The Cyber Security Policy Framework and Cyber Insurance

Dr. Athanasios Drougkas | Officer in NIS

Digital Ship Athens 2017| Athens | 1st November

Agenda

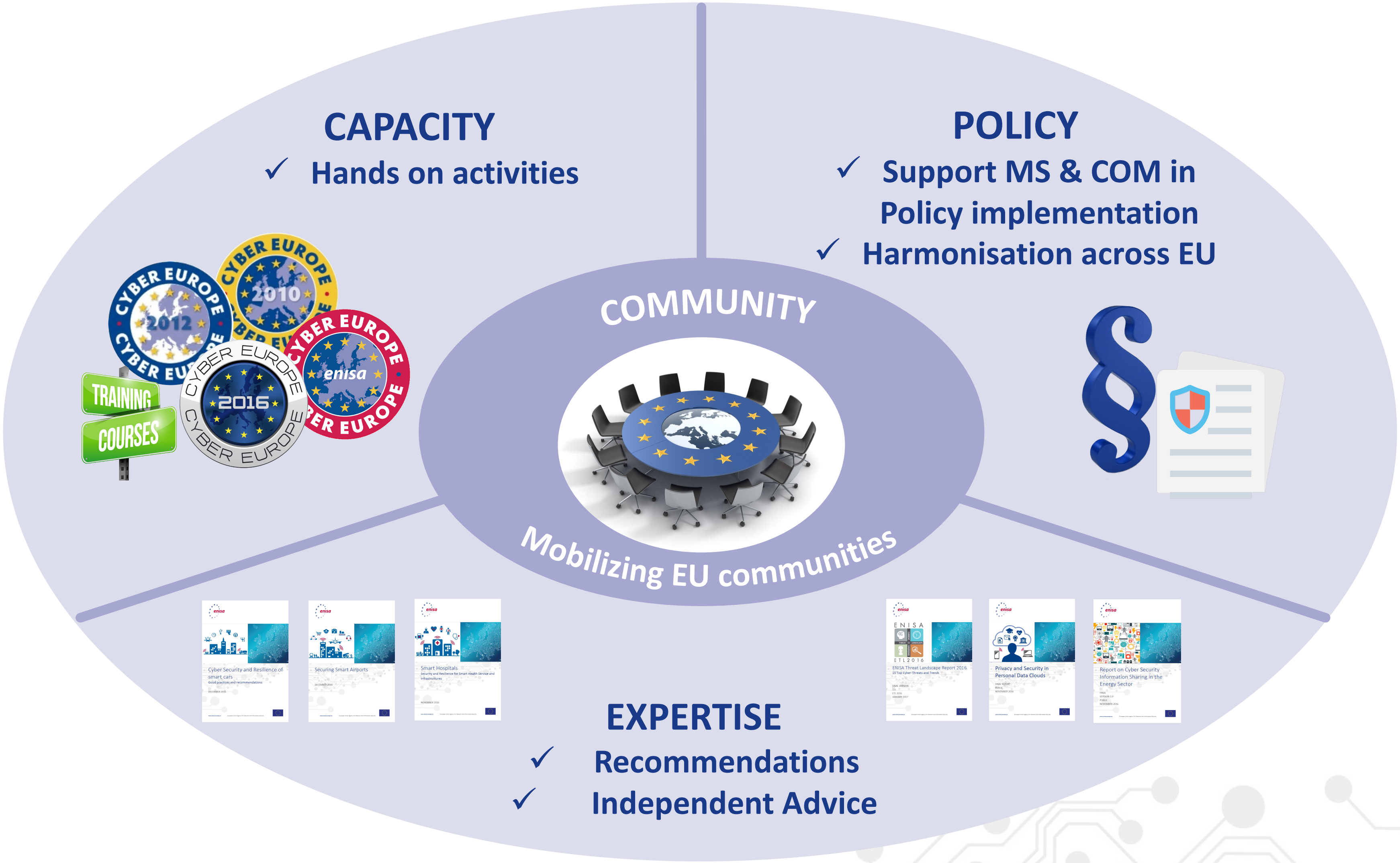
1 The NIS Directive and cybersecurity in Water Transport & relevant ENISA work

