Office of the Commissioner of Electronic Communications & Postal Regulation

OCECPR

Cybersecurity Strategy of the Republic of Cyprus

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

ITU Regional Development Forum Europe
Vilnius, Lithuania - 26 April 2017

Overview

- Cybersecurity facts
- Cybersecurity Strategy
  a. European strategy
  b. NIS Directive
  c. CY CSIRT
- National Cybersecurity Strategy
  a. Building blocks
  b. Progress made
  c. 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)

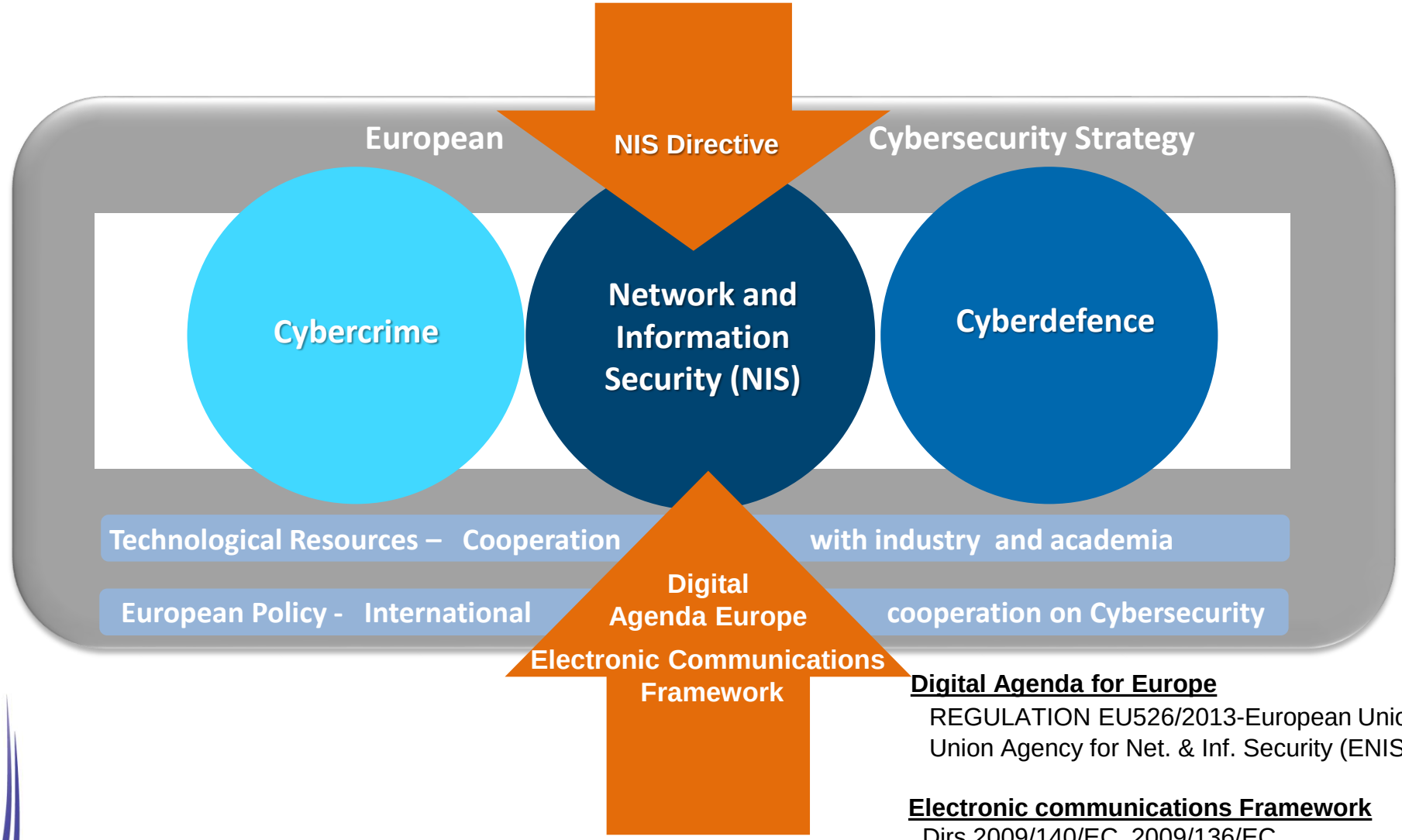
Size of Data Breach	Average total cost of breach
< 10.000	$2.1 million
10.000 – 25.000	$3.0 million
25.000 – 50.000	$5.0 million
> 50.000	$6.7 million
(source Ponemon Institute 2016)	

