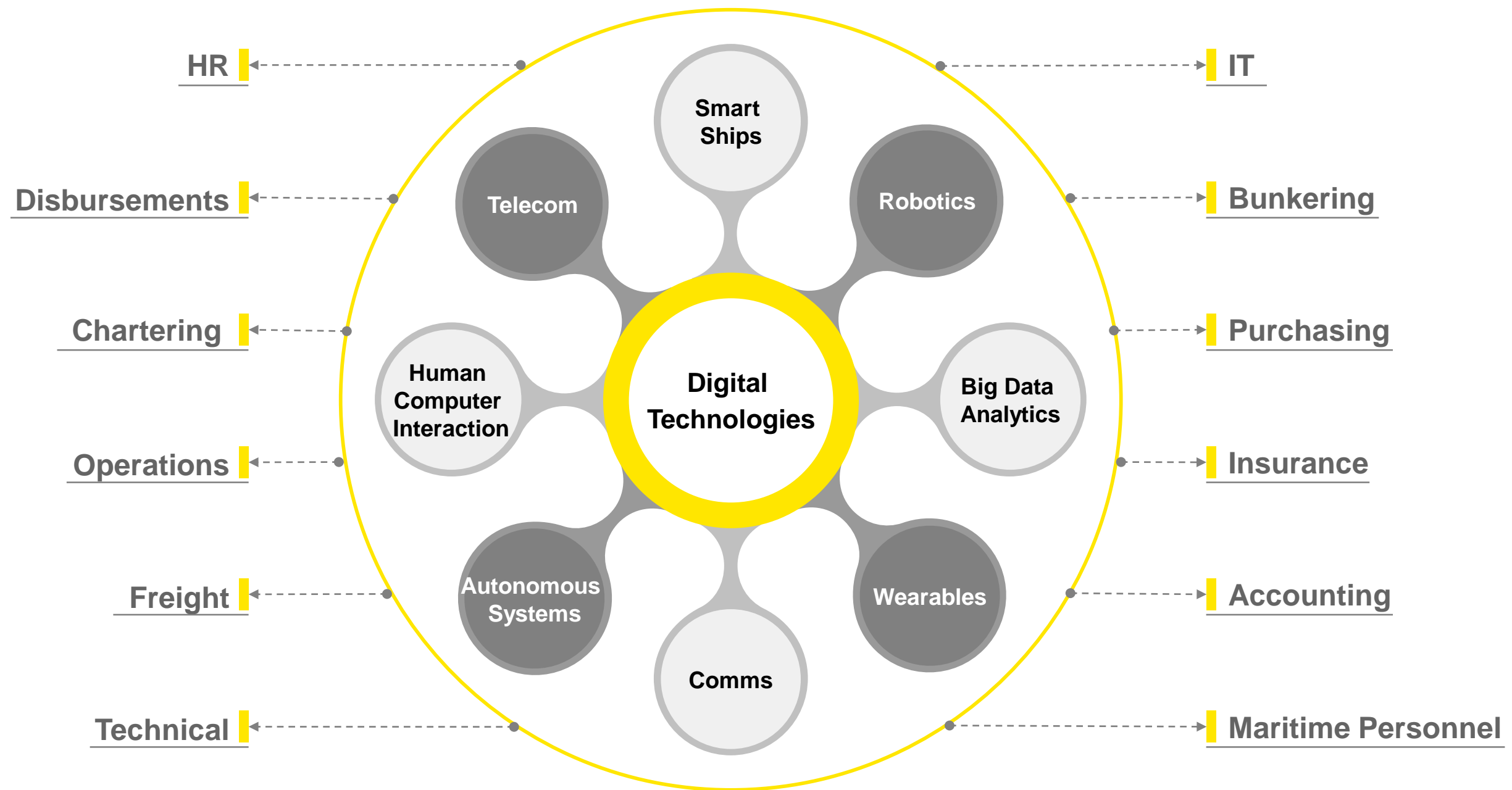# The IoT will generate tremendous value in all aspects of the value chain and business innovation

Value estimate generated by the Internet of Things in Trillion USD (until 2022)

$2.5 Asset utilization

Customer experience — $3.7

$2.5 Ecosystem Collaboration & Productivity

Business Innovation — $3.0

$2.7 Supply chain and logistics

$14.4 Trillion

(until 2022)

EY

The Shipping industry is transforming, embracing the digital era

HR
Disbursements
Chartering
Operations
Freight
Technical

IT
Bunkering
Purchasing
Insurance
Accounting
Maritime Personnel

Telecom
Smart Ships
Robotics
Human Computer Interaction
Digital Technologies
Big Data Analytics
Autonomous Systems
Comms
Wearables

