

Free and Open Source Software Communities Meeting



CYBERSECURITY AND DIGITAL TRANSFORMATION

Leandros Maglaras

*Faculty of Computing, Engineering and Media,
De Montfort University, Leicester LE1 9BH, UK*



Outline

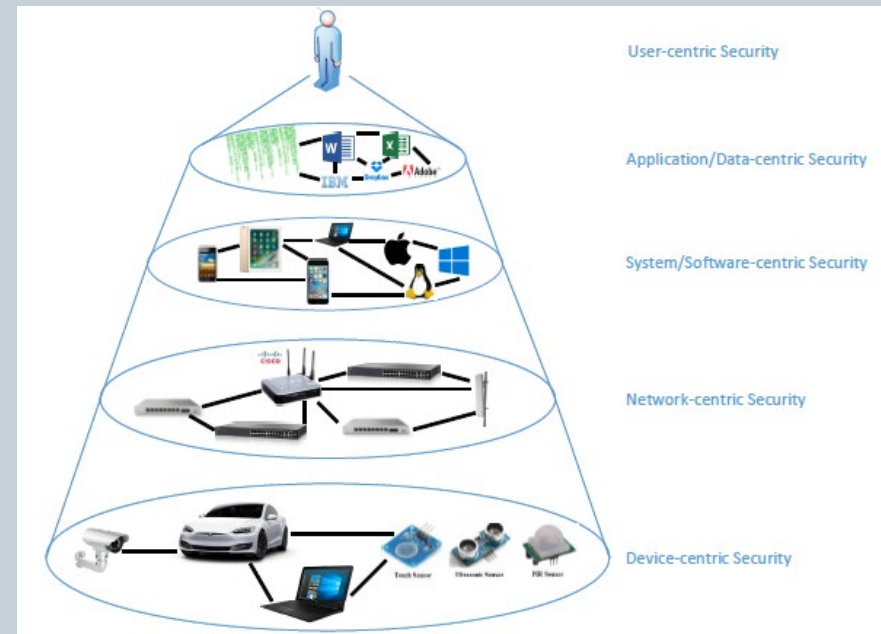
2

- Cybersecurity
- NIS Directive
- National Cybersecurity Strategy
- Identification of Risks
- Ministerial Decree 1027/2019
- Maturity Assessment
- NCSI Index