2 ENISA work on Cyber Insurance

The NIS Directive and cybersecurity in Water Transport & relevant ENISA work

Securing Europe’s Information society

Positioning ENISA activities



CAPACITY

- ✓ Hands on activities

POLICY

- ✓ Support MS & COM in Policy implementation
- ✓ Harmonisation across EU

COMMUNITY

Mobilizing EU communities

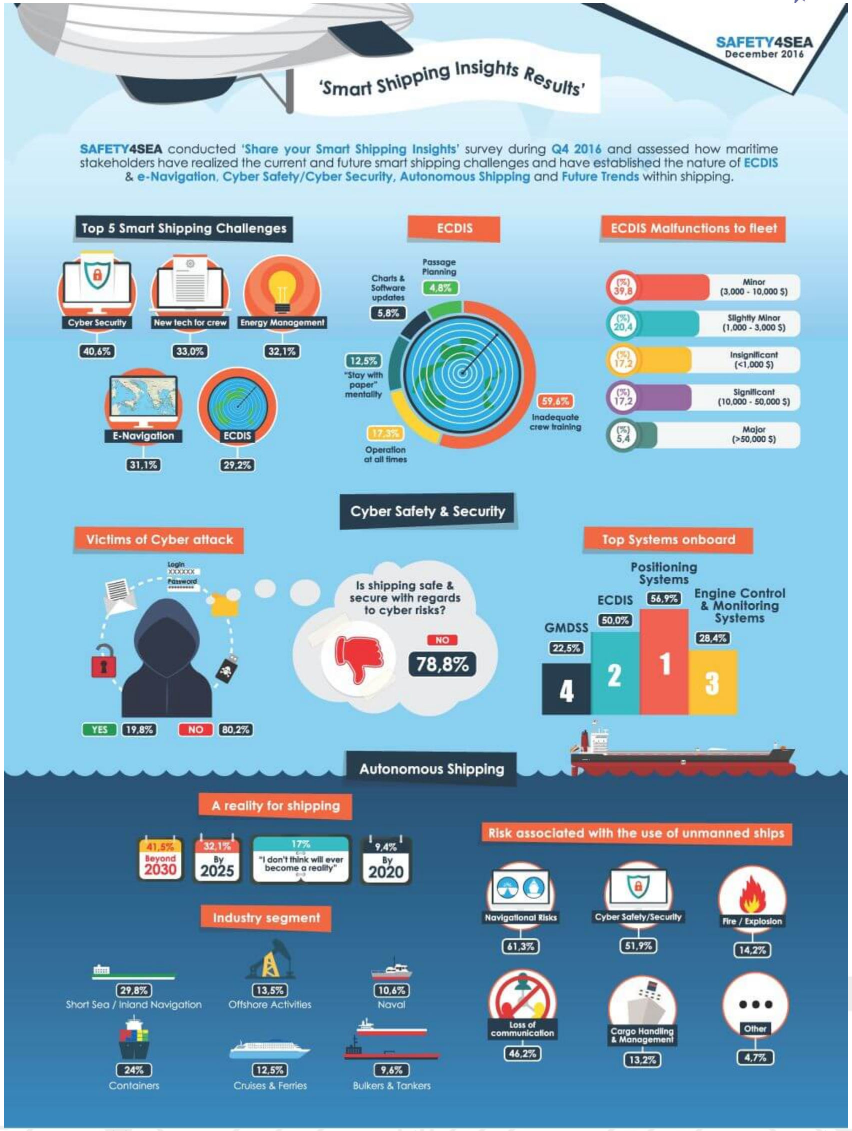
EXPERTISE

- ✓ Recommendations
- ✓ Independent Advice

CYBER EUROPE 2012
CYBER EUROPE 2010
CYBER EUROPE 2016
CYBER EUROPE enisa
TRAINING
COURSES
§
Cyber Security and Resilience of smart cars
Securing Smart Airports
Smart Hospitals
ENISA Threat Landscape Report 2016
Privacy and Security in Personal Data Clouds
Report on Cyber Security Information Sharing in the Energy Sector

Everything becomes connected

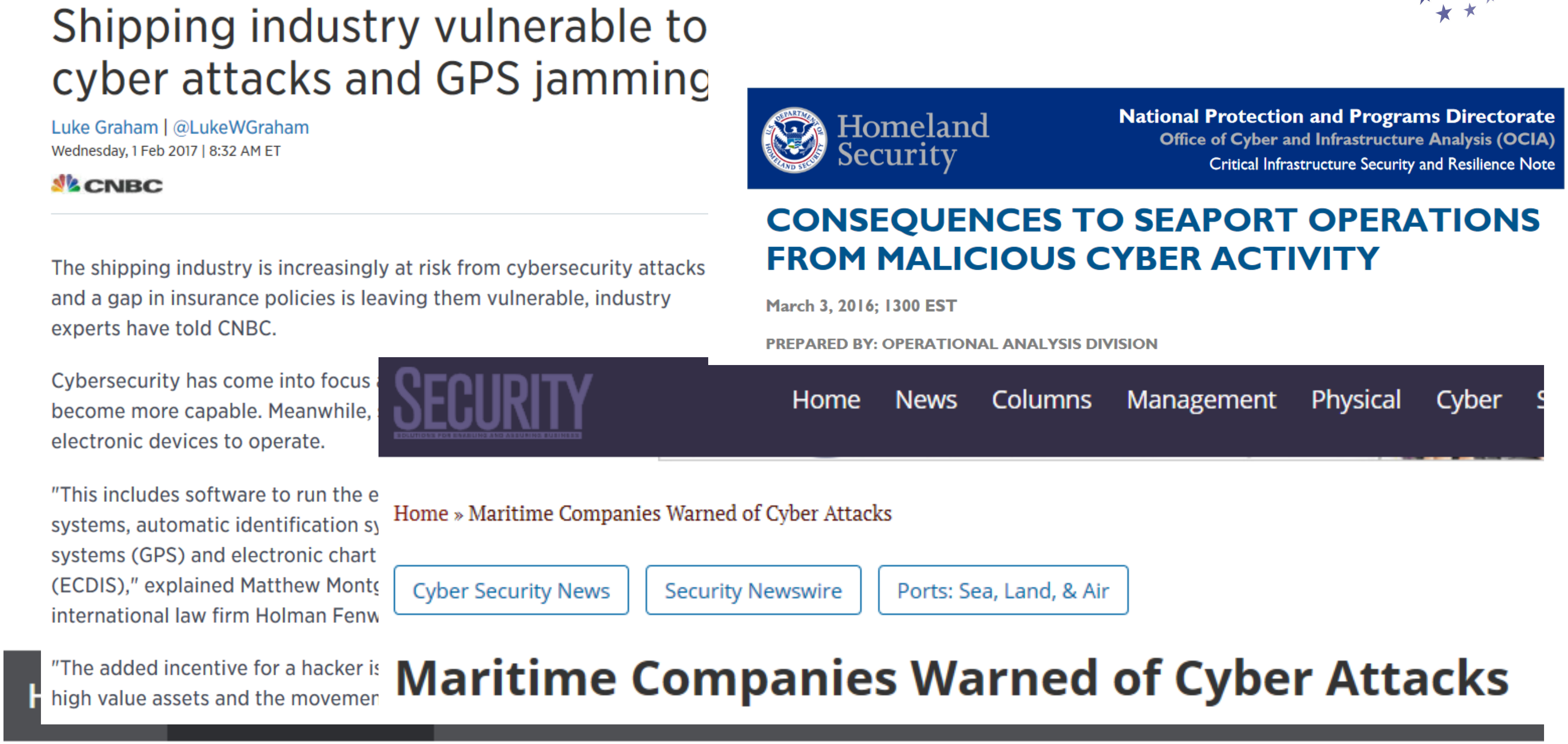
- Fundamental component of European and national Critical Infrastructures
- Passed through a significant transformation from proprietary, isolated systems to open architectures and standard technologies
- Advanced data collection and processing
- Statistics and remote control
- Convergence and interconnection with devices and services
- More functionalities



SAFETY4SEA conducted 'Share your Smart Shipping Insights' survey during Q4 2016 and assessed how maritime stakeholders have realized the current and future smart shipping challenges and have established the nature of ECDIS & e-Navigation, Cyber Safety/Cyber Security, Autonomous Shipping and Future Trends within shipping.

http://www.safety4sea.com/smart-shipping-survey-findings/

What could possibly go wrong?