EY

Cyber threat actors
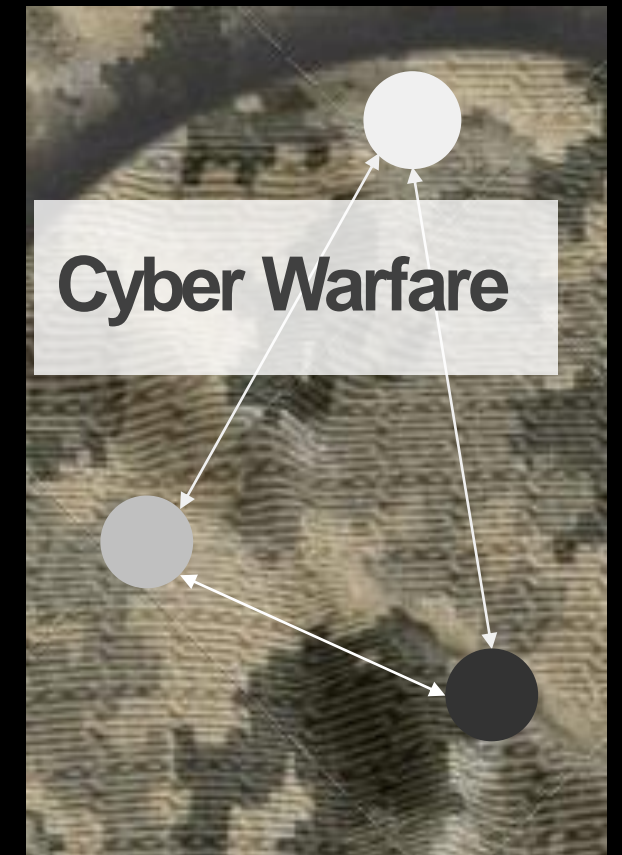

Cyber Crime

Hacktivism

Cyber Warfare

eSpionage

Cyber Terrorism

EY

Maritime cyber attacks is a reality and is happening now

Cyber Crime
Hacktivism
Cyber Warfare
eSpionage
Cyber Terrorism

- On board (ship) systems
- Cargo Systems
- On shore systems
- Propulsion
- Navigation systems
- People

Maritime cyber attacks

Cyber-attack on the Islamic Republic of Iran Shipping Lines –
The attacks damaged all the data related to rates, loading, cargo number, date and place resulting in severe financial losses.

A bug in a popular maritime platform left ships exposed
Flaws in the AmosConnect 8 software, would expose extensive operational and personal data and could even undermine other critical systems on a ship meant to be isolated.

First case of ghost shipping -
Drug traffickers hacked into the computer controlling shipping containers at the port of Antwerp

Malware was uploaded into the main computing system of the MODU

Multiple ransomware cases in the Greek market

EY

Several changes in the regulatory landscape are trying to increase cybersecurity readiness and trust

ENISA II – new mandate ☑

eIDAs Directive – article 19 ☑

EU Cyber Security Strategy (COM) ☑

General Data Protection Regulation (GDPR) ☑

The NIS Directive 👍

cPPP ☑

EU Cloud Computing Strategy and Partnership (COM) ☑

EU's CIIP action plan ☑
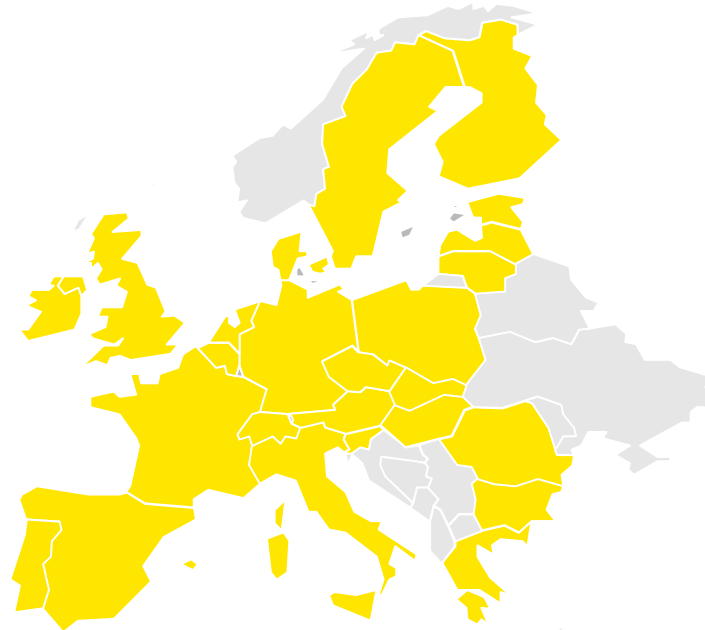
Digital Single Market Strategy (DSM) ☑