Layers of Cyber Security

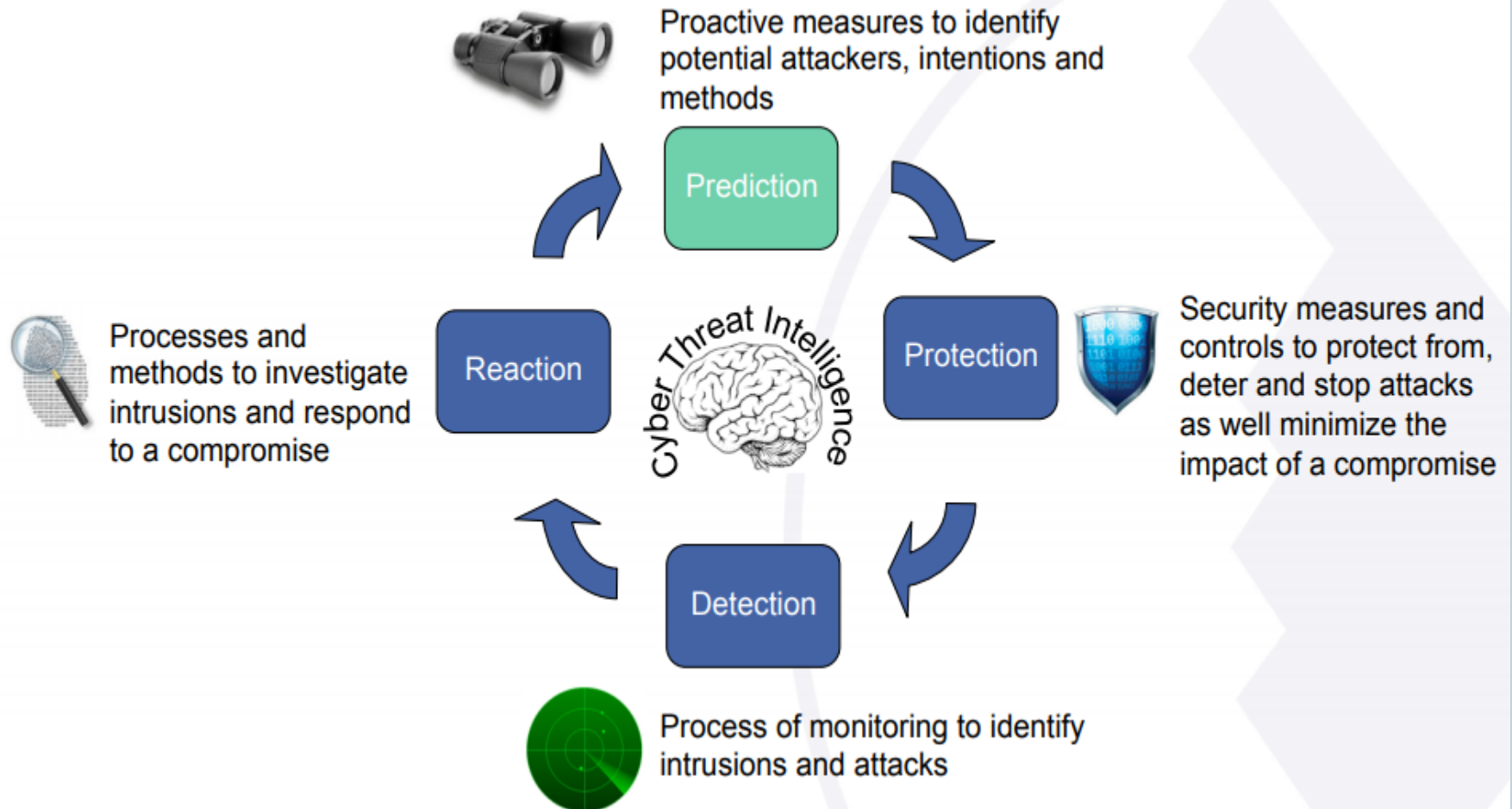
3

- Target environment of the future :
- complex interconnected systems
- highly heterogeneous
- highly dynamic environments
- highly mobile



Lifecycle of Cybersecurity

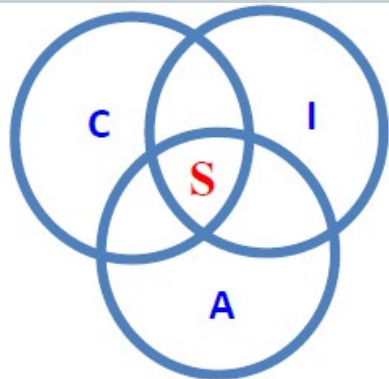
4



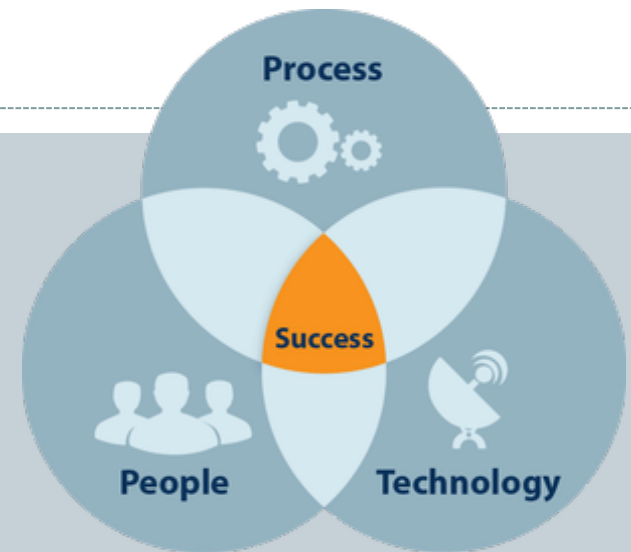
NIS directive – OES

5

- Energy(Electricity, Oil, Gas)
- Healthcare
- Banking
- Transport
- Drinking water supply and distribution
- Digital infrastructure sectors