Shipping industry vulnerable to cyber attacks and GPS jamming

Luke Graham | @LukeWGraham
Wednesday, 1 Feb 2017 | 8:32 AM ET
CNBC

The shipping industry is increasingly at risk from cybersecurity attacks and a gap in insurance policies is leaving them vulnerable, industry experts have told CNBC.

Cybersecurity has come into focus
become more capable. Meanwhile,
electronic devices to operate.

"This includes software to run the e
systems, automatic identification sy
systems (GPS) and electronic chart
(ECDIS)," explained Matthew Mont
international law firm Holman Fenw

"The added incentive for a hacker is
high value assets and the movemen

Homeland Security
National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Critical Infrastructure Security and Resilience Note

CONSEQUENCES TO SEAPORT OPERATIONS FROM MALICIOUS CYBER ACTIVITY

March 3, 2016; 1300 EST

PREPARED BY: OPERATIONAL ANALYSIS DIVISION

Home » Maritime Companies Warned of Cyber Attacks

Maritime Companies Warned of Cyber Attacks

Ships are already under cyber attack

Tue 18 Apr 2017 by Martyn Wingrove

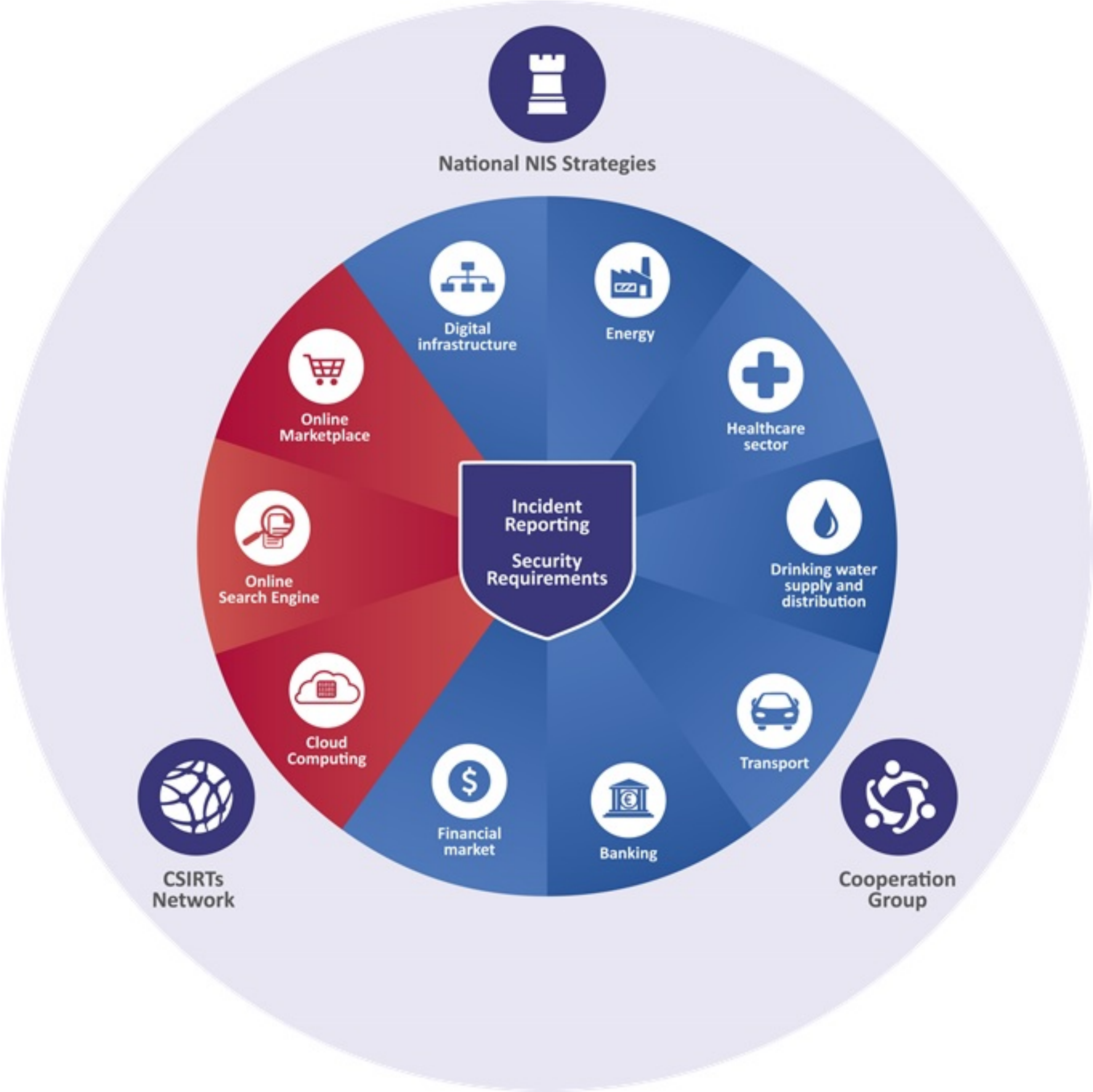
Cyber security aspects in the maritime sector

- Low awareness and focus on maritime cyber security
- Complexity of the maritime ICT environment including SCADA and emerging IoT usage
- Fragmented maritime governance context
- No holistic approach to maritime cyber risks
- Overall lack of direct economic incentives to implement good cyber security in maritime sector

Increasing attack surface

- Positioning systems
- Electronic Chart Display and Information System (ECDIS)
- Engine Control and monitoring systems
- Global Maritime Distress and Safety System (GMDSS)
- Automatic Identification System (AIS)
- Maritime ICS SCADA
  - Alarms and safety
  - Bridge Systems
  - Passenger Servicing & Mgt.
  - Passenger - facing Networks
  - Cargo Management System
  - Etc…

