Cyber Threats in Maritime: Navigating in an Uncharted Territory

Panagiotis Papagiannakopoulos, Director,
EY Advisory Services, Head of Cybersecurity,
Data Protection & Privacy

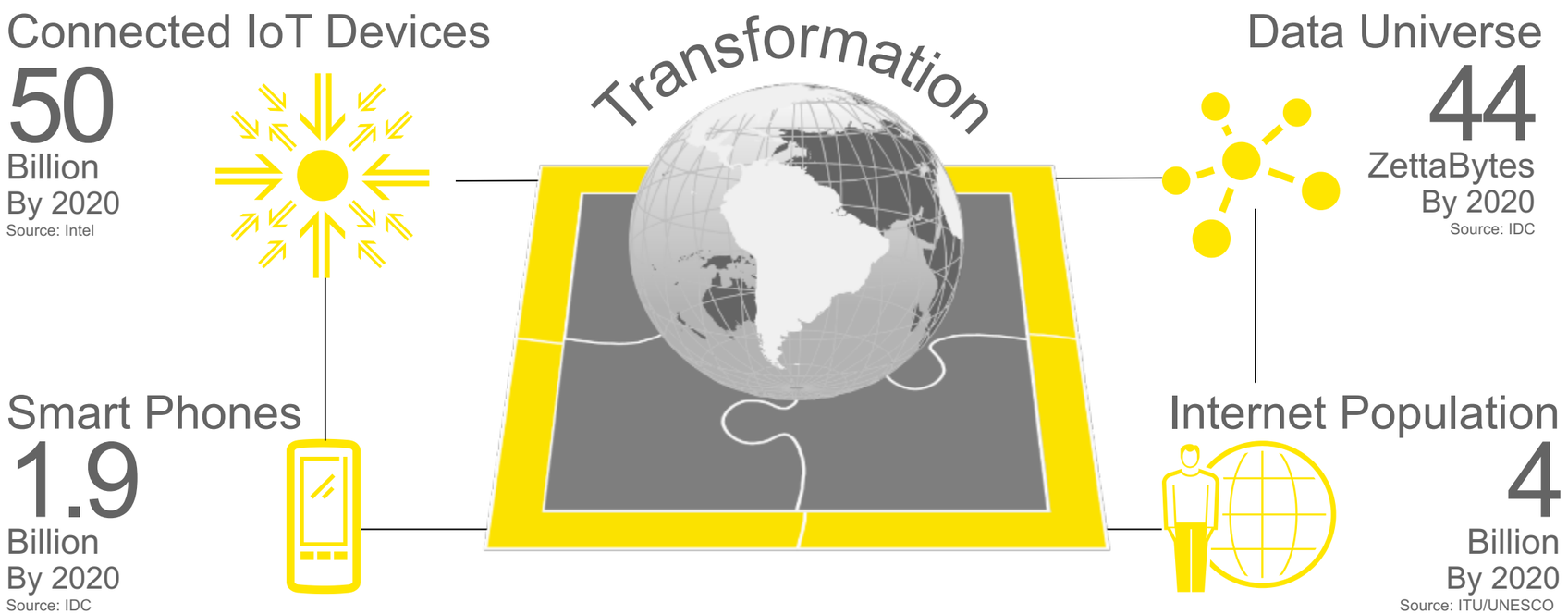
The better the question. The better the answer.
The better the world works.

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 does the transportation industry consider about cybersecurity
4. What is next, going forward

