Office of the Commissioner of Electronic Communications & Postal Regulation

OCECPR

EU - Network and Information Security (NIS) Directive

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

22nd November 2016

Overview

- Cybersecurity Facts
- European Cybersecurity Strategy
- The Objectives
- MS Capability Requirements
- NIS Scope
- NIS Requirements
- National CSIRT
  - o Coverage
  - o Activities
  - o Incident Management
- Way Forward / Timeline

Cybersecurity Facts

Percentage cost for external consequences	
Information loss	39%
Business disruption	35%
Revenue loss	21%
Equipment damages	4%
Other	2%
(source Ponemon Institute 2015)	

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

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)	

Vulnerabilities	• 2015 • 2014
Scanned Websites with Vulnerabilities	78% 76%
Percentage of Which Were Critical	15% 20%
Browser Vulnerabilities	879 639
Web Attacks Blocked per Day	~1 million 496,657
Websites Found with Malware	1 in 3,172 1 in 1,126
(source Symantec 2016)	

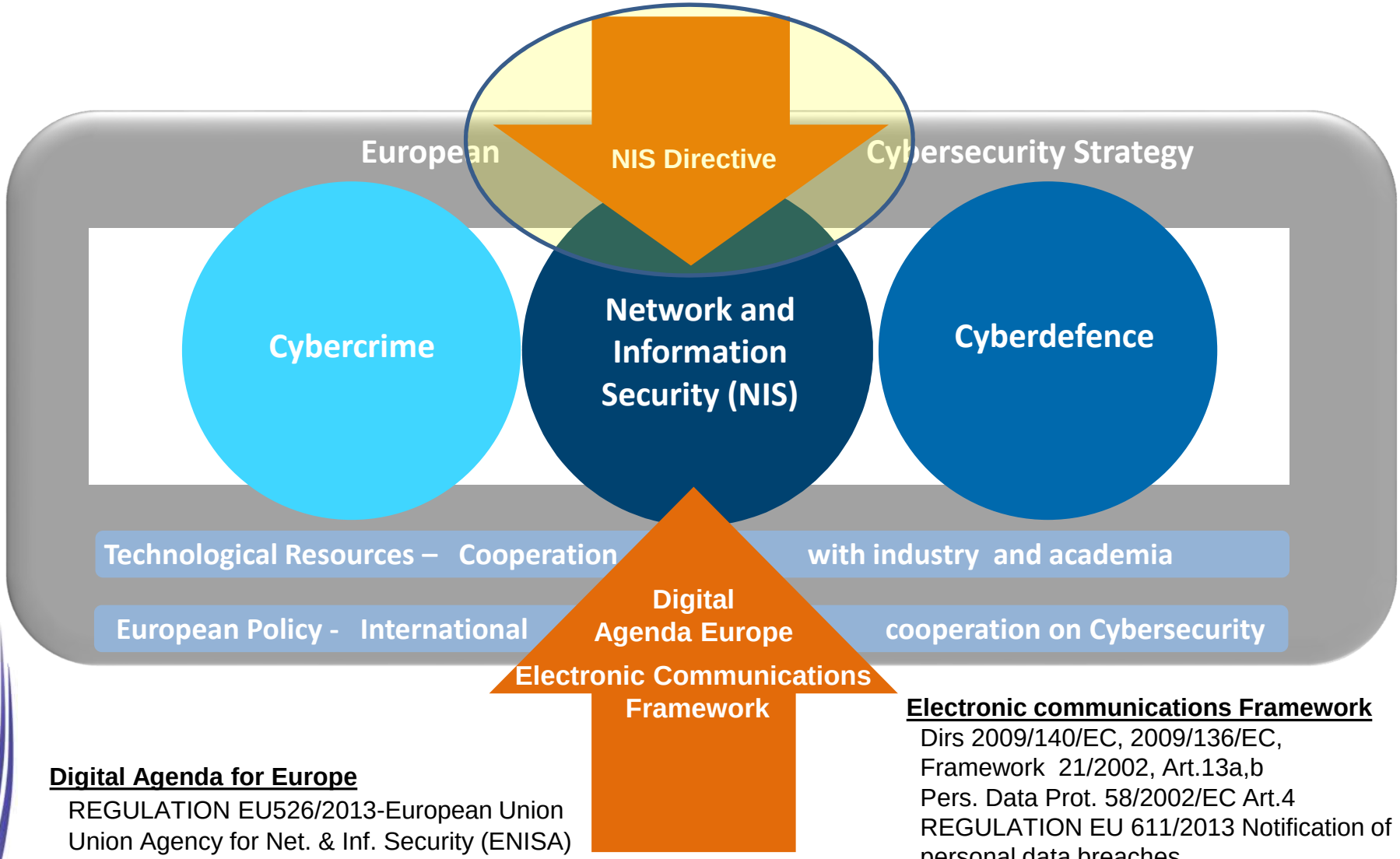
10% probability of a major CII breakdown in the next 10 years
(Source WEF)