S = Secure



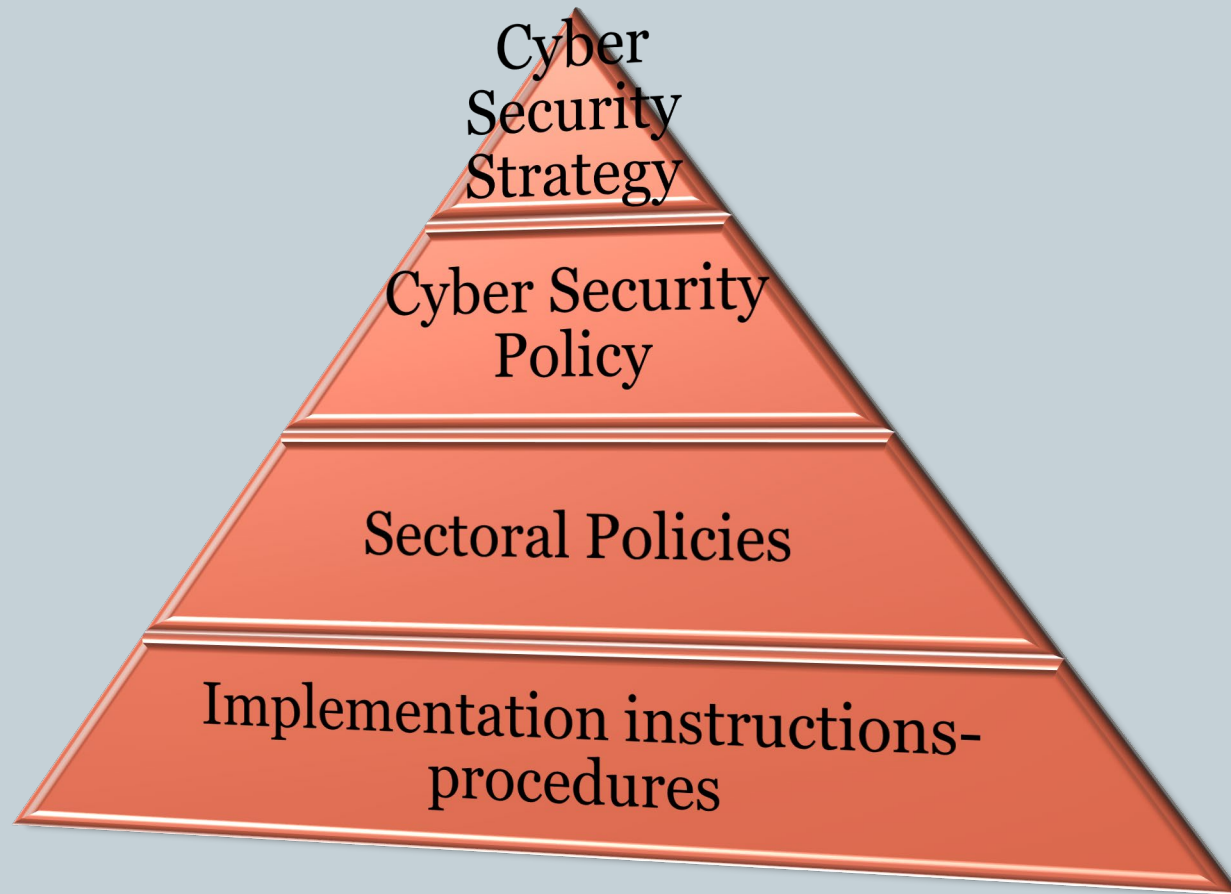
Impact on local, regional, national or global economy