Telecom Package – article 13 a, art. 4 ☑

EY

Data is personal, GDPR will ensure it stays that way

Enforcement date: 25 May 2018

GDPR Impacts

- ► Penalties for failing to comply may lead to **fines up to €20 million or 4%** of the organization's **total global revenue**
- ► Re-enforced **data subjects' rights**
- ► Less than **eight months** to implement changes and comply
- ► Imposes **new obligations** for both controllers and processors of personal data
- ► Places a greater emphasis on **accountability**, requiring greater documentation and records

Impacted Areas

Employee Data

Customer Data

Ecosystem & Third Parties

Key Challenges

1 Clear Vision

2 Sponsorship

3 Business / IT Engagement

4 Programme Governance

5 Budget / Prioritisation

IAPP-EY Annual Privacy Governance Report 2017

EY

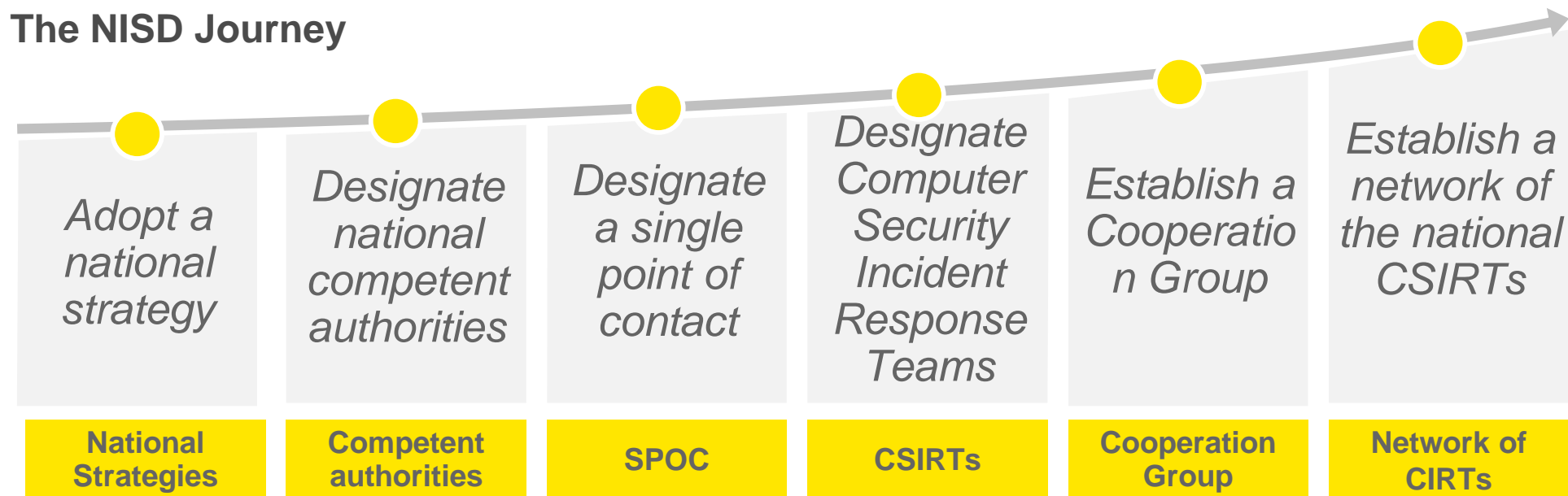# Directive on Security of Network and Information Systems

What is NISD?

The Directive was adopted on 6 July, 2016 and is the first EU horizontal legislation addressing cybersecurity challenges and a true game changer for cybersecurity resilience and cooperation in Europe.

Key Objectives

1 **Improve cybersecurity capabilities at national level**

2 **Build and increase cooperation at EU level**

3 **Promote a culture of risk management and incident reporting among OES and DSPs**

The NISD Journey

Adopt a national strategy	*Designate national competent authorities*	*Designate a single point of contact*	*Designate Computer Security Incident Response Teams*	*Establish a Cooperation Group*	*Establish a network of the national CSIRTs*
National Strategies	**Competent authorities**	**SPOC**	**CSIRTs**	**Cooperation Group**	**Network of CIRTs**

Sectors

‣ Energy infrastructures
‣ **Transport**
‣ Banking ‣ Health
‣ Financial market ‣ Water
‣ Digital infrastructure