Industry	• 2015 • 2014
Finance, Insurance & Real Estate	35% 20%
Services	22% 20%
Manufacturing	14% 13%
Transportation	13% 9%
Wholesale	9% 10%
Top 10 Industries Targeted in Spear-Phishing Attacks	
(source Symantec 2016)	

Office of the Commissioner of Electronic Communications & Postal Regulation

OCECPR

European Cybersecurity Strategy



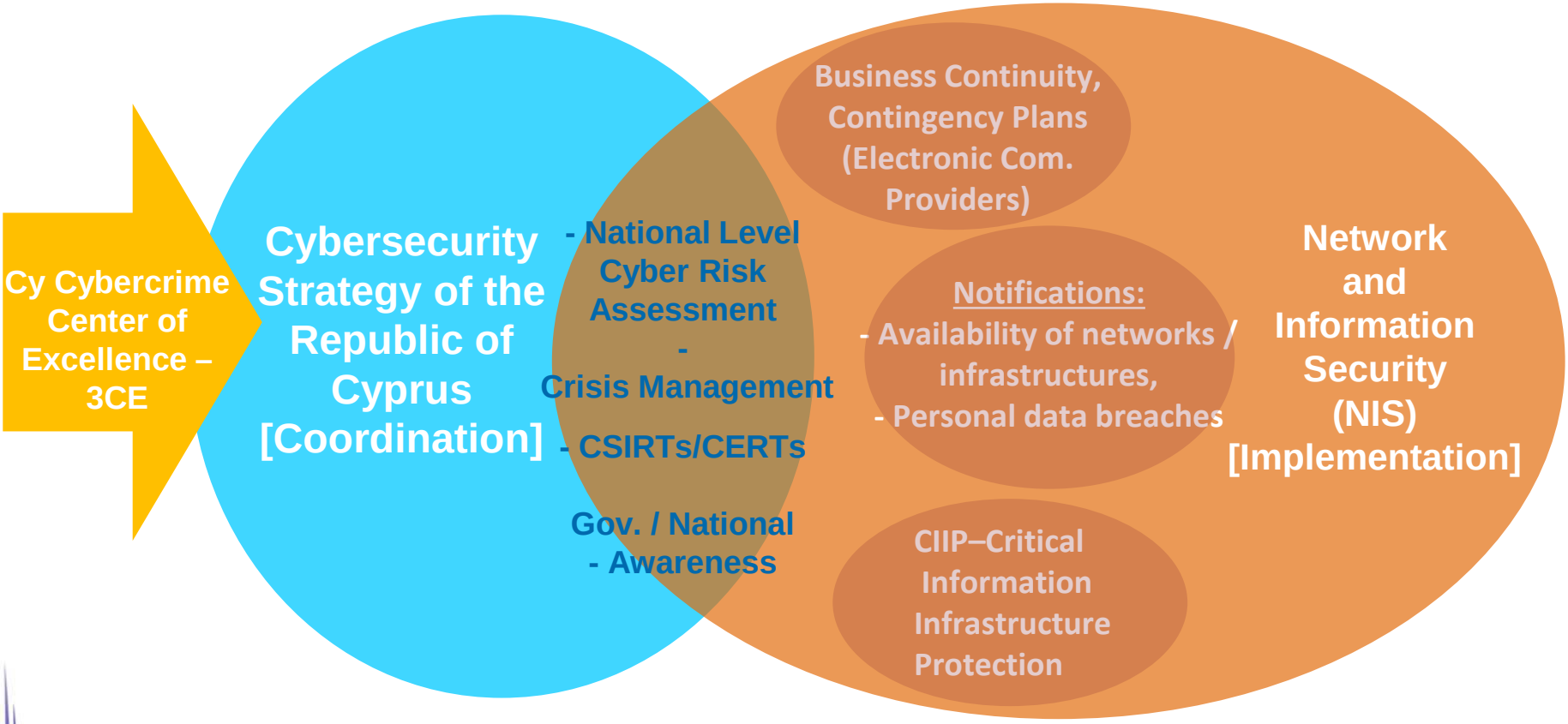
Digital Agenda for Europe

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

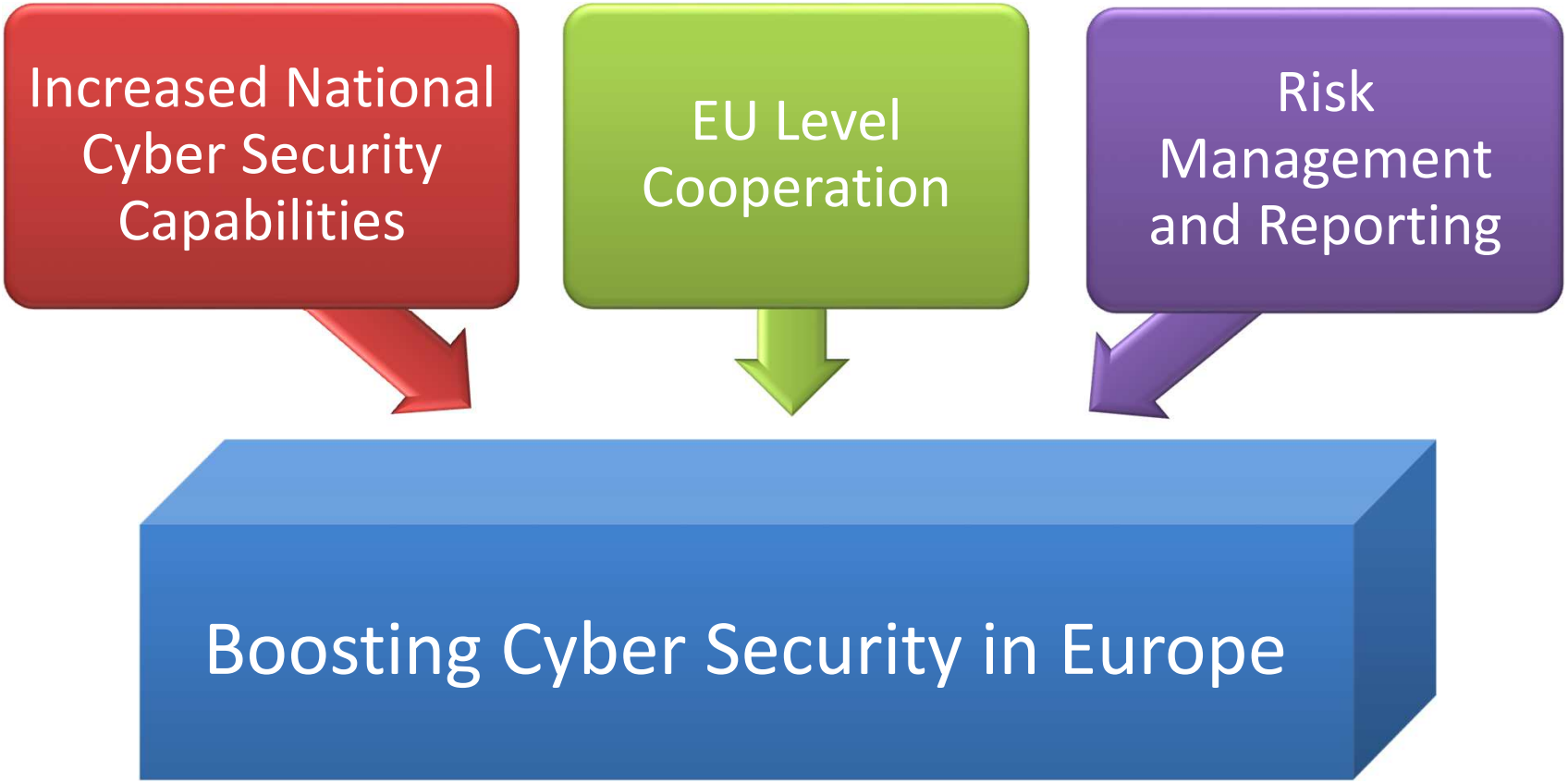
Electronic communications Framework

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

OCECPR Role and Responsibilities

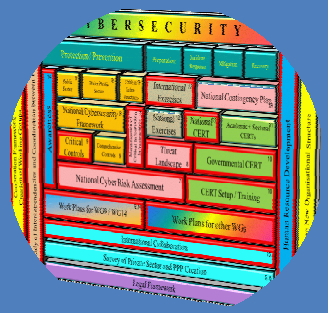


The Objectives



Office of the Commissioner of Electronic Communications & Postal Regulation
OCECPR

Member States (MS) Capability Requirements



National NIS / Cybersecurity Strategy

NIS Competent National Authority

National CSIRT

National Cyber Security Capability

Office of the Commissioner of Electronic Communications & Postal Regulation
OCECPR

Scope of NIS

Operators of Essential Services

- The entity provides a service which is essential for the maintenance of critical societal / economic activities
- The provision of that service depends on network and information systems
- A NIS incident would have significant disruptive effects on the provision of the essential service

Digital Service Providers

- Online marketplaces
- Online search engines
- Cloud computing services

Office of the Commissioner of Electronic Communications & Postal Regulation
OCECPR

Security Requirements

Prevent Risks	• Organisational measures that are appropriate and proportionate to the risk
Ensure NIS	• The measures should ensure a level of NIS appropriate to the risks
Handle Incidents	• The measures should prevent and minimise the impact of incidents on the IT systems used to provide the services

Office of the Commissioner of Electronic Communications & Postal Regulation
OCECPR

Notification Requirements

Operators of Essential Services

- Incidents having a significant impact on the continuity of the essential services they provide