Attack vectors similar to IT

- Reconnaissance
- Malware delivery and propagation
- Spear phishing
- Remote access

Cyber security implementation steps

6

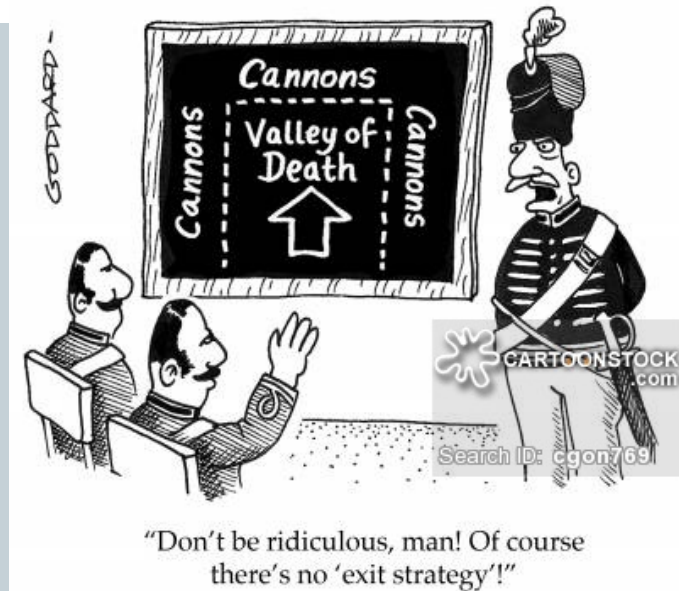


Leandros Maglaras, Mohamed Amine Ferrag, Abdelouahid Derhab, Mithun Mukherjee, and Helge Janicke, “[Cyber Security: From Regulations and Policies to Practice](#)”, International Conference on Strategic Innovative Marketing and Tourism (ICSIMAT 2018), 17-20 October 2018, Athens, Springer Proceedings in Business and Economics

National Cyber Security Strategy

7


- Define objectives
- Define stakeholders
- Define Critical Infrastructures
- Determine basic security requirements
- Cyber security incident handling
- National Cyberspace Contingency Plan
- National preparedness exercises
- User-citizen awareness
- Reliable information exchange mechanisms
- Record and improve the existing institutional framework
- Support of research and development programmes and academic educational programmes
- Cooperation at international level
- Evaluation and revision of the National Strategy



R. o. Greece, "Approval of the National Cybersecurity Strategy of Greece," in *Diavgeia Governmental Platform*, AAA: Ψ4P7465X00-Z6Ω, Athens, 2018.

National Cyber Security Strategy

8

 Greece

Greek National Cyber Security Strategy








[Download in English](#)
PDF document, 694 KB

[Download in Greek](#)
PDF document, 675 KB

Strategy status
Complete

Implementation date
21/09/2017

▼ Objectives (18)

-  Address cyber crime
-  Balance security with privacy
-  Citizen's awareness
-  Critical Information Infrastructure Protection
-  Develop national cyber contingency plans
-  Engage in international cooperation
-  Establish a public-private partnership
-  Establish an incident response capability
-  Establish an institutionalised form of cooperation between public

▼ National Cyber Security Organizations (12)

Authorities (7)

Hellenic Data Protection Authority (DPA) | GDPR
Hellenic Police - Cyber Crime | Cyber Crime
Ministry of Digital Policy, Telecommunications and Media - Directorate of Cyber Security | NIS
Ministry of National Defence (MOD) - Hellenic National Defence General Staff | CSIRT for NIS
Telecommunications & Post Commission (EETT) | National regulator for electronic communications
"ADAE" Hellenic Authority for Communication Security and Privacy
Authority for Communication Security and Privacy
"EYP" National Intelligence Service - National CERT | National CER

Centres (5)