The Network and Information Security Directive



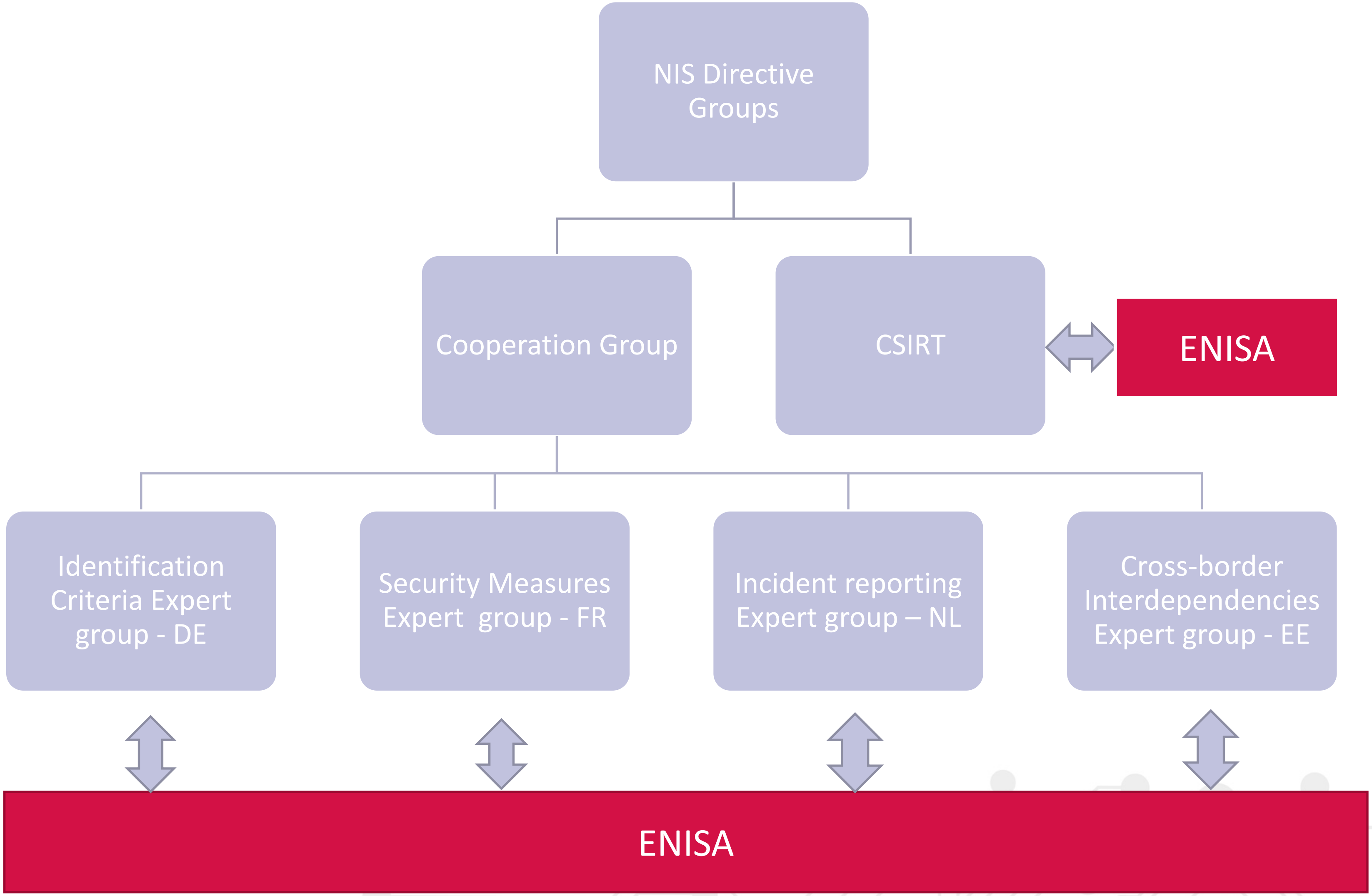
Operators of Essential Services in the context of the NIS Directive for water transport

- Inland, sea and coastal passenger and freight water transport companies (Annex I to Regulation (EC) No 725/2004)
- Managing bodies of ports (point (1) of Article 3 of Directive 2005/65/EC), including their port facilities (point (11) of Article 2 of Regulation (EC) No 725/2004), and entities operating works and equipment contained within ports.
- Operators of vessel traffic services (point (o) of Article 3 of Directive 2002/59/EC)

Obligations for MSs on OESs

- Identification of operators of essential services
- Minimum security measures to ensure a level of security appropriate to the risks
- Incident notification to prevent and minimize the impact of incidents on the IT systems that provide services
- Make sure authorities have the powers and means to assess security and check evidence of compliance for OES