Digital Services Providers

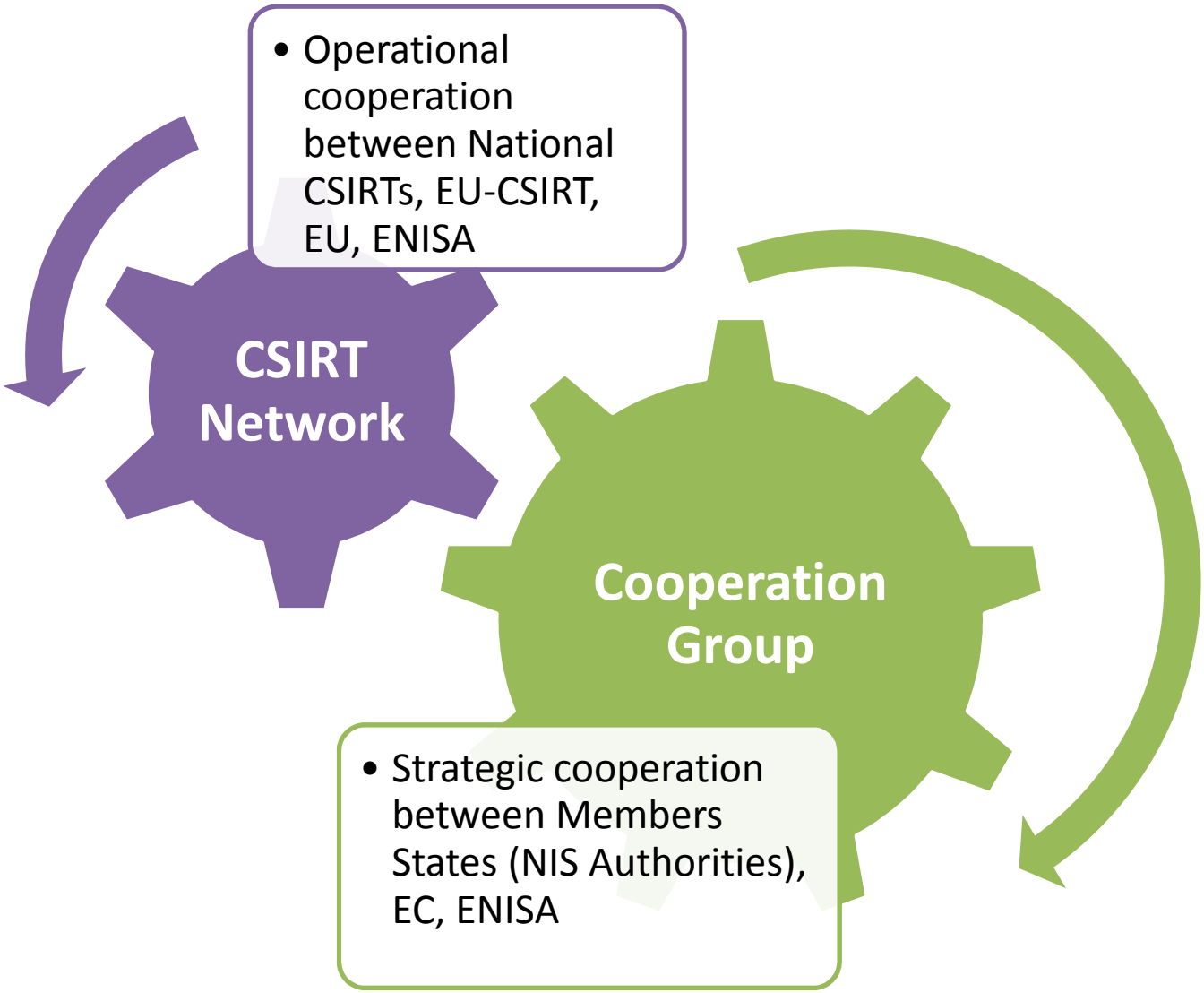
- Incidents having a substantial impact on the provision of a service

Notification Requirements

Parameter	OES	DSP
Number of users affected / relying in the service	✓	✓
Impact – Economic and Societal	✓	✓
Geographic spread	✓	✓
Duration of disruption	✓	✓
Extent of the disruption to the functioning of the service		✓
Importance of the entity for maintaining a sufficient level of service	✓	
Impact - Safety	✓	
Market share (e.g. proportion of national power generated)	✓	
Dependency of other essential sectors on the service	✓	