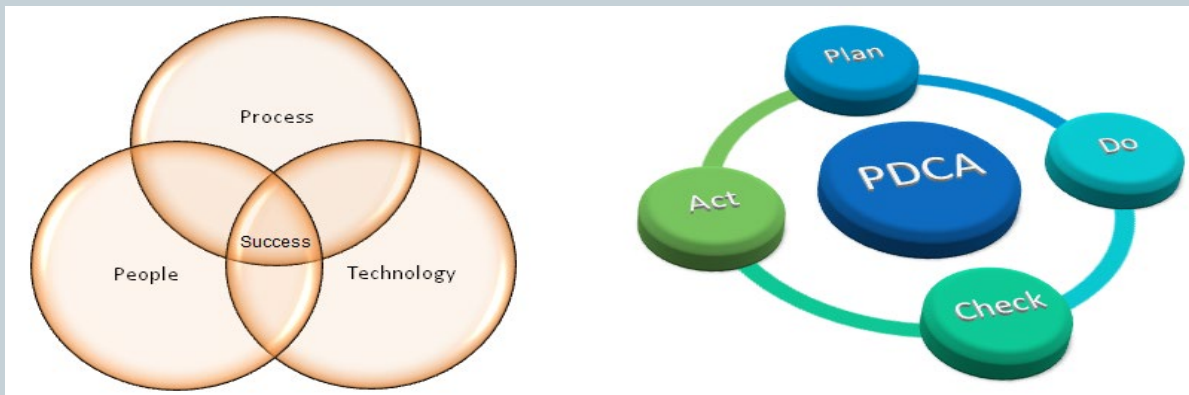
"ATHENA RC" Research & Innovation Information Technologies
"DEMOKRITOS" National Centre for Scientific Research
"FORTH-ICS" Foundation for Research and Technology- Hellas
Institute of Computer Science
"CERTH/ITI" Center for Research and Technology HELLAS

<https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map>

Cyber Security Framework: Success Ingredients & Lifecycle

9

1. Design → NCSA with Working Groups
2. Implementation → Bodies
3. Evaluation → Under the supervision of the NCSA
 - Internal (Self-Assessment)
 - External (Outsourcing)
4. Correction / Redefining → NCSA+ Bodies