Working groups under the NISD


NIS Directive Groups

Cooperation Group

CSIRT

ENISA

Identification Criteria Expert group - DE

Security Measures Expert group - FR

Incident reporting Expert group – NL

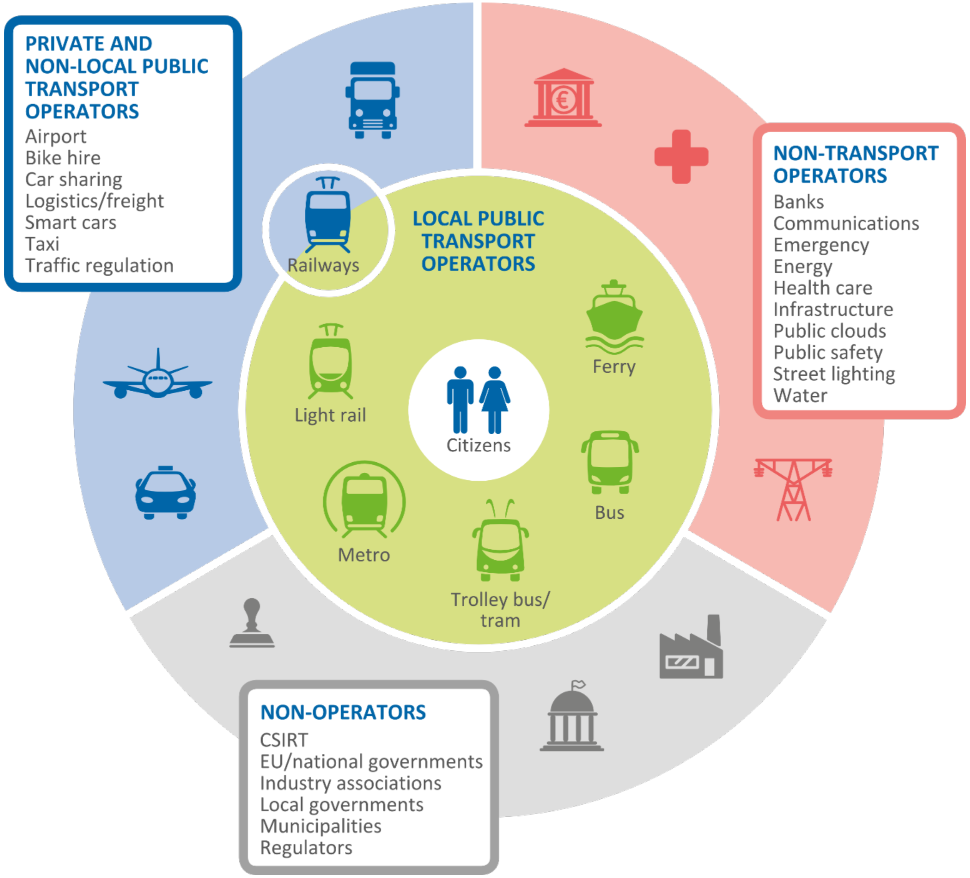
Cross-border Interdependencies Expert group - EE

ENISA

NIS directive - TIMELINE

August 2016	-	Entry into force
February 2017	6 months	Cooperation Group starts its tasks
August 2017	12 months	Adoption of implementing on security and notification requirements for DSPs
February 2018	18 months	Cooperation Group establishes work programme
9 May 2018	21 months	Transposition into national law
November 2018	27 months	Member States to identify operators of essential services
May 2019	33 months (i.e. 1 year after transposition)	Commission report - consistency of Member States' identification of OES
May 2021	57 months (i.e. 3 years after transposition)	Commission review

Securing transport in Europe



PRIVATE AND NON-LOCAL PUBLIC TRANSPORT OPERATORS
Airport
Bike hire
Car sharing
Logistics/freight
Smart cars
Taxi
Traffic regulation

LOCAL PUBLIC TRANSPORT OPERATORS

NON-TRANSPORT OPERATORS
Banks
Communications
Emergency
Energy
Health care
Infrastructure
Public clouds
Public safety
Street lighting
Water

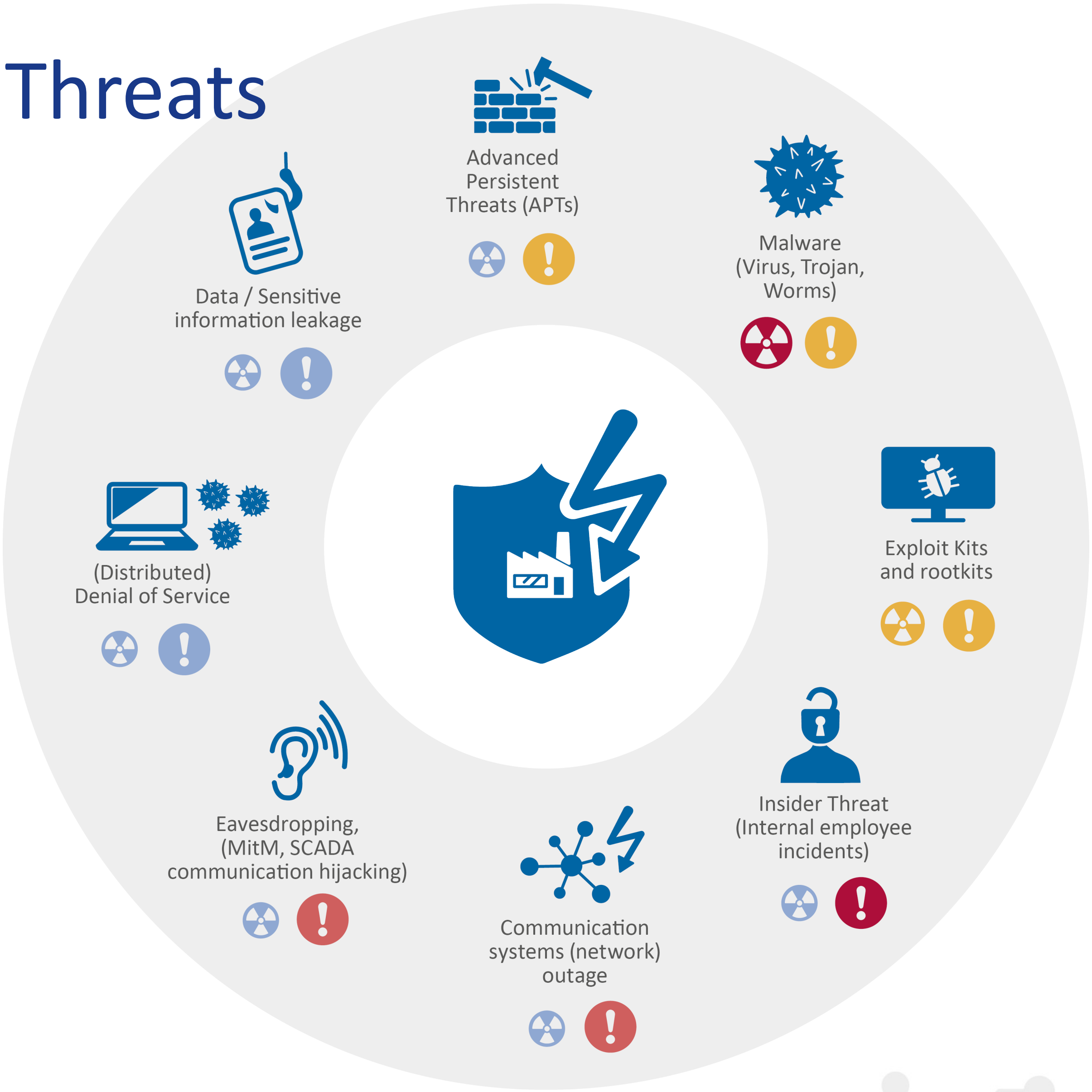
NON-OPERATORS
CSIRT
EU/national governments
Industry associations
Local governments
Municipalities
Regulators