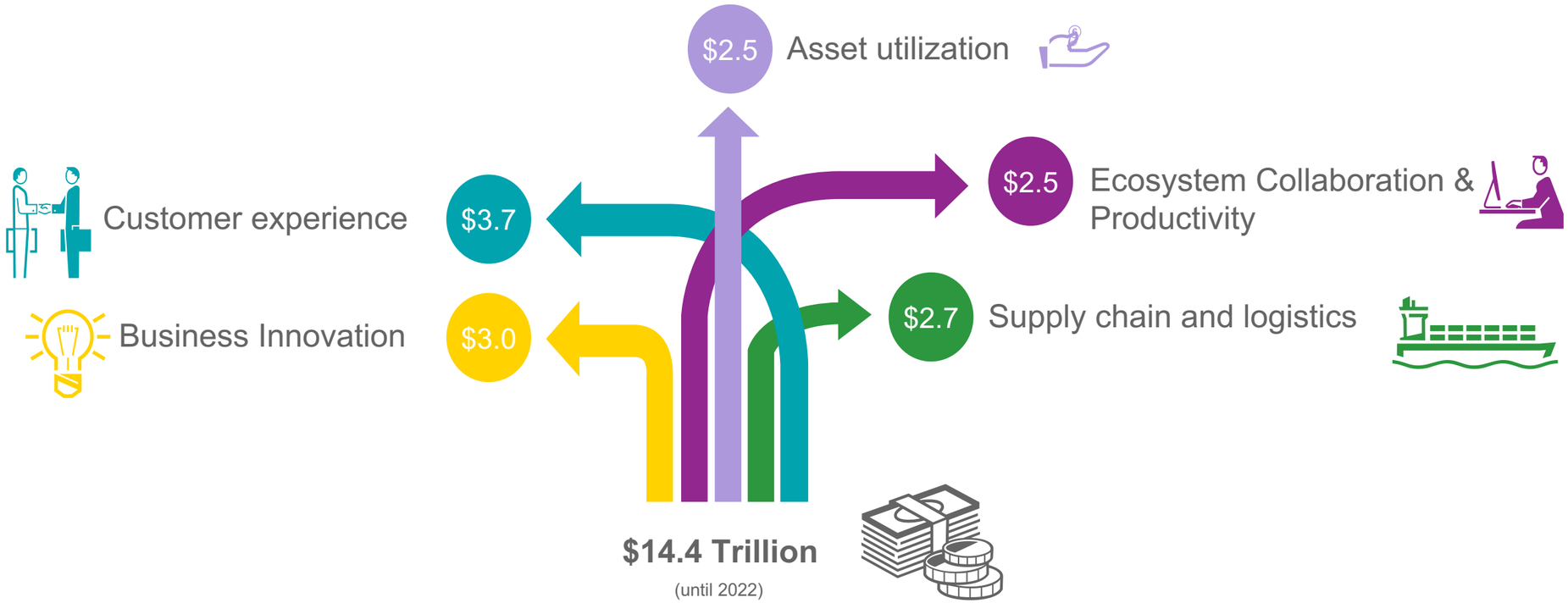
Things are only just starting to get interesting … and the growth has just begun



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

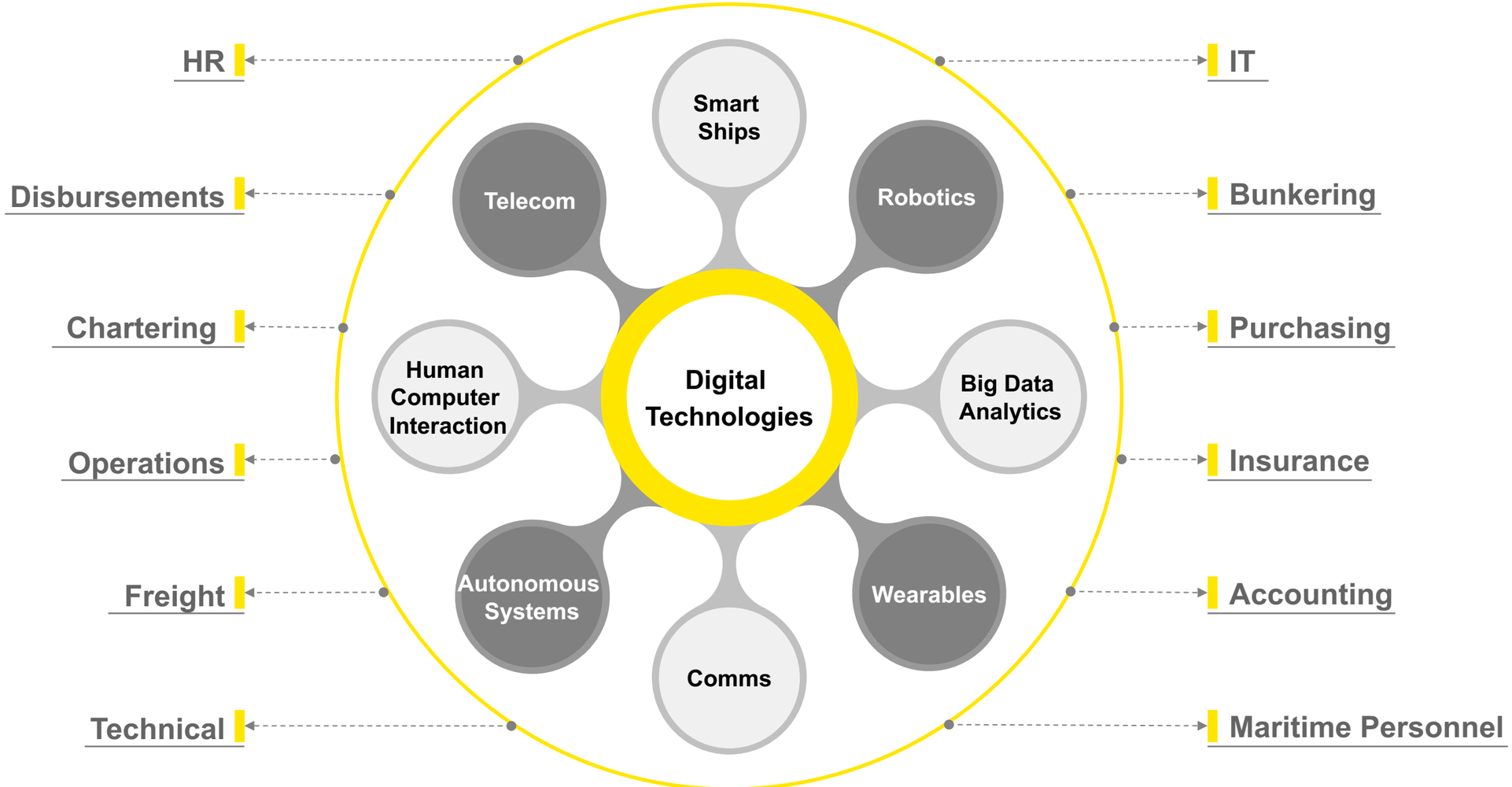
The IoT will generate tremendous value in all aspects of the value chain and business innovation

