Office of the Commissioner of Electronic Communications & Postal Regulation

Cybersecurity Strategy of the Republic of Cyprus

George Michaelides
Commissioner of Electronic Communications & Postal Regulation
http://www.ocecpr.org.cy

2nd February 2017

Overview

- Cybersecurity facts
- Cybersecurity Strategy
  a. European strategy
  b. NIS Directive
- OCECPR responsibilities
  - Net Neutrality regulation
- National Cybersecurity Strategy
  - Building blocks
  - Progress made
  - Fields of further Cooperation
- Important messages

Cybersecurity Facts

New malware	
Samples of new malware found in Q3 2016	18 million
(source Panda Security Labs 2016)	

Internet of Things

By 2020, more than **25%** of identified enterprise attacks will involve IoT, though IoT will account for only **10%** of IT security budgets.

(source Gartner 2016)

Global economic cost of over $445B
(Source Mcafee)

10% probability of a major CII breakdown in the next 10 years
(Source WEF)

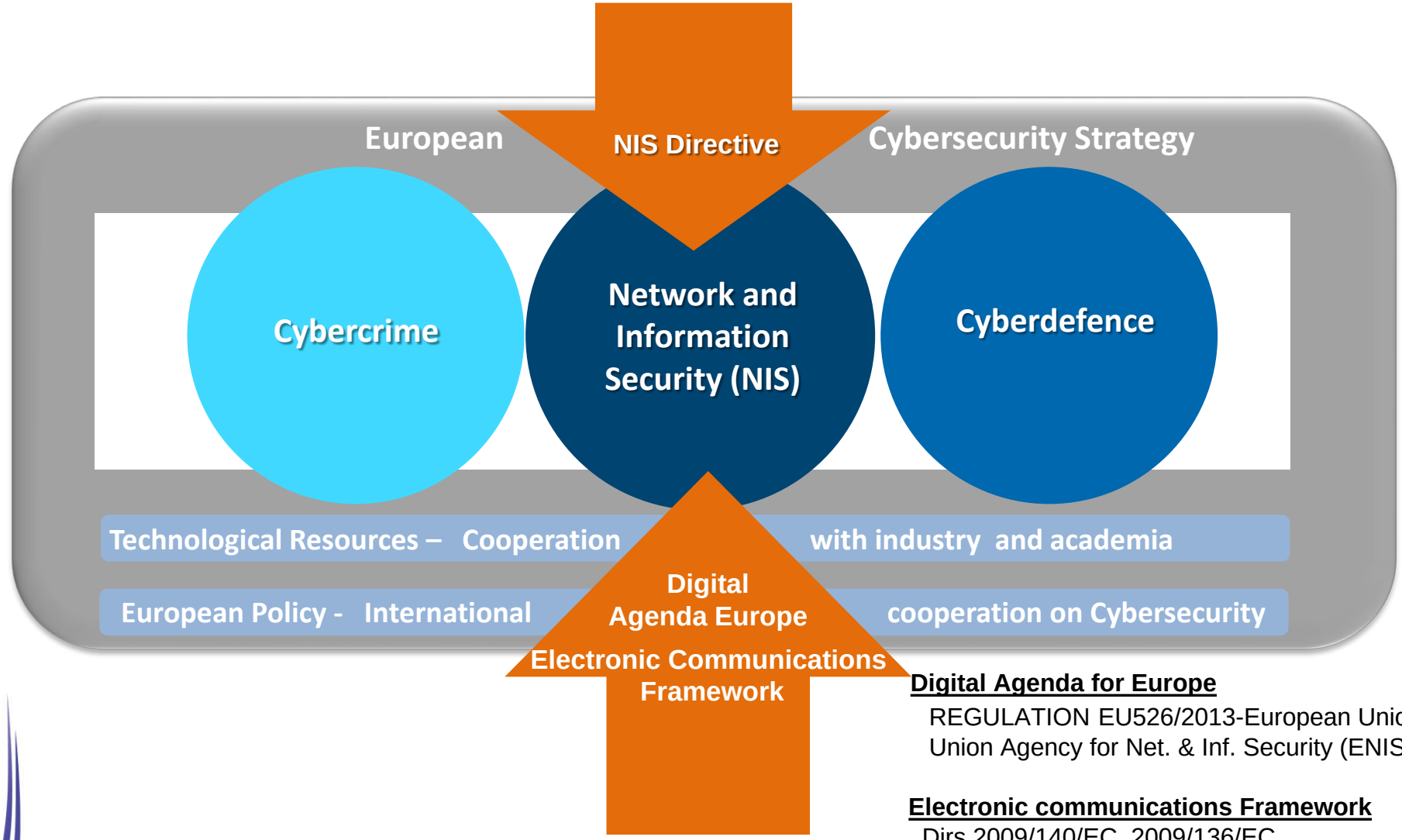
Size of Data Breach	Average total cost of breach
< 10.000	$2.1 million
10.000 – 25.000	$3.0 million
25.000 – 50.000	$5.0 million
> 50.000	$6.7 million
(source Ponemon Institute 2016)	