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

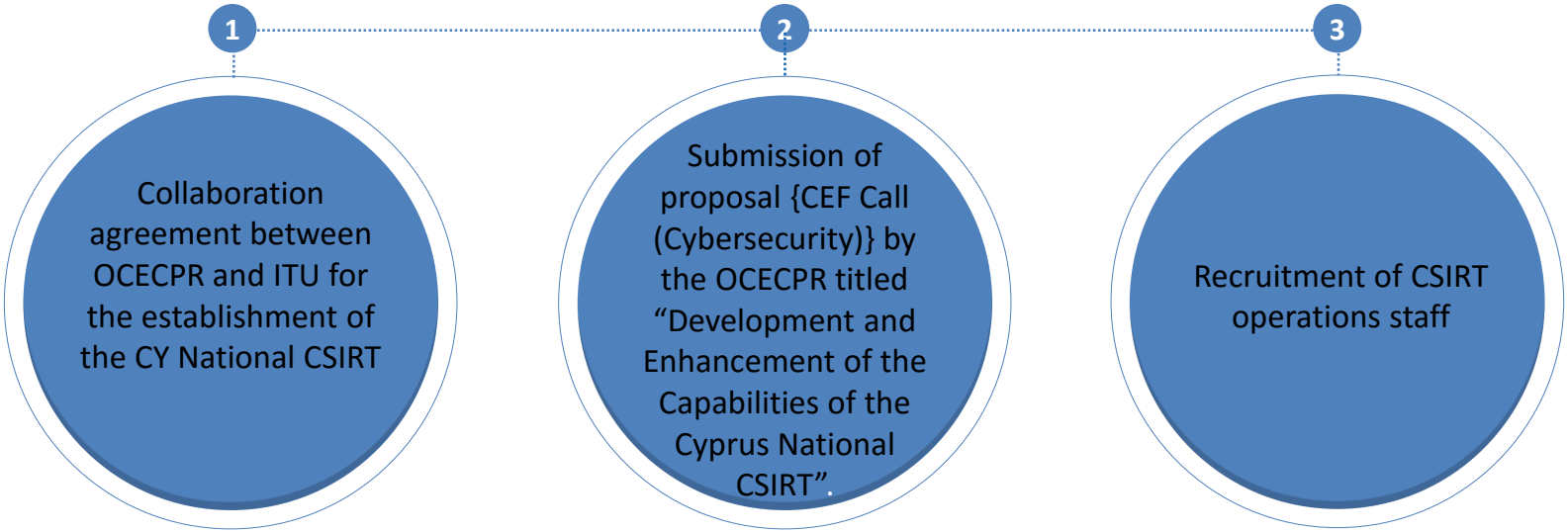
NIS Directive

Subject matter

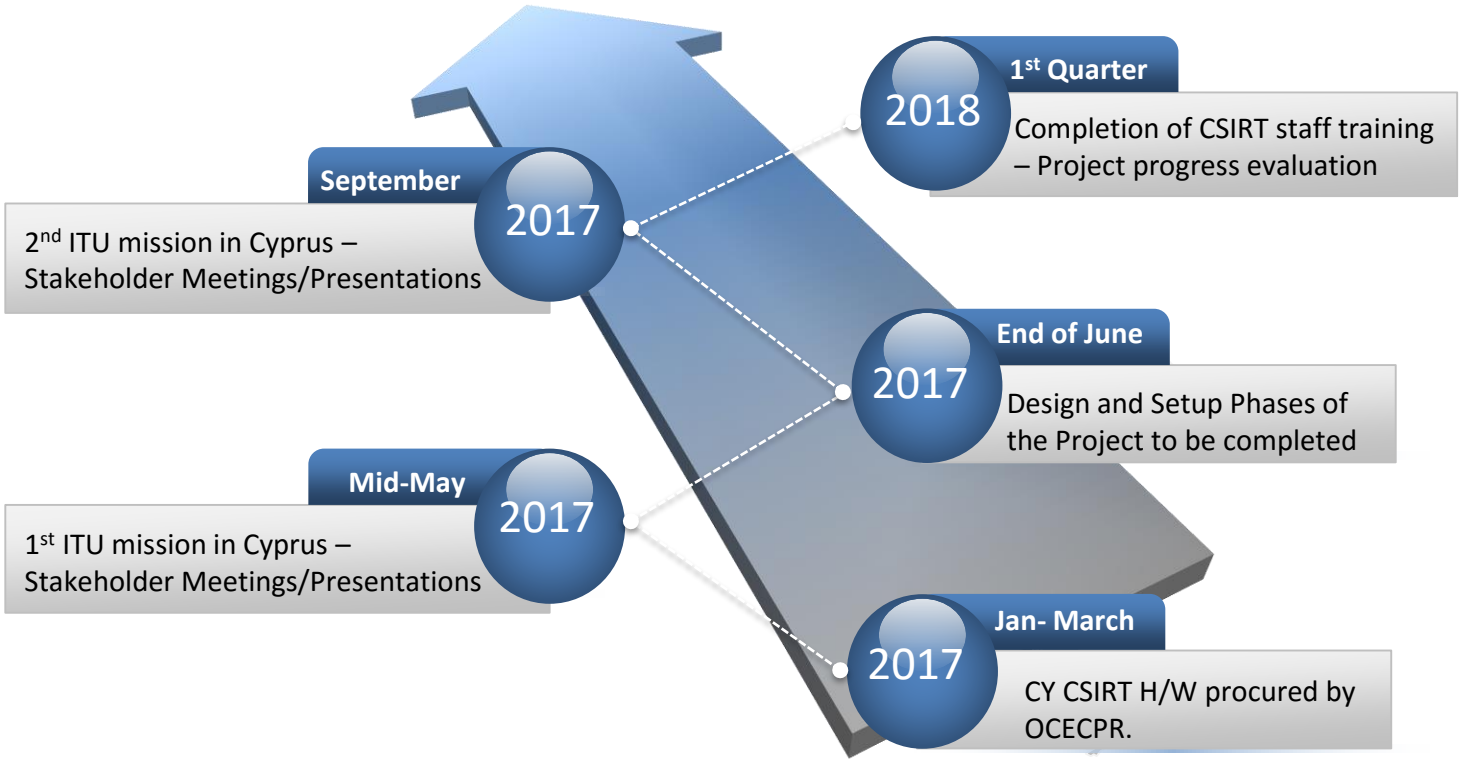
The NIS Directive aims to ensure a uniform level of cybersecurity across the EU. Within the scope of the directive, MS, ENISA and the Commission should ensure:

- 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

CY CSIRT- Pillars of Action



CY CSIRT – ITU Project Work



For more information visit:

www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=9CYP17002

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

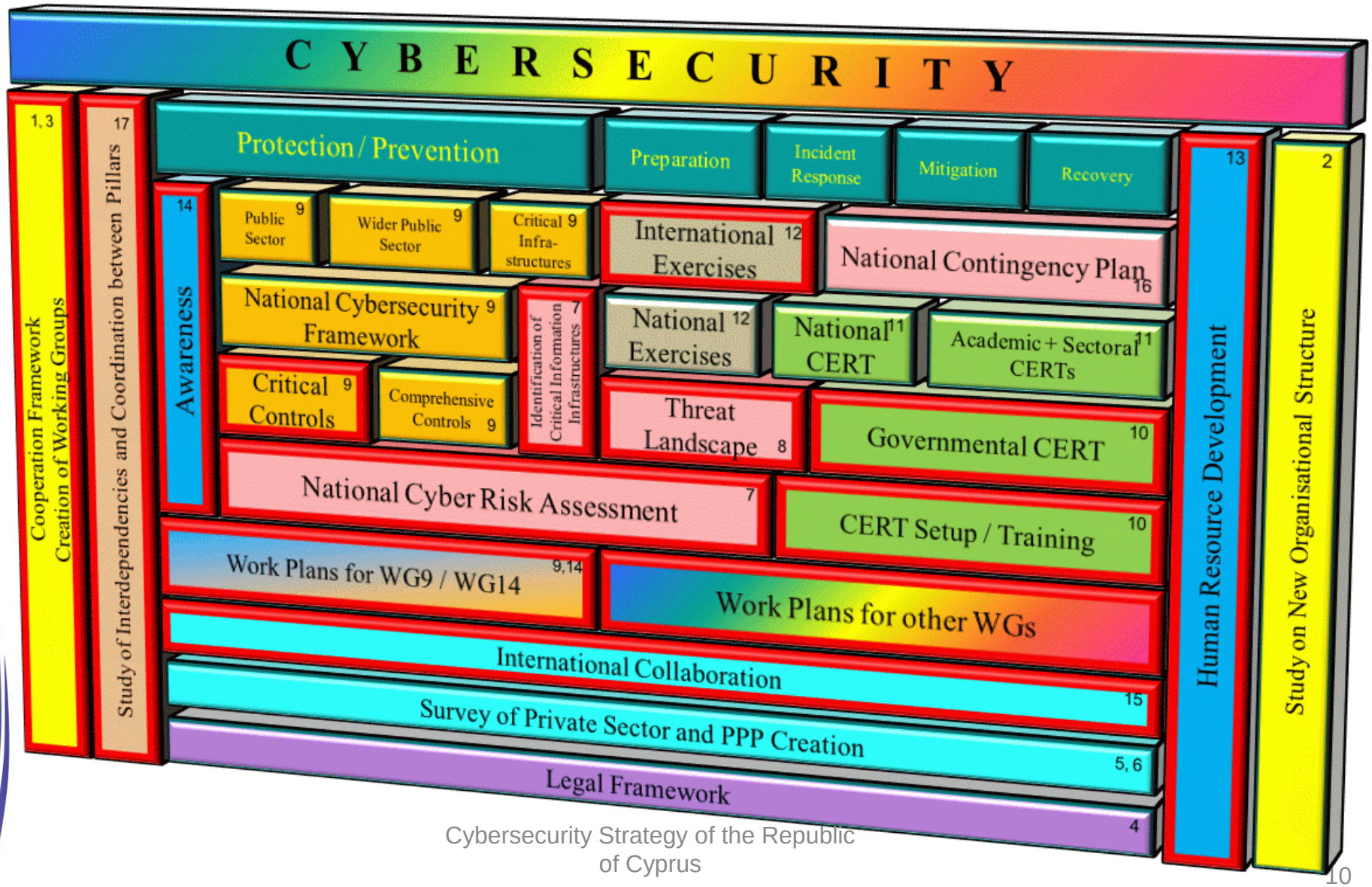
Financial sector

Public sector/security services

Electronic communications

Education – Training – Awareness – Cooperation – Trust

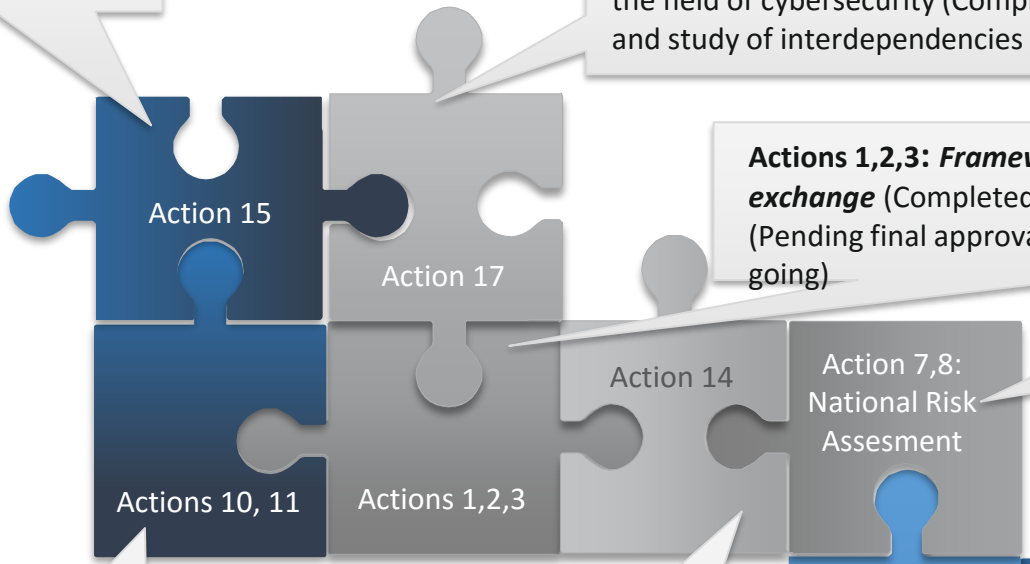
Cyprus Cybersecurity Strategy Building blocks