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

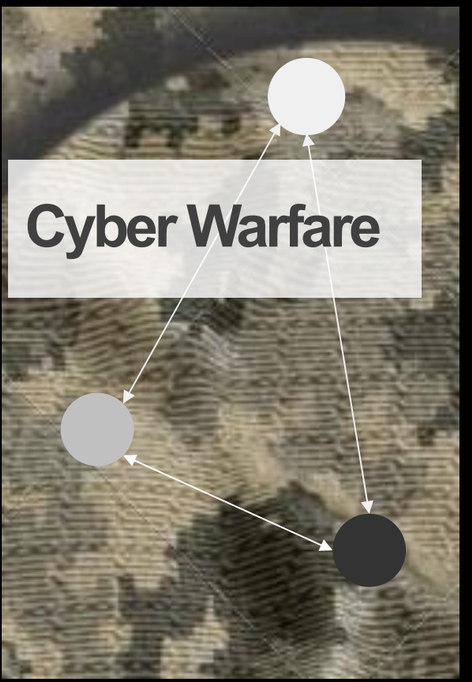


Source: Cisco white paper "Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion", 2013

The Shipping industry is transfo-rming, embracing the digital era

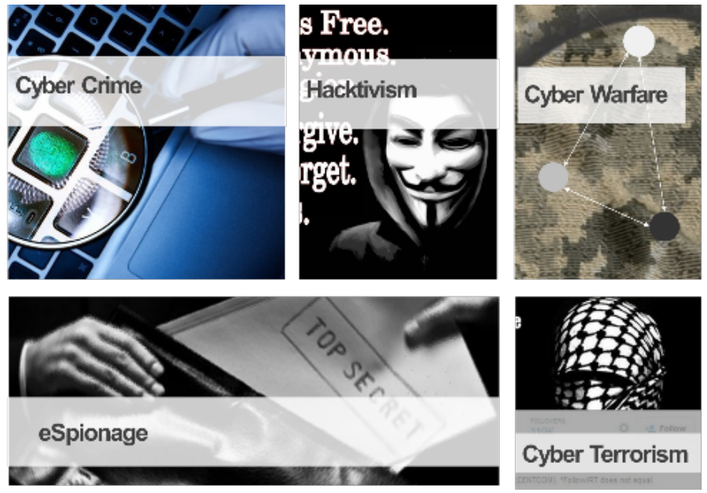


Cyber threat actors



Maritime cyber attacks is a reality and is happening now

Threat Actors



Attack Surface

- 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.