Known Vulnerabilities!

Through 2020, **99%** of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year...

(source Gartner 2016)

European Cybersecurity Strategy



Digital Agenda for Europe

REGULATION EU526/2013-European Union Union Agency for Net. & Inf. Security (ENISA)

Electronic communications Framework

Dirs 2009/140/EC, 2009/136/EC,
Framework 21/2002, Art.13a,b
Pers. Data Prot. 58/2002/EC Art.4
REGULATION EU 611/2013 Notification of personal data breaches

NIS Directive

Scope

The NIS Directive applies to operators of "essential services" in "critical sectors" :

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Drinking water supply and distribution

as well as to "digital service providers":

- Digital infrastructure
- Online marketplace
- Online search engine
- Cloud computing service

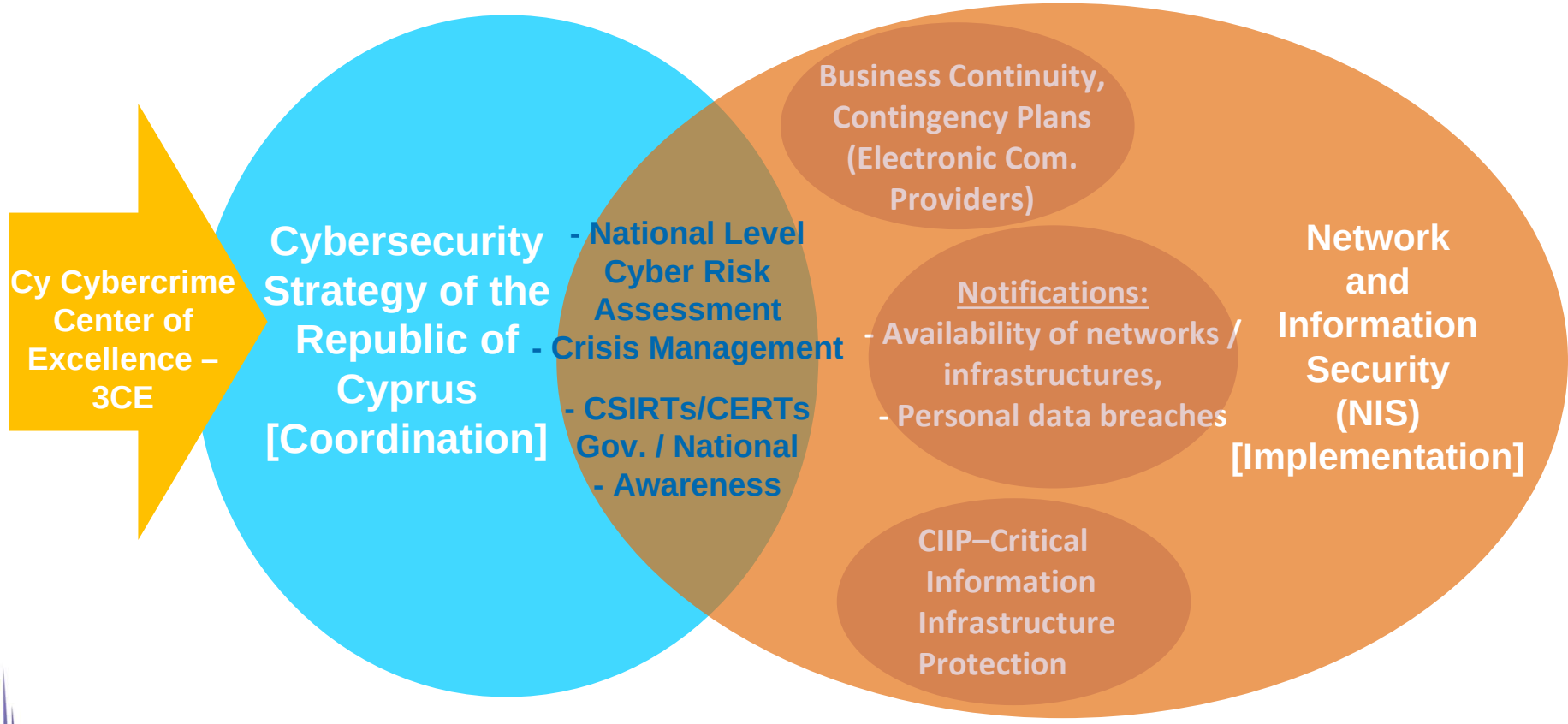
NIS Directive

Subject matter

The NIS Directive aims to ensure a uniform level of cybersecurity across the EU. Within the scope of the directive, MS, ENISA and the Commission should ensure:

- NIS Strategy and Cooperation plan in all MS
- Identification of operators of essential services at national level
- National Computer Security Incident Response Team (CSIRT) in all MS