Identification of Threats and Risks

10

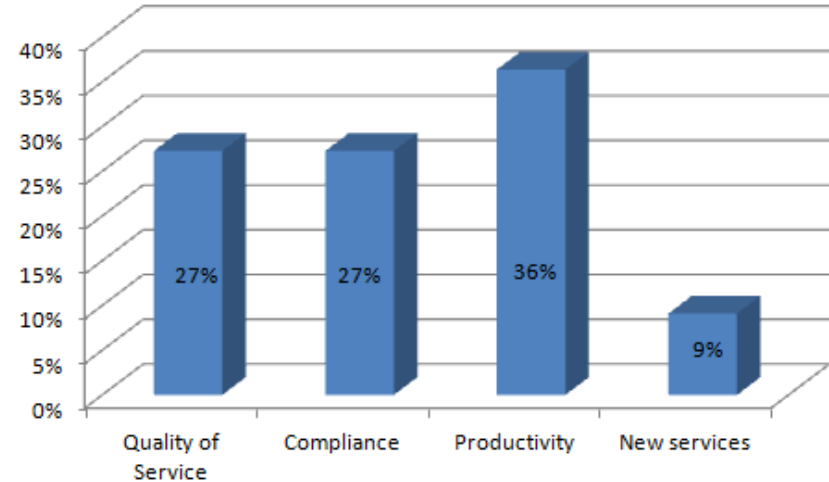
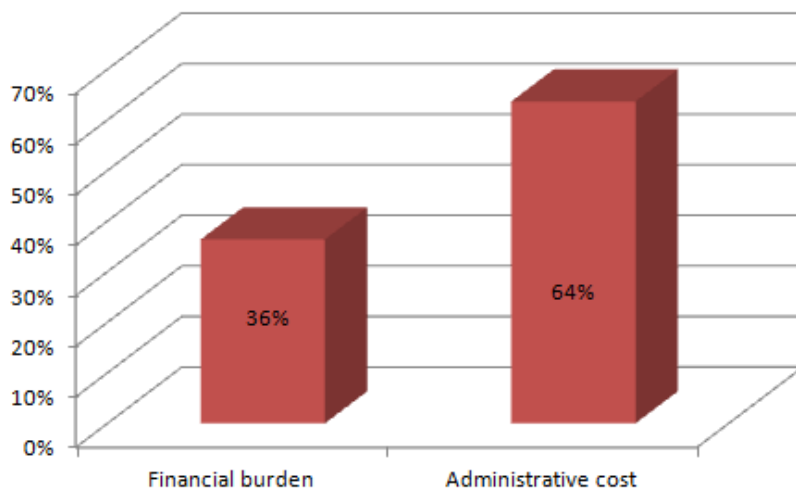
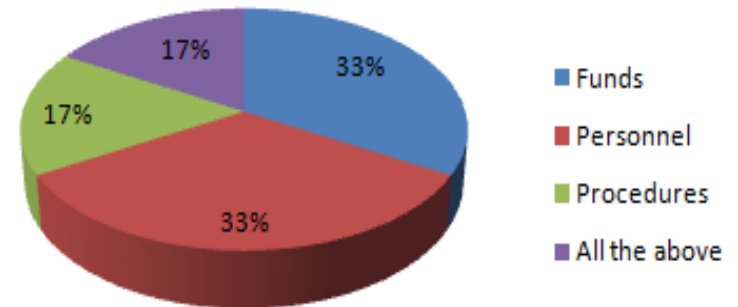
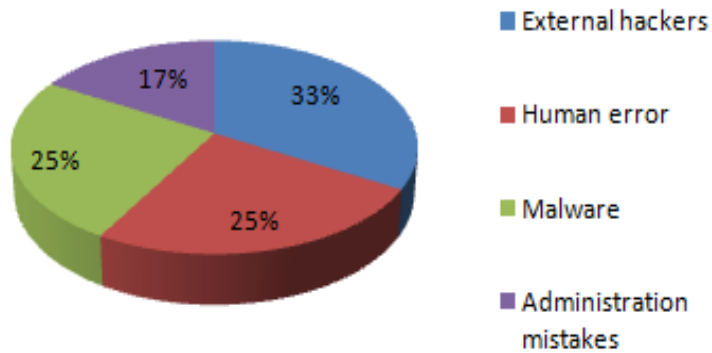
- The aim of this project was to assess the security level of central ICT infrastructures of Greece.

Objectives:

- Build a network of security officers
- Determine major threats to central infrastructures
- Analyze capacity building priorities
- Capture current situation in terms of procedures, security measures and policies
- Determine if there is an incident response plan in place
- Capture training and education policies and mechanisms