Appropriate **security measures** & notification of **serious incidents**

‣ **Preventing risks**
‣ **Ensuring security of network and information systems**
‣ **Handling incidents**
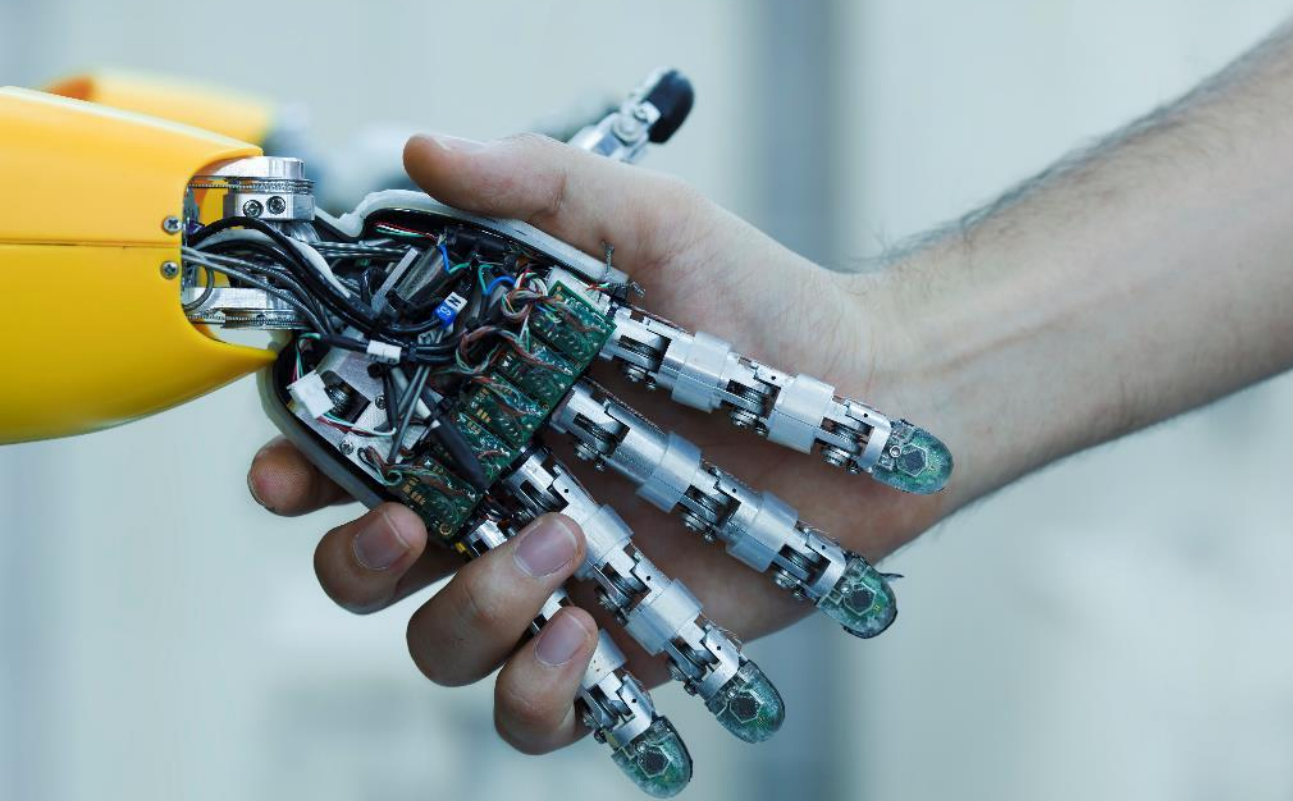
Transposition deadline

9 May 2018

Deadline for the identification of OES

9 Nov 2018

EY

Key Takeaways for creating a cyber resilient enterprise

1 **Build a Cyber and Information Security function**

Having a dedicated team of cyber and information security experts is a key step towards enhancing your defense & compliance mechanisms

2 **Determine the critical assets – the crown jewels**

Organize and implement mechanisms and controls around what really matters, strategic plans, R&D, IP, etc

3 **Assess your current status**

Assess your cybersecurity posture and compliance gaps, will provide a rationale for prioritized investments

4 **Improve your level of defense & compliance**

Perform prioritized and justified actions towards improving the cybersecurity posture and level of compliance

5 **Manage the human element**

Awareness, clear communication, direction, and example setting from leadership are essential

6 **Be prepared**

100% security and compliance is a utopia. Be prepared on how to respond to potential incidents

EY

Thank you

Q & A

panagiotis.papagiannakopoulos@gr.ey.com
gr.linkedin.com/in/papagiannakopoulos
@ppapajohn

EY

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY's Advisory Services
In a world of unprecedented change, EY Advisory believes a better working world means solving big, complex industry issues and capitalizing on opportunities to help deliver outcomes that grow, optimize and protect clients' businesses. From C-suite and functional leaders of Fortune 100 multinationals to disruptive innovators and emerging market small and medium sized enterprises, EY Advisory teams with clients — from strategy through execution — to help them design better outcomes and deliver long-lasting results. A global mindset, diversity and collaborative culture inspires EY consultants to ask better questions. They work with the client, as well as an ecosystem of internal and external experts, to co-create more innovative answers. Together, EY helps clients' businesses work better.
The better the question. The better the answer. The better the world works.