- Establishment of a CSIRTs network at EU level
- Establishment of a cooperation group at EU level
- Security requirements and Incident Notifications mechanism
- Encourage Standardization

OCECPR Responsibilities



EU, ITU, ICANN vs OCECPR responsibilities

EC Vision: Delivering the Digital Single Market (DSM)

Better online access for consumers and businesses across Europe

DSM

Maximising the growth potential of our European digital economy

Creating right conditions for digital networks to flourish

European Parliament

EU Council

Legislation / Regulation

CY: Information Society

[OCECPR Responsibilities]

Supply

Demand

Networks

- Trends
- Available income
- Consumer protection
- Consumer awareness [Tel2Me, Net2Map]
- Market developmet +Consumer benefits]

Services [& bundles]

Legislation / Regulation

Network neutrality [2B2T – Mlab]
NIS Directive

EU: ENISA, FoP Cyber, HLIG

World: ITU, ICANN

Open Internet

EU Cybersecurity Strategy [NIS, Cybercrime]

EU position on Internet Governance [GAC-ICANN, IANA]

Open Internet

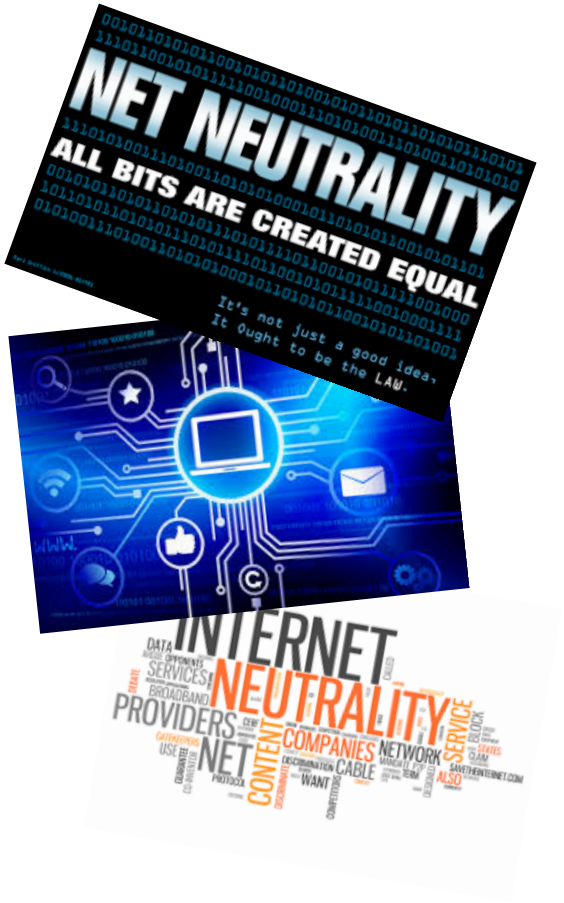
CY Cybersecurity Strategy [NIS, CERT, Risk Assessment, Awareness, Interdependencies]