Major Threats - Capacity Building Security Updates Pros & Cons

11



Ministerial Decree 1027/2019

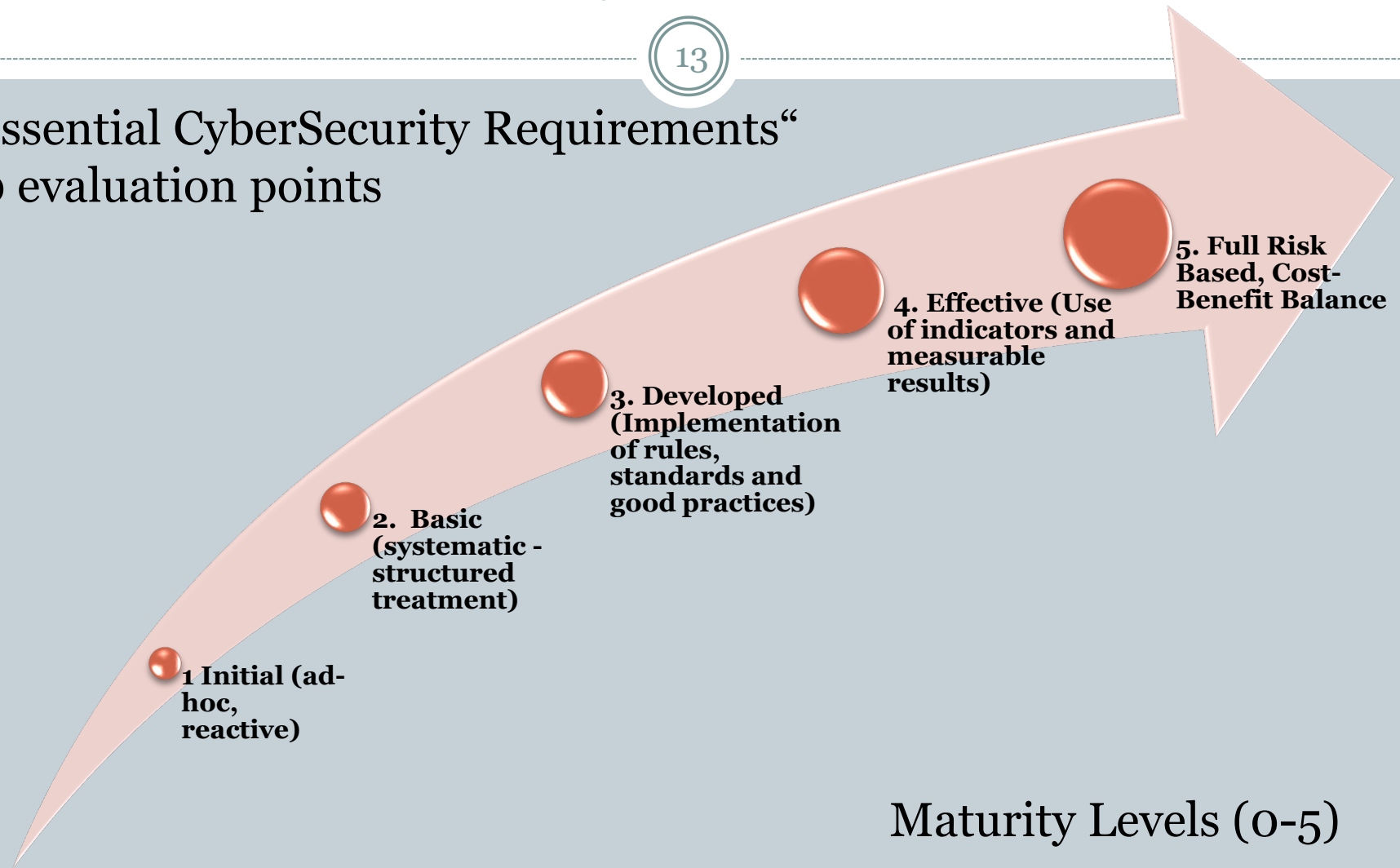
12

- Identification of Operators of Essential Services
- Incident response procedure
 - Incident Notification Platform & Form
- NIS Officer
 - Contact point with the National Authority
 - Informing the Agency on Cybersecurity issues and obligations arising from the law
- Security Policy - objectives
- Minimum security requirements
- Penalties

Maturity Assessment

13

"Essential CyberSecurity Requirements"
20 evaluation points



George Drivas, Argyro Chatzopoulou, Leandros Maglaras, Costas Lambrinoudakis, Allan Cook and Helge Janicke, "[A NIS Directive compliant Cybersecurity Maturity Model](#)", IEEE Computer Society Signature Conference on Computers, Software and Applications (COMPSAC 2020), 13-17 July 2020

- Requirement G1. Security Policy

G. GENERIC

I. IDENTIFY

- Requirement I1. Operational Environment
- Requirement I2. Asset Management
- Requirement I3. Risk Assessment
- Requirement I4. Risk Management Strategy
- Requirement I5. Supply Chain Risk Management
- **Requirement I6. Self-assessment – Improvement**