APT attacks on Japanese and South Korean maritime and shipbuilding groups

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

Organizations still have to evolve their Cyber security function

87%

of board members and C-level executives have said they lack confidence in their organisation's level of cybersecurity

86%

of responders say they need up to 50% more budget

57%

of responders have had a recent cybersecurity incident

44%
of responders

- Do not have any type of SOC function
- Do not have a threat intelligence program
- Do not have or have an informal vulnerability management program

Top Threats

- Careless or unaware employees
- Outdated information security controls or architecture
- Unauthorized access

Top Vulns

- Malware
- Cyber-attacks to steal financial information
- Phishing

What are your prorities?

1. Operational Resilience
2. Data leakage / data loss prevention
3. Security awareness

Source: EY - Global Information Security Survey 2016-2017 -Transportation Sector results

EY

Going forward

Grow

Enterprise strategy

Incubation and innovation

Optimise

Continuous Experience Implementation

Operations

Protect

Trust

In order to make this performance breakthrough, companies need to reinvent themselves in five capability areas

Sense, Resist, React

▸ Sense

The ability of organizations to **predict** and **detect** cyber threats:

- Cyber Threat Intelligence
- Vulnerability Identification
- Security Operations Center
- Cyber Security Analytics

▸ Resist

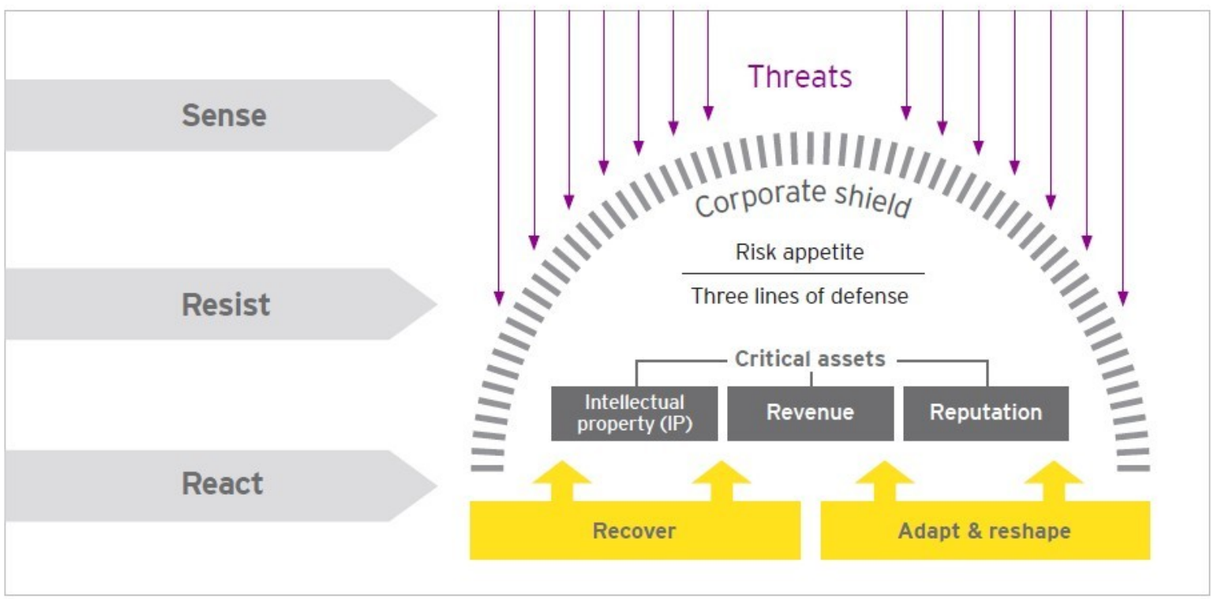
The corporate shield, starting with **how much risk** an organization is **prepared to take**:

- Software Security
- Identity and Access Management
- Network Security
- Data Protection

▸ React

Being ready to deal with the **disruption**, with **incident response capabilities**, **crisis management**, preservation of evidence and investigation of the breach.