CY position on Internet Governance [GAC-ICANN, IANA], .cy, .κπ

Net Neutrality - Regulation (EU) 2015/2120

Subject matter and Scope

- Adoption of measures on ensuring access to the open Internet
- Establishment of common rules to ensure:
  - equitable and non-discriminatory traffic management, in the provision of internet access services,
  - the rights of end users
- Users have the right to access and to distribute information and content, to use and to provide applications and services and use terminal equipment of their choice



Vision of the Cybersecurity Strategy of the Cyprus Government

Electricity

Natural Gas/oil

Water supply

Transports

“The protection of all critical information infrastructures of the state and the operation of information and communication technologies with the necessary levels of security, for the benefit of every citizen, the economy and the country”

Public Health

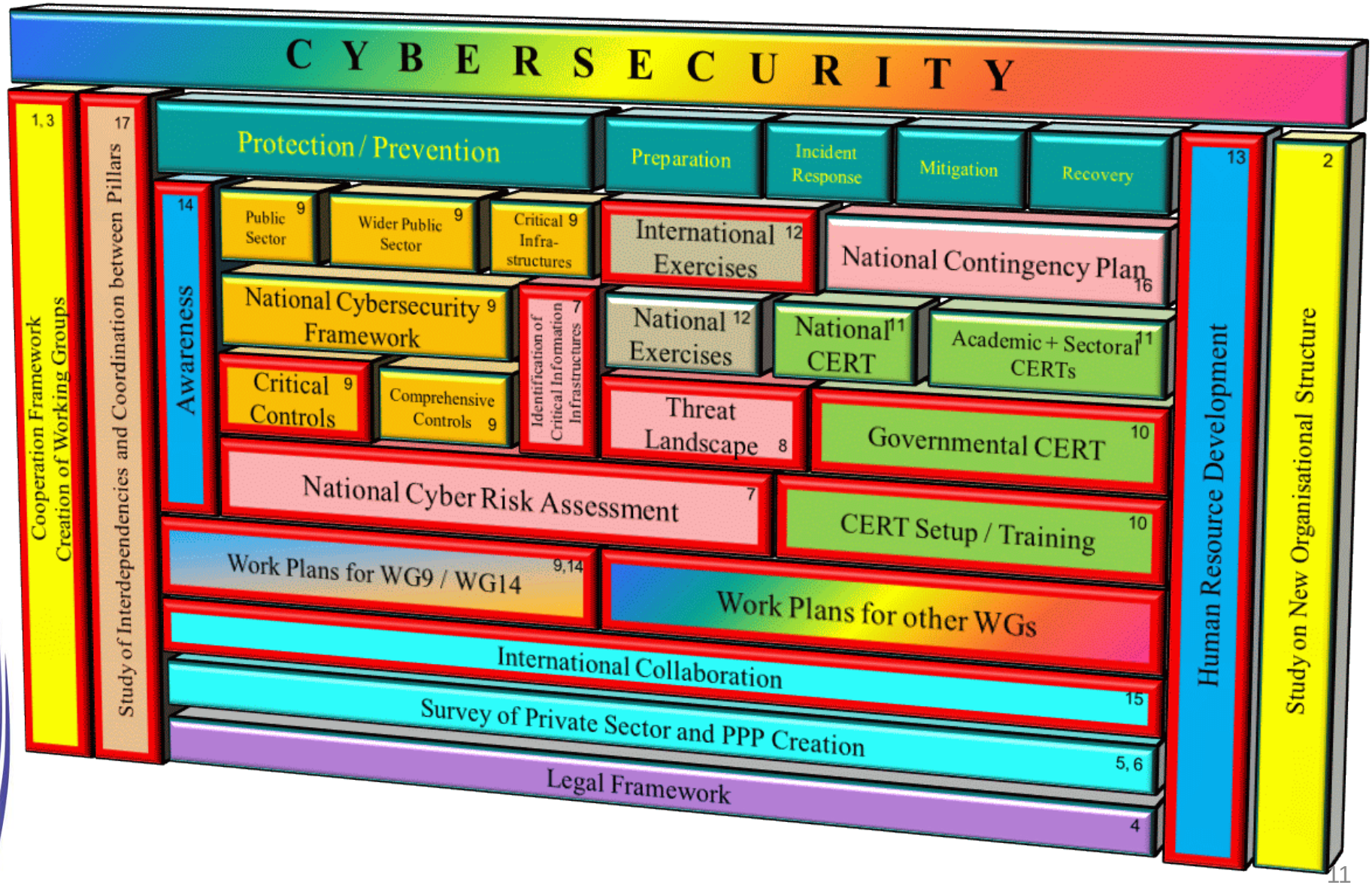
Financial sector

Public sector/security services

Electronic communications