OES: Operators of Essential Services
DSP: Digital Service Providers

NIS Cooperation Requirements



National CSIRT – Sector Coverage

Electricity

Natural Gas/Oil

Water supply

Transport

“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

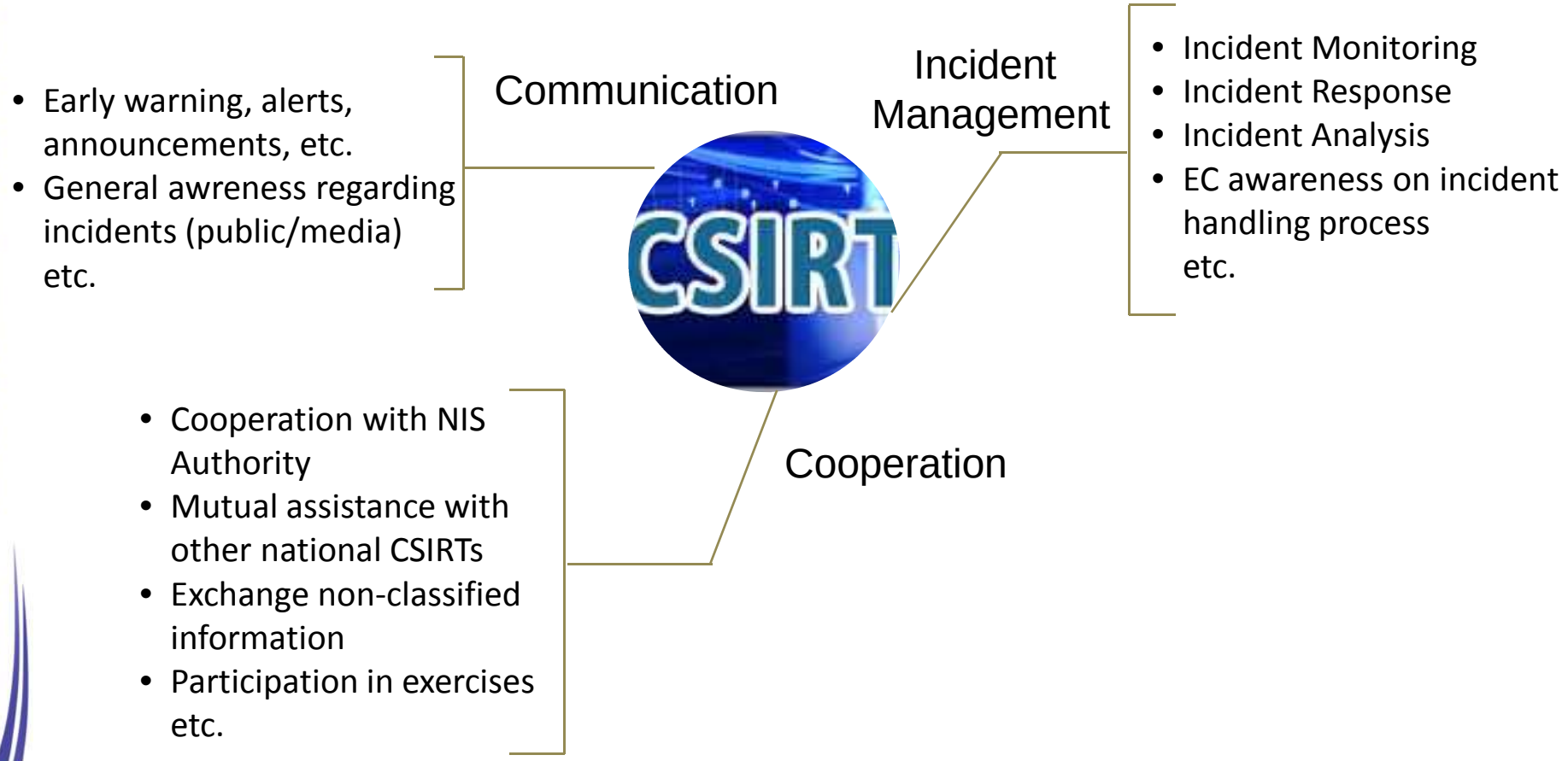
Public Sector/Security Services

Electronic Communications

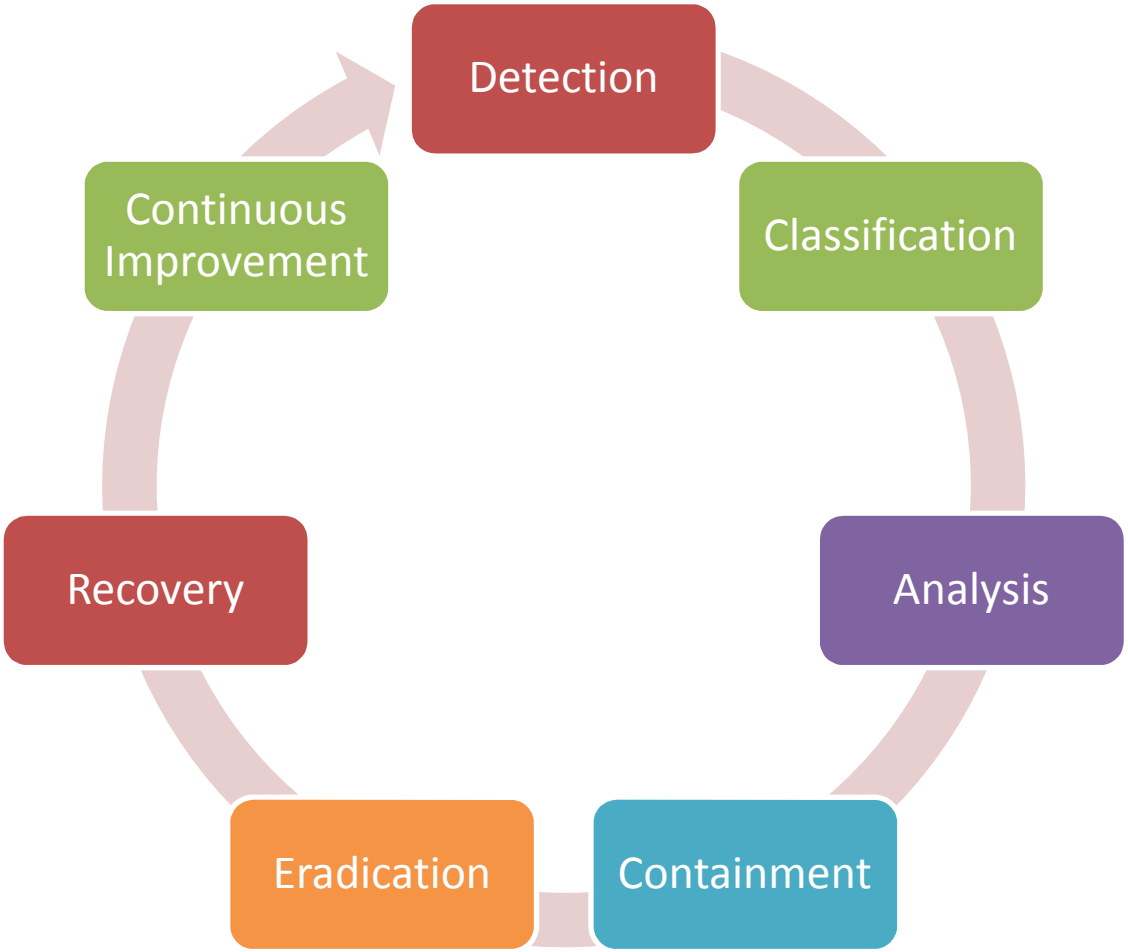
Cyprus National Cybersecurity Strategy Vision

Office of the Commissioner of Electronic Communications & Postal Regulation
OCECPR

National CSIRT – Areas of activities



National CSIRT Functions – Incident Management



Office of the Commissioner of Electronic Communications & Postal Regulation
OCECPR

NIS Authority and National CSIRT

National Cybersecurity Strategy

National Collaboration

Cyber Crisis Management

Operational Coordination

NIS Authority

National CSIRT

Security Requirements

Incident Reporting

Supervision

European Cybersecurity Strategy

International Collaboration

Cooperation Group

CSIRT Network

OSCE

enisa

EUROPEAN COMMISSION

ECS
EUROPEAN CYBER SECURITY ORGANISATION

Operators of Essential Services (~50)
Energy, Water, Transport, Health, Banking, Financial, Digital Infrastructure

Digital Service Providers (<10)
Cloud Computing Services, Online Marketplaces, Search Engines

Office of the Commissioner of Electronic Communications & Postal Regulation

OCECPR

Implementation Timeline

6 **Nov 2018** – MS to identify operators of essential services

5 **May 2018** – Transposition into national law

4 **Feb 2018** – Cooperation Group establishes work programme

3 **August 2017** – Adoption of implementing acts on requirements for DSPs

2 **Feb 2017** – Cooperation Group begins NIS Directive tasks

1 **Aug 2016** – NIS Directive entry into force

Office of the Commissioner of Electronic Communications & Postal Regulation
OCECPR

Thank you