Progress made - Active Groups

Action 15: International cooperation activities

Action 17: Guidance and coordination on operations in the field of cybersecurity (Completed). Identification and study of interdependencies (Ongoing).



Actions 1,2,3: ***Framework for collaboration and information exchange*** (Completed). Report on policies and structures (Pending final approval). Formation of working groups (On going)

Actions 7,8: ***National Level Cyber Risk Assesment*** (Completed)

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

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

Accredidation of Cyprus ***Gov CERT/CSIRT*** (In Progress).

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

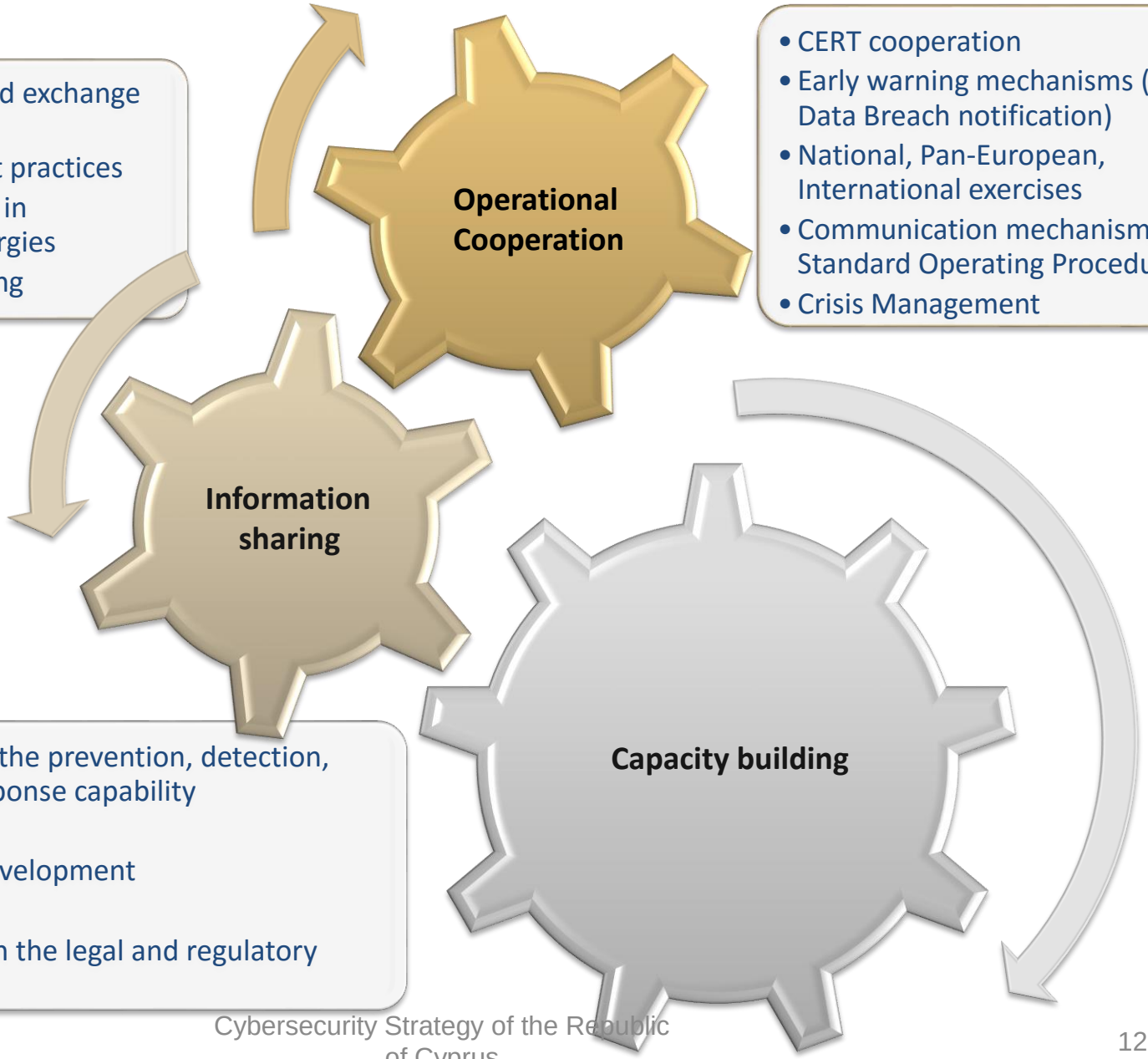
Action 14: Development of a comprehensive ***National Awareness Programme*** for Cybersecurity (In Progress).