Education – Training – Awareness – Cooperation – Trust

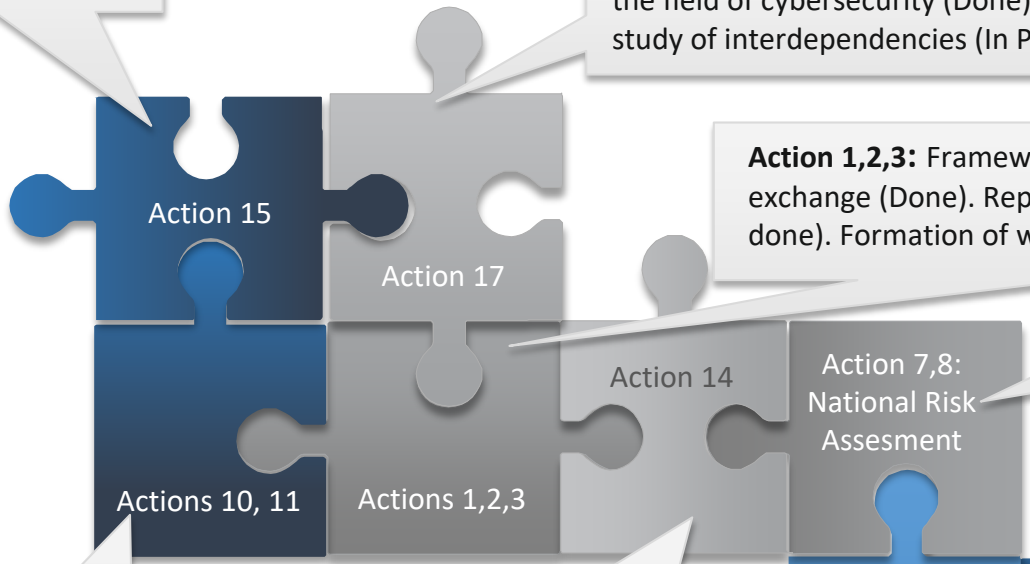
Cyprus Cybersecurity Strategy Building blocks



Progress made - Active Groups

Action 15: International cooperation activities

Action 17: Guidance and coordination on operations in the field of cybersecurity (Done). Identification and study of interdependencies (In Progress).



Action 1,2,3: Framework for collaboration and information exchange (Done). Report on policies and structures (To be done). Formation of working groups (In Progress)

Action 7,8: National Level Cyber Risk Assesment (In Progress)

Actions 7, 16: Identification and assessment of the Critical Information Infrastr. (In Progress) (Development of National Conting. Plan. (In Progress)

Action 10: Establisment of Government CERT/CSIRT (done).

Accredidation of Cyprus gov CERT/CSIRT (In Progress).

Action 11: Study for the Establisment of a National CERT/CSIRT (In Progress).

Action 14: Development of a comprehensive National Awareness Programme for Cybersecurity (In Progress).