ENISA efforts:

- Understand threats and assets
- Highlight security good practices in specific sectors
- Provide recommendations to enhance cyber security
- Engage with communities

https://www.enisa.europa.eu/smartinfra

SCADA Threats



Advanced Persistent Threats (APTs)

Malware (Virus, Trojan, Worms)

Exploit Kits and rootkits

Insider Threat (Internal employee incidents)

Communication systems (network) outage

Eavesdropping, (MitM, SCADA communication hijacking)

(Distributed) Denial of Service

Data / Sensitive information leakage

Likelihood: ☢ Low ☢ Medium ☢ Very high

Impact: ❗ Medium /High ❗ High ❗ High/Crucial ❗ Crucial

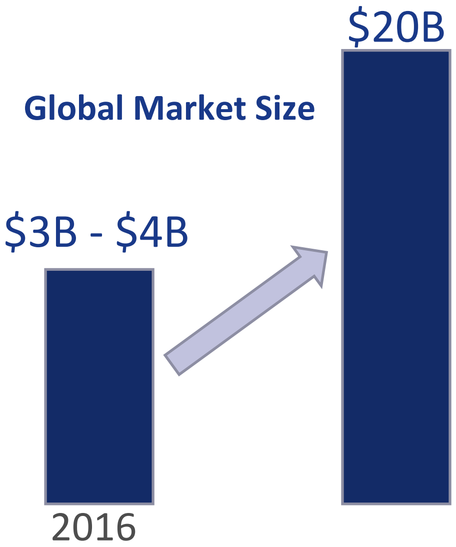
What you can do from today:

- Consider the cybersecurity impact on safety
- Include cyber security in your governance model in order to define liabilities
- Ensure you consider cyber security in all stages of the life cycle of products and services
- Consider network connectivity and interdependencies and cascading effects
- Start reusing existing good practices from other sectors, for example for SCADA

ENISA work on Cyber Insurance

The Global Cyber Insurance Market

- ⇧ Currently a small % of overall cybersecurity spending but **rapidly growing**
- ⇧ **High growth potential** as organisations become more aware of their cyber exposure
- ⇧ Regulation has historically been one of the biggest drivers for market adoption of cyber insurance
- ⇧ Growth is fuelled by the fact that cyber is now acknowledged as a **top global risk**
- ⇩ Market growth is hampered by **lack of data**, particularly for aggregated loss scenarios
- ⇩ **Lack of standardisation in policies** and limited understanding of options are an obstacle from the customer's perspective
- ⇩ Constantly **evolving cyber threat landscape** increases complexity of cyber insurance offerings