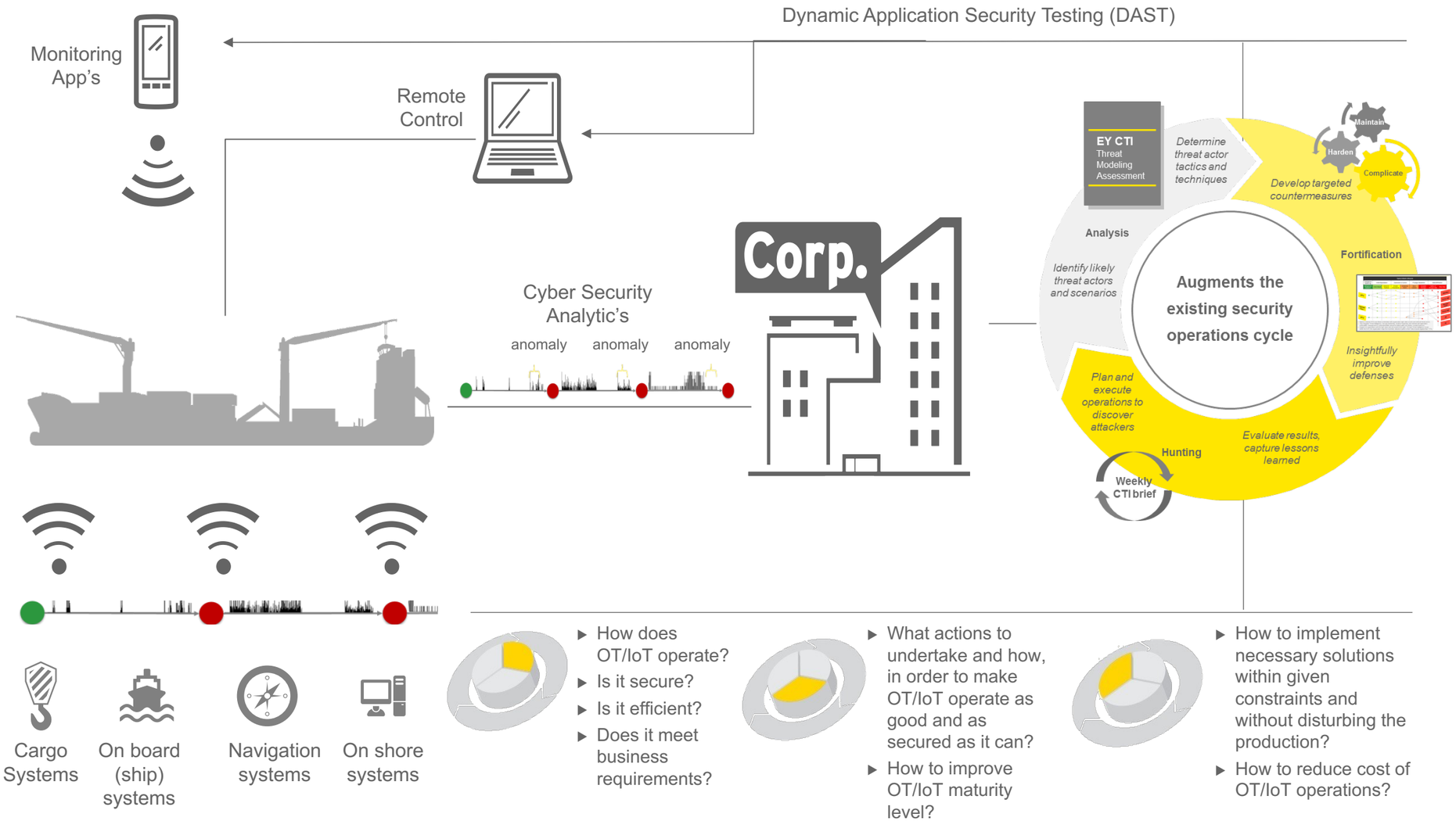
- Incident Response
- Resilience
- Crisis Management