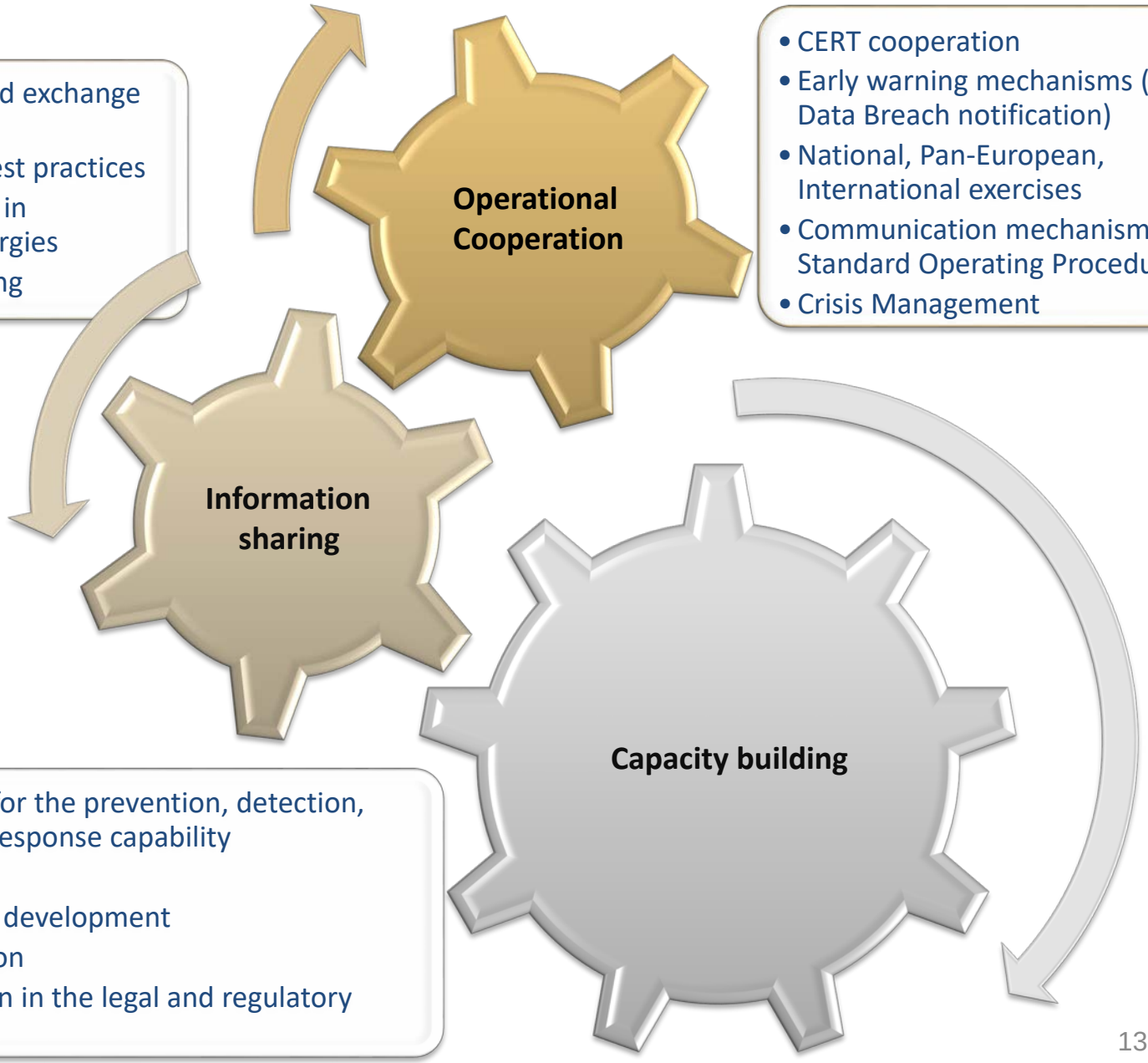
Establisment of the Awareness subgroup for students/ teachers/ Kids/parens (Done).

3CE (Cyprus Cyber Center of Excellence)

Action 9: Development of a National Cybersecurity Framework for the critical information infrastructures in Cyprus, as well as the government sector (In Progress).

Initialised with the development of Critical controls (Done).

Fields of further Cooperation



- Development and exchange of Know-how
- Exchanging of best practices
- Providing advice in Developing Synergies
- Awareness Raising

- CERT cooperation
- Early warning mechanisms (e.g Data Breach notification)
- National, Pan-European, International exercises
- Communication mechanisms – Standard Operating Procedures
- Crisis Management

- Cooperation for the prevention, detection, analysis and response capability
- Training
- Research and development
- Standardization
- Harmonization in the legal and regulatory framework

Important messages

6 Awareness raising at the highest level,

5 Trust between stakeholders - the key to the successful implementation of the Strategy,

4 Multi-stakeholder approach to the implementation of the Strategy,

3 Cooperation and collaboration between public and private sector is essential,

2 Cooperation - Absolutely necessary, at National, European and International level,

1 Cybersecurity - A complex task - Great responsibility to the relevant bodies,

Thank you!