D. DEFEND

P. PROTECT

- Requirement D.17. Threat detection and analysis
- Requirement D.18. Incident Management
- Requirement D.19. Business Continuity
- Requirement D.20. Disaster recovery

- Requirement P7. Policies, Processes and Procedures for the protection of Basic services
- Requirement P8. Identity Management and access control
- Requirement P.9. Physical and environmental security
- Requirement P.10. Security of systems and applications
- Requirement P.11. Data Security
- Requirement P.12. Backups
- Requirement P.13. Technical Security Measures
- Requirement P.14. System Testing
- Requirement P.15. Change Management
- Requirement P.16. Awareness and training

NCSI Index

15

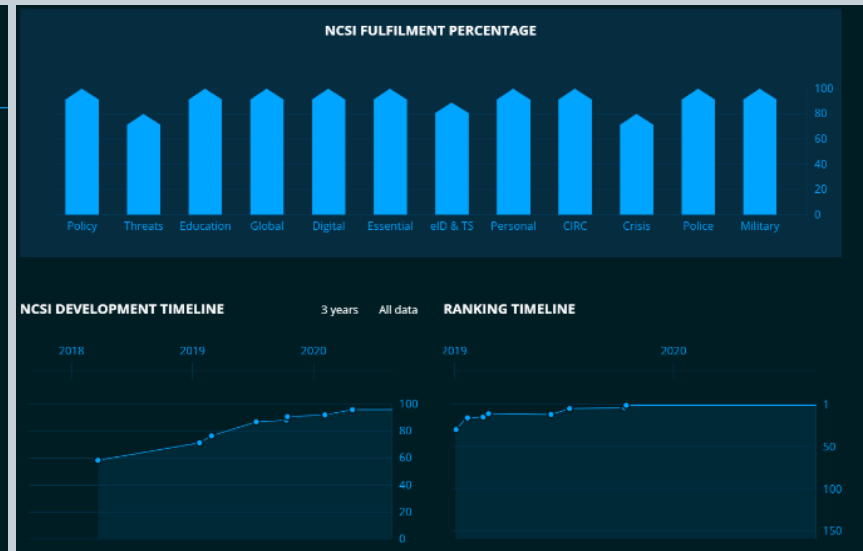
- The NCSI focuses on measurable aspects of cyber security implemented by the central government of each country in four main pillars:
- Legislation in force: legal acts, regulations, decrees, etc.
- Established units: existing authorities, organisations, departments, etc.
- Cooperation formats: committees, working groups, etc.
- Outcomes: policies, exercises, technologies, websites, programmes, etc.

NCSI Index

16

Greece by following a structured development plan, managed to climb several places and reach the 1st place among 160 countries

			
Rank	Country	National Cyber Security Index	Digital Development Level
1.	 Greece	96.10 	65.44 
2.	 Czech Republic	92.21 	69.37 
3.	 Estonia	90.91 	79.27 
4.	 Lithuania	88.31 	70.95 
5.	 Spain	88.31 	73.24 
6.	 Belgium	85.71 	77.62 
7.	 Slovakia	83.12 	66.73 
8.	 Croatia	83.12 	66.91 
9.	 France	83.12 	79.06 
10.	 Finland	81.82 	82.26 



EU initiatives - Stakeholders

17

NIS directive, GDPR regulation etc.

Provide a secure environment

European Cybersecurity Act EU cybersecurity certification framework for ICT products

Will prove confidentiality, integrity, availability and privacy of services, functions and data

European Cybersecurity Industrial, Technology & Research Competence Centre

Increase the competitiveness of the Union's cybersecurity industry

Coordinate funding, ensure cooperation between industries, research institutions and governments, help deploy EU cybersecurity products and solutions

ENISA

Increase of financial and human resources, opportunity to carry out operational tasks



Academic and research
organisations



Industry
(demand and supply)



Public Authorities



Other stakeholders



Union bodies with
relevant experience



Relevant Associations

18