Source: EY - Global Information Security Survey 2016-2017

Embed the Digital Ship in your Cyber Security Program

▸ Sense ▸ Resist ▸ React

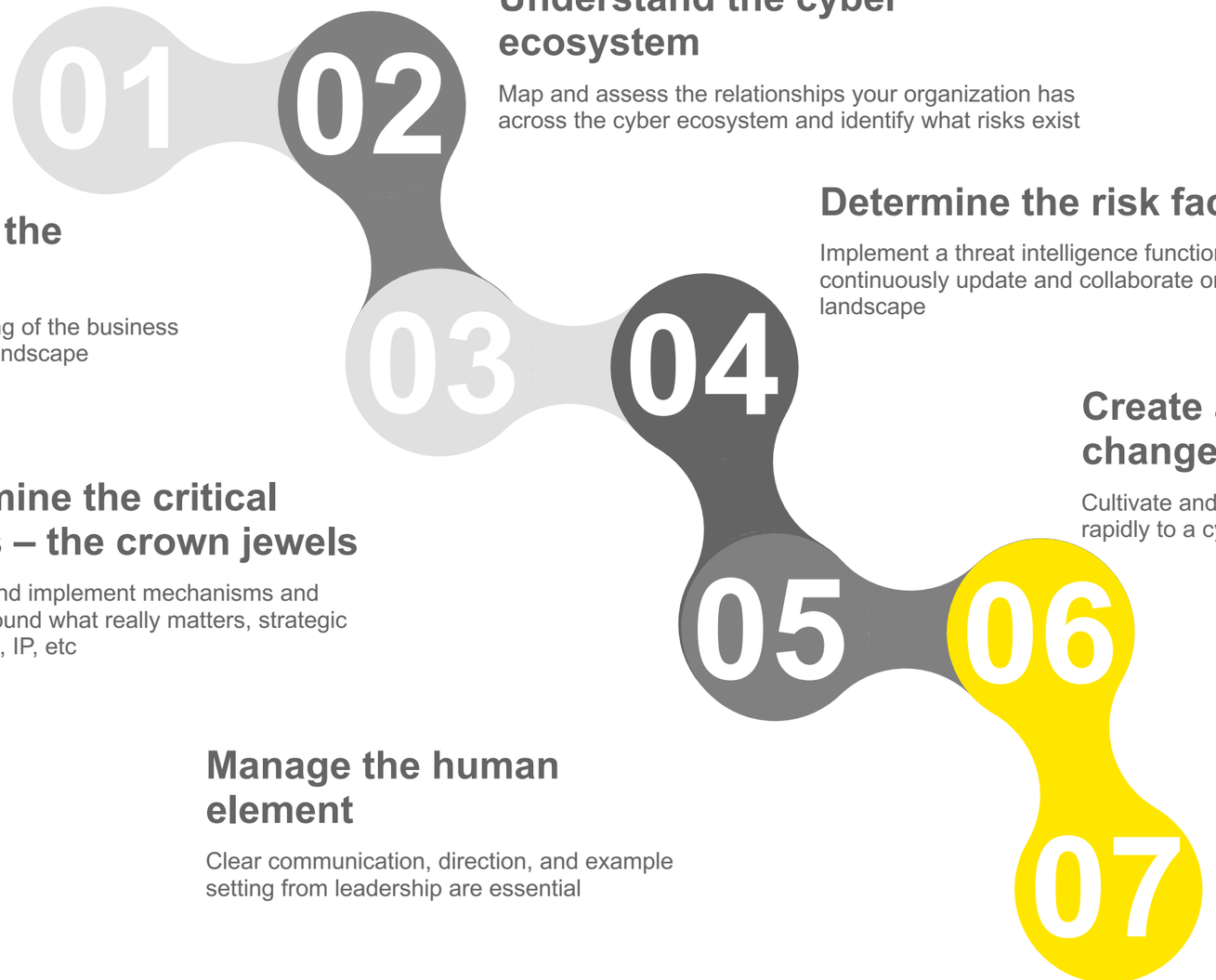


- How does OT/IoT operate?
- Is it secure?
- Is it efficient?
- Does it meet business requirements?

- What actions to undertake and how, in order to make OT/IoT operate as good and as secured as it can?
- How to improve OT/IoT maturity level?

- How to implement necessary solutions within given constraints and without disturbing the production?
- How to reduce cost of OT/IoT operations?

Key Characteri-stics of a cyber resilient enterprise



Understand the business

In depth understanding of the business and the operational landscape

Understand the cyber ecosystem

Map and assess the relationships your organization has across the cyber ecosystem and identify what risks exist

Determine the risk factors

Implement a threat intelligence function to continuously update and collaborate on the threat landscape

Create a culture of change readiness

Cultivate and train on the capability to react rapidly to a cyber attack

Determine the critical assets – the crown jewels

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

Manage the human element

Clear communication, direction, and example setting from leadership are essential

Be prepared and create an incident response scheme

Thank you

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

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.