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

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 (Completed).

Fields of further Cooperation



- Development and exchange of Know-how
- Exchange 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

National Awareness Programme

Safe Internet for children

National Cybersecurity Strategy

National Awareness Programme – Action14

On going activities in Education

- ICT
-Media and Information literacy
-Safe internet
- Safer Internet Programme by the Connecting Europe Facility (CEF)
- CyberEthics funded by the European Commission Innovation and Networks Executive Agency (INEA)

National targeted strategic planning for Safe Internet for children, teachers, parents:

- Stakeholders Workgroup
- Cybersecurity training center

Safe Internet for children

National targeted strategic planning: Stakeholders Workgroup

Goals

- Develop a Safe internet national strategy for students, teachers and parents for 2015-2020
- Provide suggestions and proceed with implementation of actions
- Promote through recommendations, processes and infrastructure for the sustainability of the work

Work in Progress

- Description of current status
- Recording of new needs
- Suggestions for new actions
- Search for funding resources
- Action plan
- Time frame: 1 December 2016

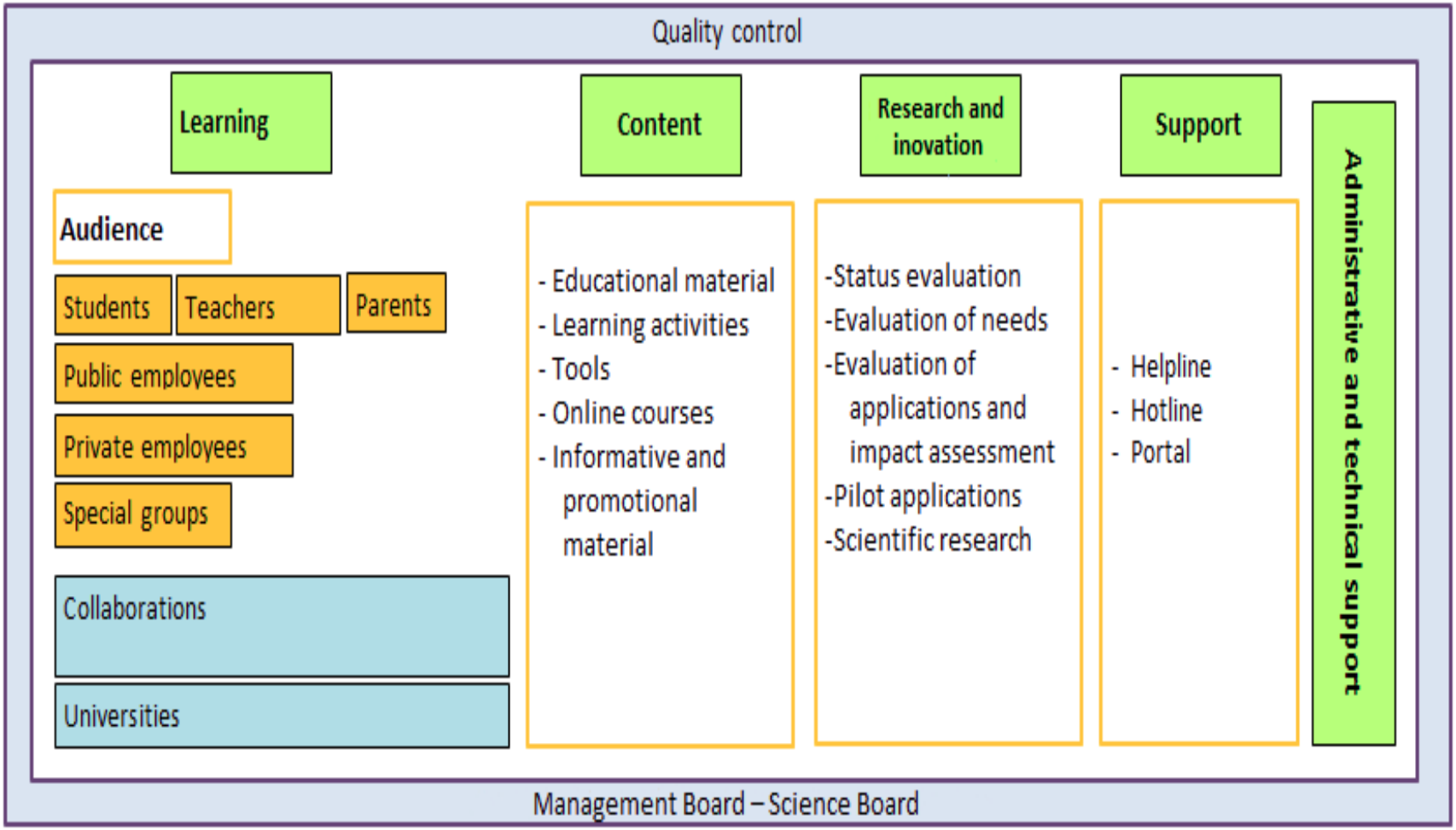
Safe Internet for children

Stakeholders Workgroup

A good representation of stakeholders through an open invitation by the OCECPR

Safe Internet for children

National targeted strategic planning: Cybersecurity training center

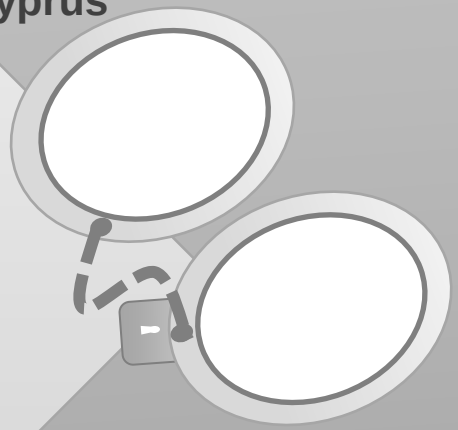


Cyprus Cybercrime Center of Excellence -3CE for Training, Research and Education

Establishment of Cyprus Cybercrime Centre of Excellence (3CE)

- 3CE provided short-term, highly focused and specialised training seminars on cybercrime-related issues for public and private sector participants.
- 3CE aspires to become an exemplary Centre of Excellence in the area of Cybercrime by conducting research in relevant fields.

Main platform for collaboration, coordination and exchange of knowledge regarding Cybercrime in Cyprus



Combines expertise of:

- Academic research groups
- Public sector organizations
- Law Enforcement Agencies (LEAs)
- Judicial Personnel
- Civil servants and
- Private sector stakeholders

Collaboration with:

- Other National Cybercrime Centers EC3 and
- Europol

Co-funded by the Prevention of and Fight against Crime Programme of the European Union

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 for the relevant bodies,

Thank you!

george.michaelides@ocecpr.org.cy