Source: Allianz

US Cyber Insurance Market Growth 2016

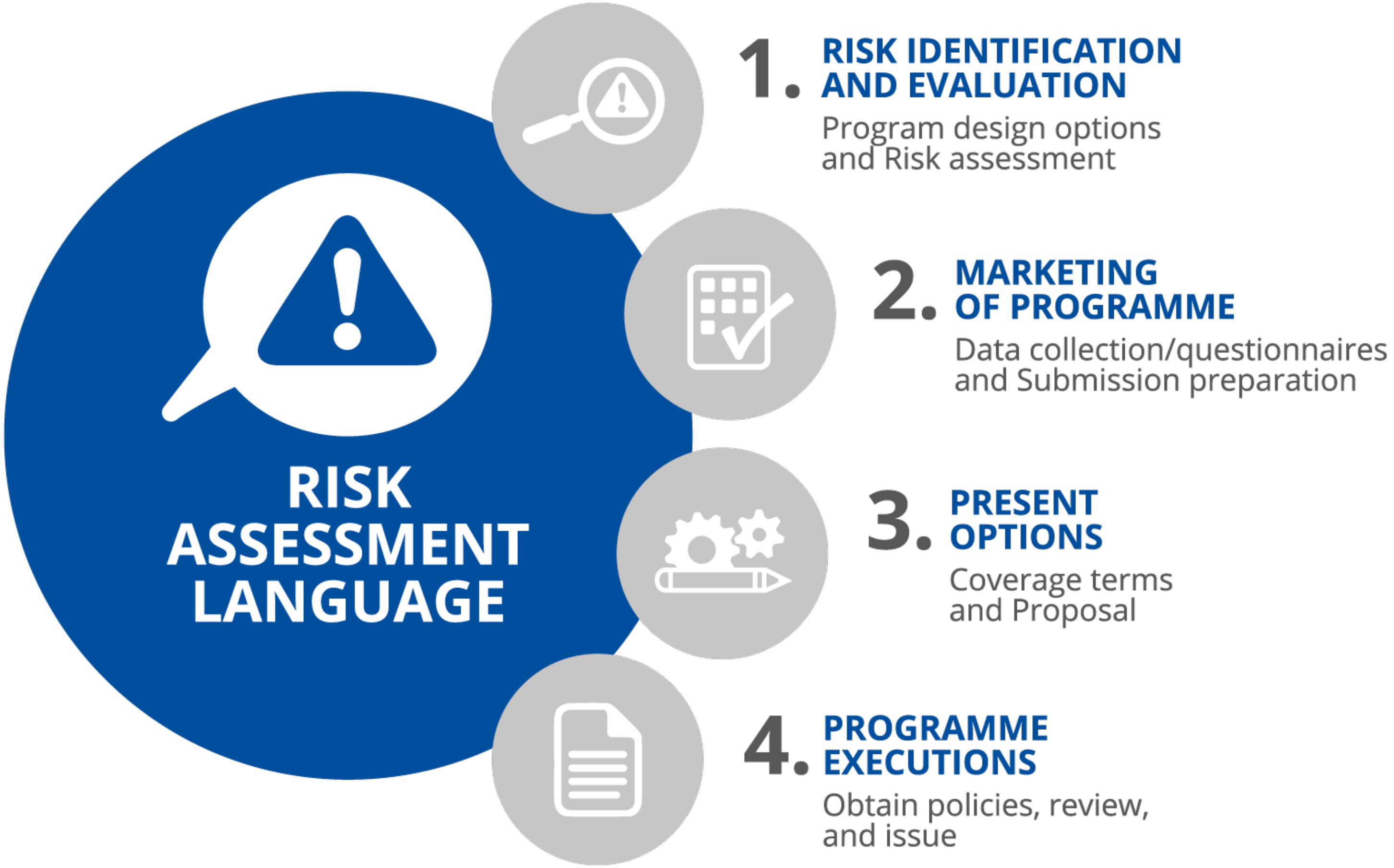
35%

Source: Fitch

ENISA Work on Cyber Insurance

- Incentives and barriers of the cyber insurance market in Europe (2012)
  - *analysis of the structure and the characteristics of the cyber insurance market*
- Cyber Insurance: Recent Advances, Good Practices and Challenges (2016)
  - *good practices and challenges during the early stages of the cyber insurance lifecycle*
- Commonality of risk assessment language in cyber insurance (on-going)
  - *incentives and barriers towards harmonization/standardisation of risk assessment language in cyber insurance*

Risk Assessment Language in the Cyber Insurance application process



RISK ASSESSMENT LANGUAGE

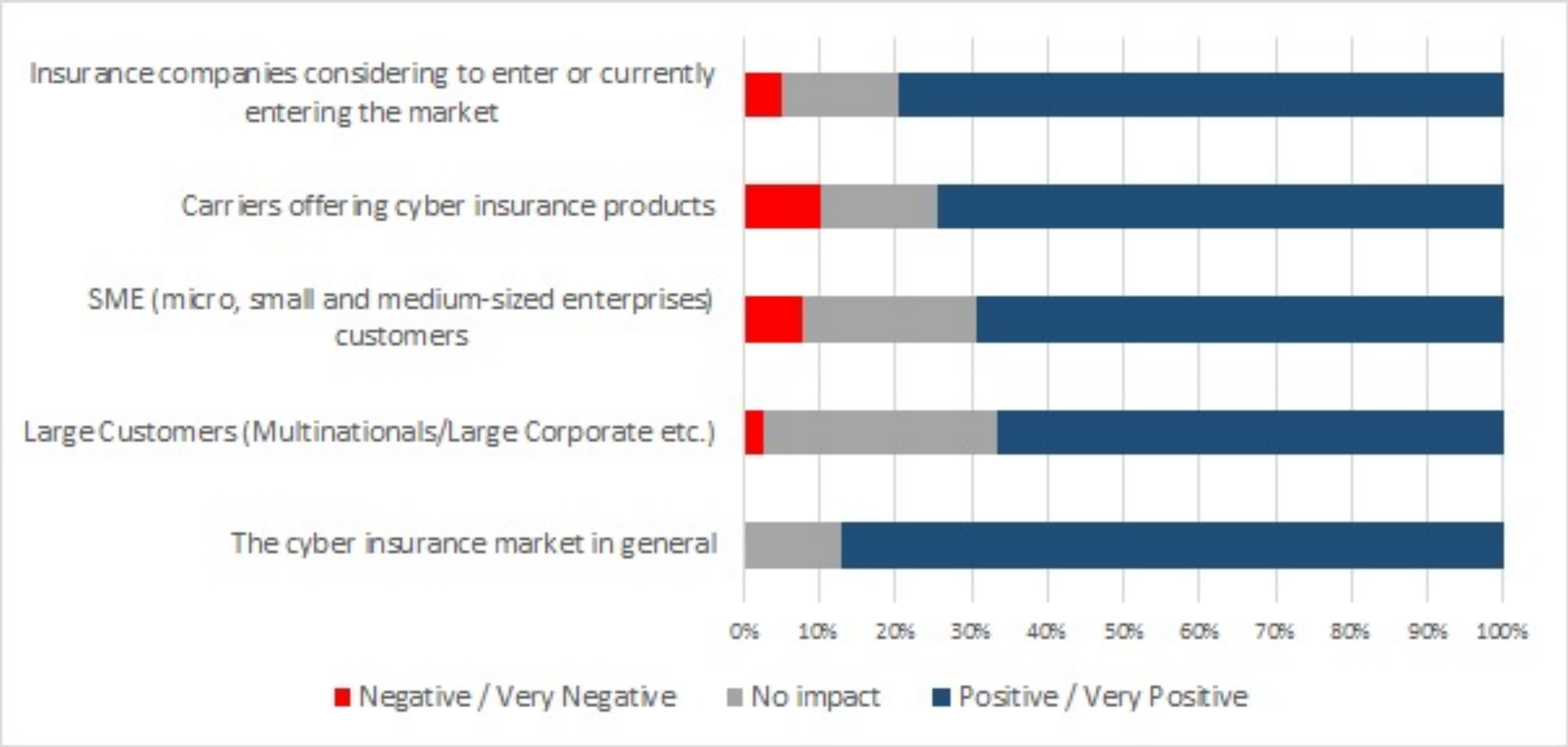
1. **RISK IDENTIFICATION AND EVALUATION**
   Program design options and Risk assessment

2. **MARKETING OF PROGRAMME**
   Data collection/questionnaires and Submission preparation

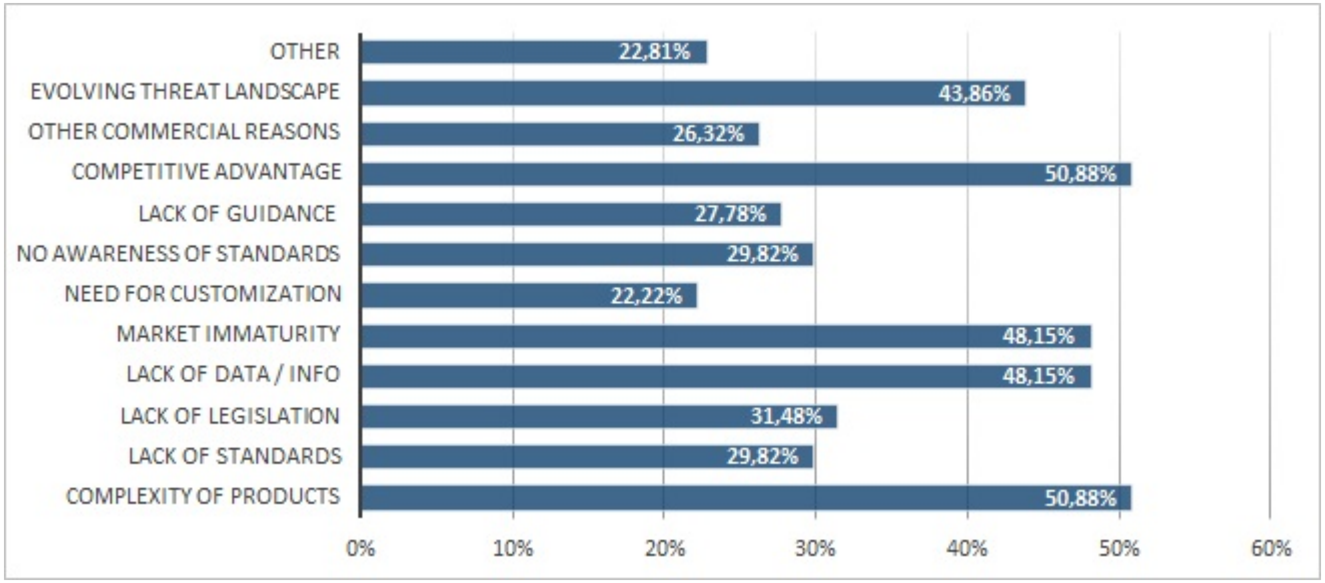
3. **PRESENT OPTIONS**
   Coverage terms and Proposal

4. **PROGRAMME EXECUTIONS**
   Obtain policies, review, and issue

The impact of risk assessment language harmonisation



Barriers against harmonisation



Some key points

- **Competitive advantage –** harmonisation perceived as loss of unique selling points
- **Lack of data –** very difficult to understand threats and reluctance to share data
- **Complexity –** multiple parameters increase the difficulty of risk assessment model convergence
- **Market immaturity** - carriers compete by trying to develop the best possible product with little experience
- **Evolving threat landscape** - language convergence is slower to catch-up, and maintain, to the highly dynamic cyber risk environment

Market drivers towards harmonisation

Regulations and Standards

- **Common requirements** for security controls and incident reporting
- **Convergence** in terms of security practices and residual risks
- Increased adoption of **specific security standards**
- **Consistent** definitions and taxonomies

Data Availability

- **Improved risk assessment models** and understanding of risk
- **Expansion of data source** to include other feeds
- Development of **cybersecurity skillset** in the industry
- **Efficient and automated** underwriting process

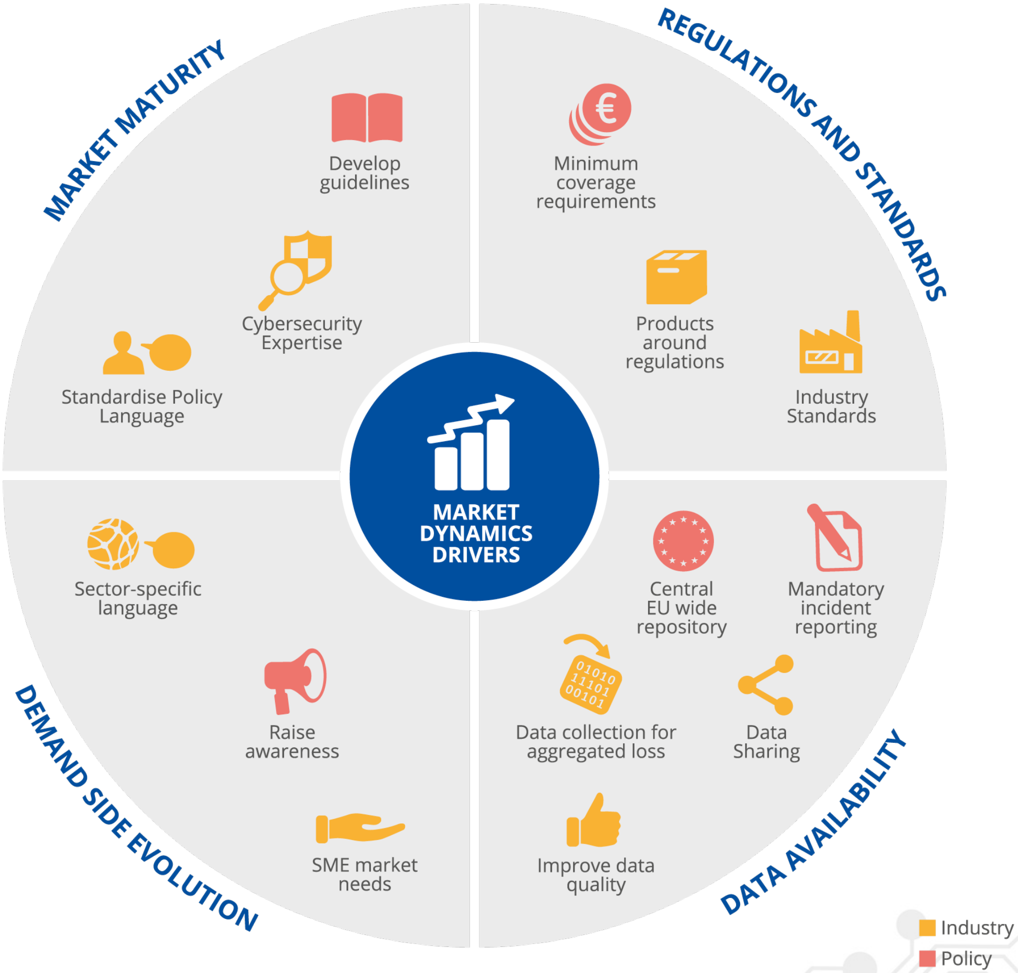
Demand Side Evolution

- **Address SME market** with standardized products
- **Maturing demand side** favours comparable products
- **Compliance** with emerging regulations
- Increased customer **cyber risk awareness**

Market Maturity

- Market **convergence** and **information sharing**
- Improved **information gathering** and **benchmarking**
- Consensus on a **minimum of standards**
- Mechanics of **competition** - best practices

Supporting harmonisation and growth of the cyber insurance industry



Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu