eHealth project

Dimitra Liveri

Security and Resilience of Com. Networks Officer- ENISA

Critical Information Infrastructure Protection

Sectors	Energy	ICT	Water	Food	Health	Financial	Public & Legal Order	Civil Admin.	Transport	Chemical & Nuclear Industry	Space & Research
AU	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
BE	✓	✓				✓			✓		
CZ	✓	✓	✓	✓		✓		✓	✓		
DK	✓	✓		✓	✓				✓		
EE	✓	✓	✓	✓	✓	✓	✓	✓	✓		
FI	✓	✓	✓	✓	✓	✓	✓		✓		
FR	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
DE	✓	✓	✓	✓	✓	✓	✓		✓		
EL	✓								✓		
HU	✓	✓	✓	✓	✓	✓	✓		✓		
IT	✓								✓		
MT	✓	✓			✓	✓		✓	✓		
NL	✓	✓	✓	✓		✓	✓	✓	✓	✓	
PL	✓	✓	✓	✓	✓	✓		✓	✓	✓	
SK	✓	✓	✓		✓				✓		
ES	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓
UK	✓	✓	✓	✓	✓	✓		✓	✓		
CH	✓	✓	✓	✓	✓	✓		✓	✓		

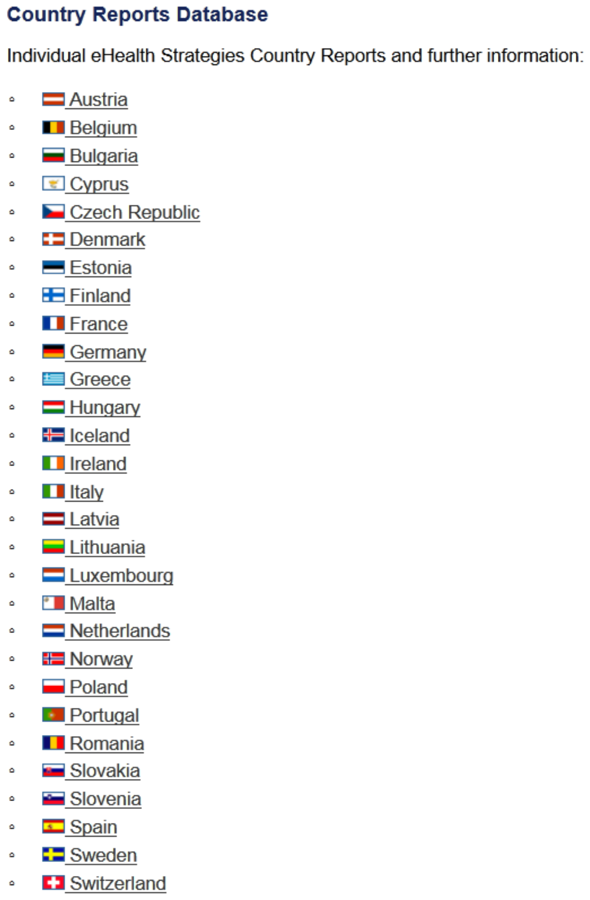
eHealth in the EU and the EC

- The first EU eHealth Action Plan 2004-2011
- The second eHealth Action Plan 2012-2020

- eHealth Strategies across the EU
  - Ministries of health
  - EU task force

- ICT security not in scope
  - Electronic health records
  - Health information networks

- Security incidents increased



Country Reports Database

Individual eHealth Strategies Country Reports and further information:

- Austria
- Belgium
- Bulgaria
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Norway
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland

ENISA work on eHealth – the beginning

- Security and Resilience in eHealth infrastructures and services

- Scope:
  - Health information networks (eHealth networks in hospitals in national/ regional level, peripheral networks that offer access to professionals, hyper-nation private networks)
  - Health jurisdictions responsible (centralized or decentralized approach)
  - Electronic health records (data that is exchanged/ transferred)

eHealth Study

- Approach:
  - Creation of a working group of experts
  - Interviews, surveys (topics: eHealth services and infrastructures, security and privacy requirements, security practices, national strategy and legal aspects)
  - Use case scenarios (eHealth and cloud computing, smart ehealth devices etc)

- Stakeholders:
  - South Denmark
  - Communidad de Madrid
  - Scottish Centre for Telehealth and Telecare
  - INSERM
  - Health Cluster Portugal

Questions?

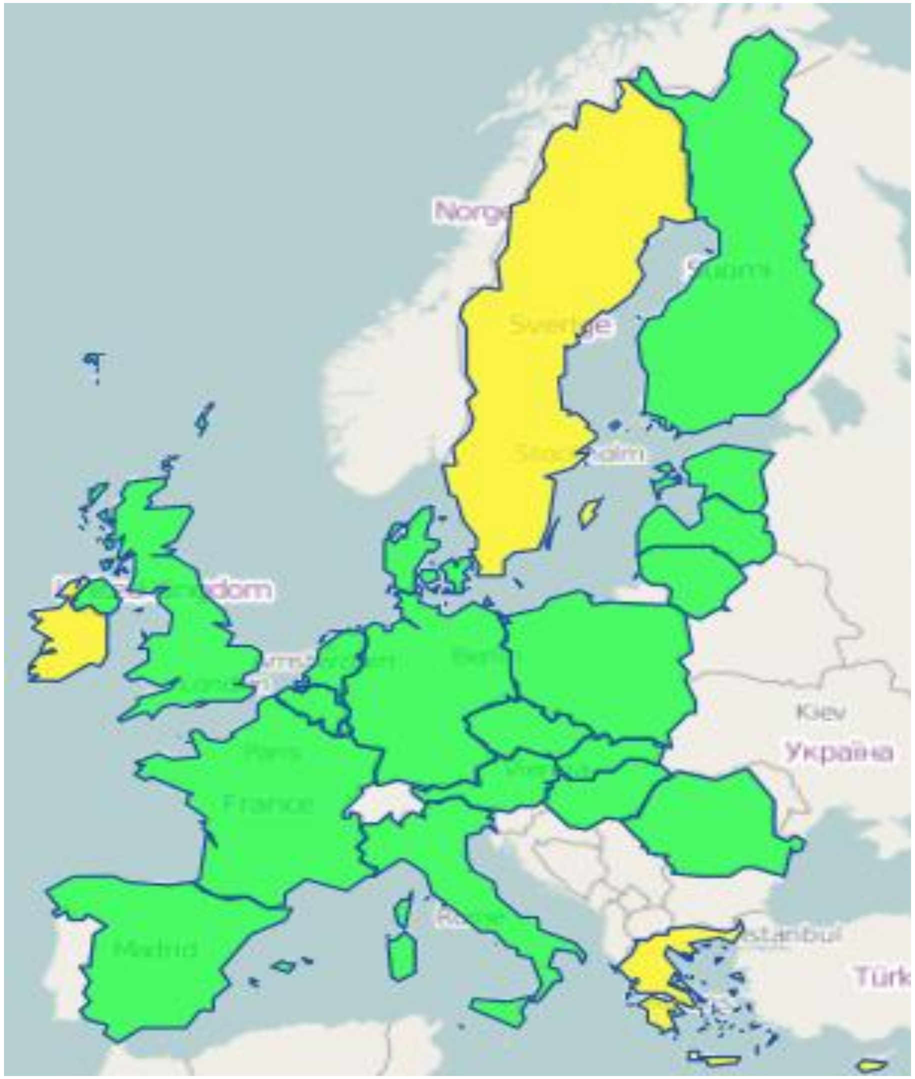
National Cyber Security Strategies

Dimitra Liveri

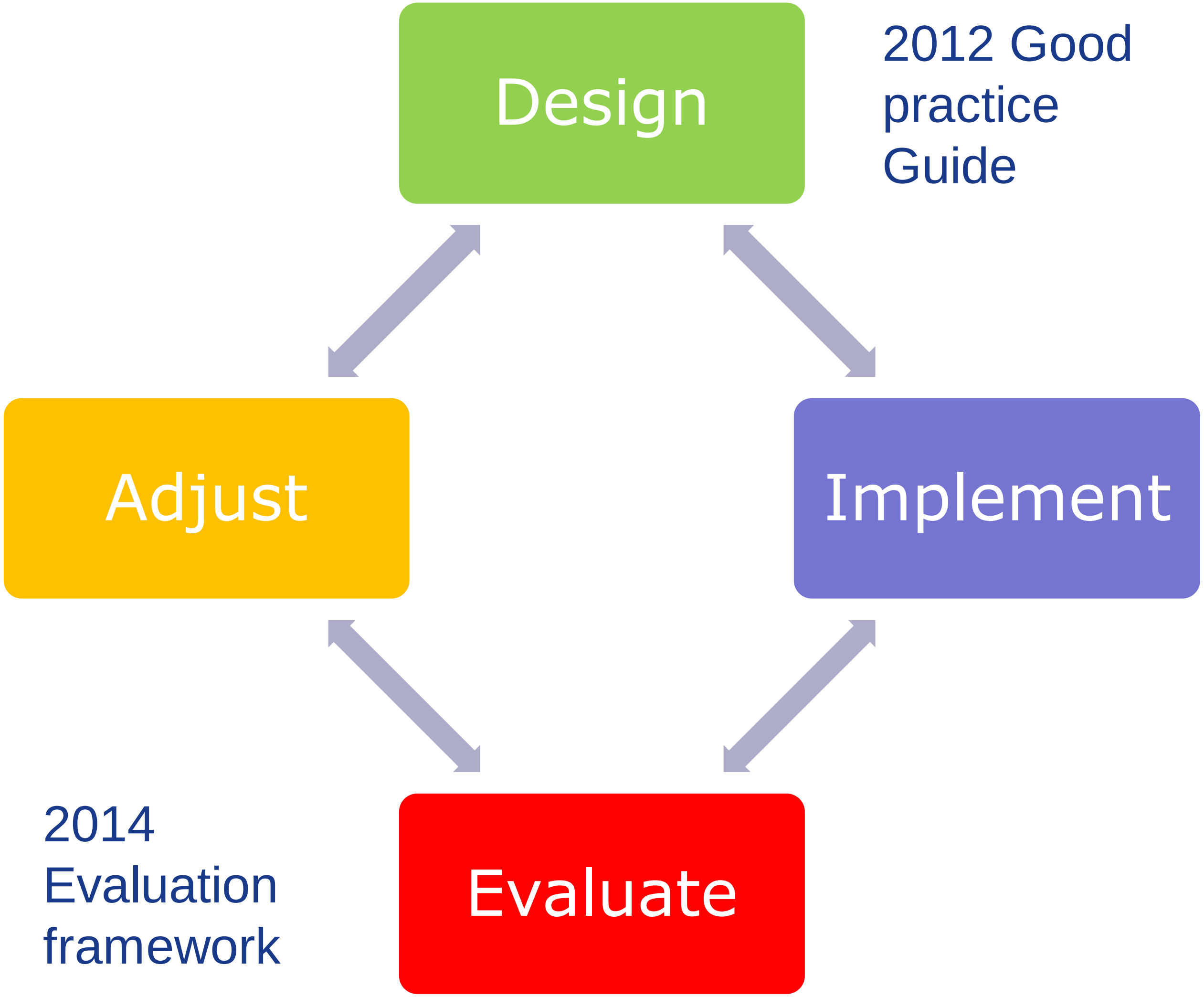
Security and Resilience of Com. Networks Officer- ENISA

NCSS in EU

20 NCSS in EU



ENISA doctrine: NCSS Lifecycle

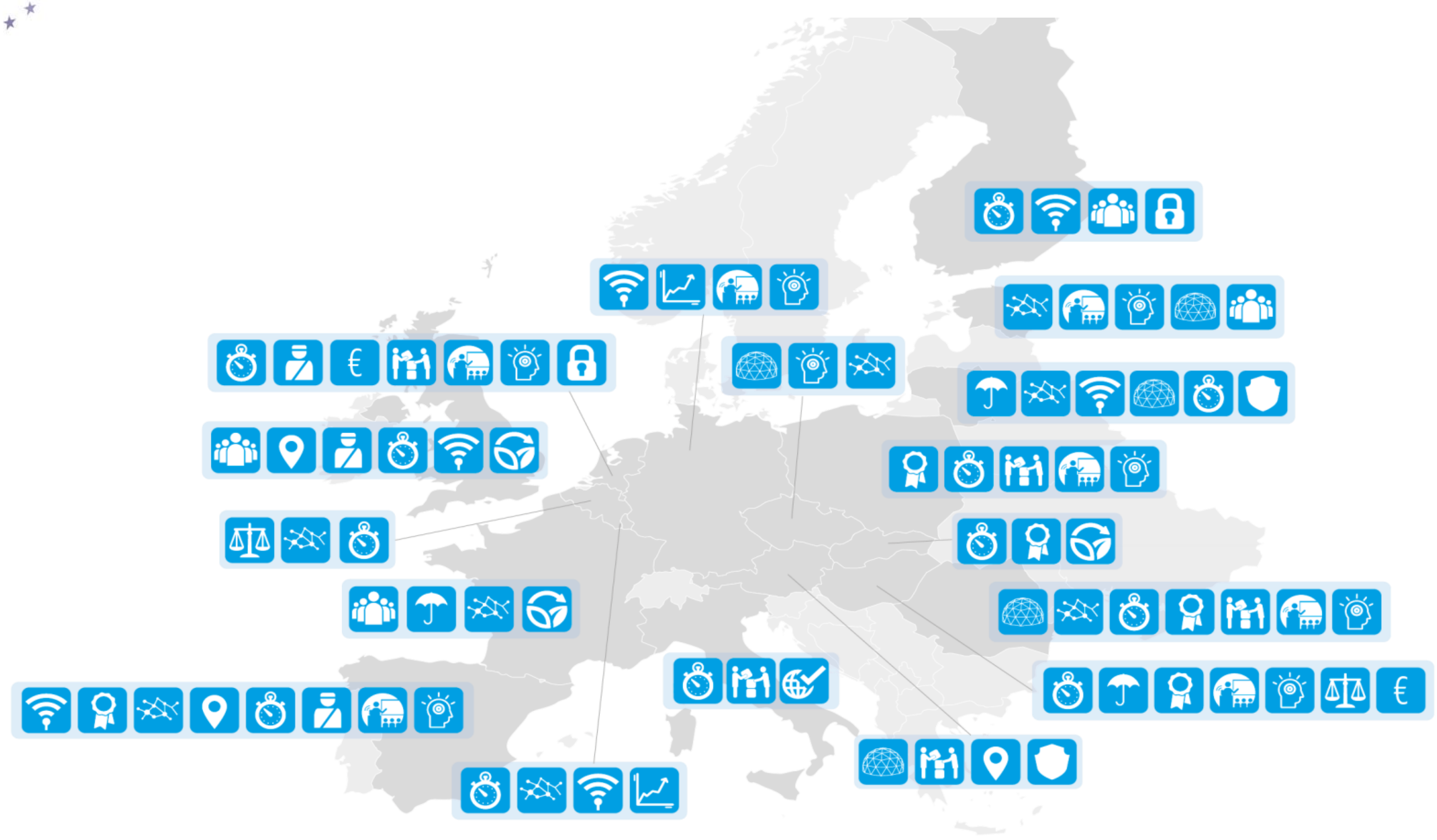


2012 Good practice Guide

2012 Good practice Guide

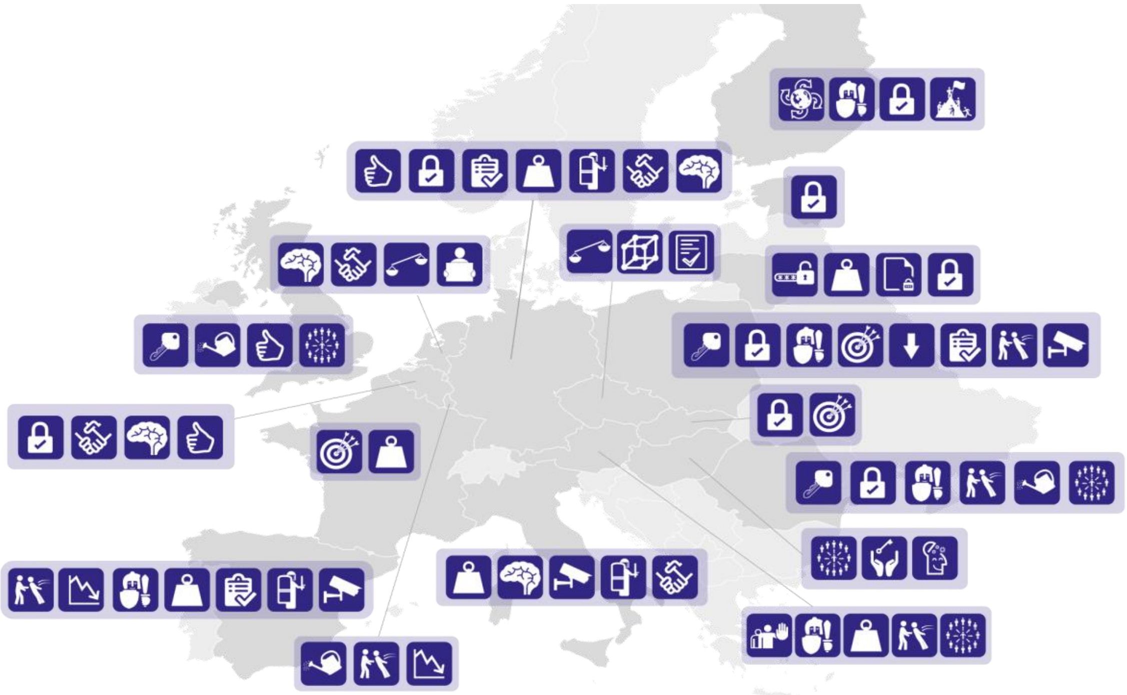
2014 Evaluation framework

High level goals



- Establish and implement legislative framework
- Citizens' perception of sufficient data protection
- Preparedness, resilience and adequate response to cyberthreats and attacks
- Safe use of information and communication in the cyberdomain by citizens, businesses and authorities
- Establish and clarify roles in collaboration between the public and private sector
- Protect digital national information resources
- Promote economy reliant on digitalized industry
- Secure safe place to do business
- € Invest in ICT and innovation for cybersecurity and privacy
- Education and training
- Awareness raising
- Quality of IT and communication products and security standards
- Protection and efficient functioning of critical information infrastructure
- International leadership position
- Tackle cybercrime
- Secure cyberspace with respect for fundamental rights and values
- Sustainability: shape an open, stable and secure cyberspace
- Secure vital national functions and interests against cyber threats and attacks
- Endorse and respect certain rules of behaviours in the digital arena consistent with national values

Long term impact



(Critical) information infrastructure and services: information security

- Better coordination and greater competence of public and private actors involved in the information infrastructure security
- Ensure confidentiality, integrity and accessibility of electronic information and services
- Reduction or elimination of disruptions in the normal functioning of essential services that are vital to functioning of society
- Strengthened capabilities protecting critical information infrastructures, communication networks and services

Business & innovation

- A cyberspace optimal for societal development
- Creation of an internationally recognized competitive and exportable cybersecurity cluster
- Development of effective and innovative ebusiness solutions
- Establishing a cost-effective structure avoiding excessive burden on private entities
- Foster a growing business sector and expanding digital economy
- Innovative public services
- Maintaining and promoting economic and social prosperity
- Stimulate technological capabilities and national academic initiatives in security and privacy knowledge

Rights and society

- A balance between privacy, fundamental rights and liberties, free access to information with the need to guarantee security
- Protection of personal data and privacy
- Ability to counter online criminal activities
- Awareness and a culture of security among citizens and institutions

Public – private relations

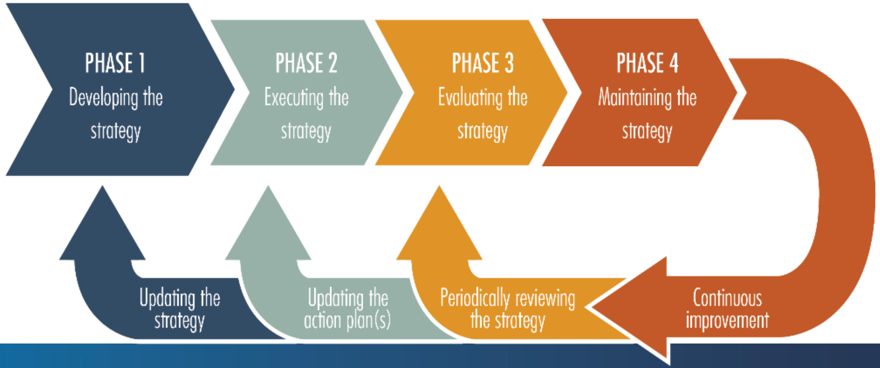
- Allow citizens and businesses to safely handle their affairs with the government

General

- A cybersecurity policy consistent for all the involved agents
- A secure, credible and reliable cyberspace for all users
- Enhanced national security
- Greater confidence in safety of using cyberspace by citizens, businesses, public sector
- Increased resilience against cyberthreats and attacks
- International cooperation
- International leadership position
- Lower effectiveness of internet terrorism and lower costs of countering cyberterrorism
- Prevention of threats
- Better cybersecurity practices and procedures

Supporting the MSs creating a strategy

- Cyber Security is important for the well functioning of the society and economy; MS recognize the importance and develop NCSS
- Critical Services and Infrastructures should be better protected from cyber attacks and threats
- ENISA develops good practices for EU MS and Private Sector to address the emerging issues; training material to support MSs to create a strategy
- Sharing experiences and deploying good practices improves the situation quickly
- When it is necessary, additional regulatory measures are introduced to resolve issues



2015 activities for NCSS

- Focus on Working group: currently 14 MS participating (8 actively) +1 EU Country (CH); need for more participation and contribution
- WG will focus on small papers on NCSS components and will describe the specific approaches per country i.e.
  - CIIP approaches (governance perspective),
  - Public Private Partnerships
  - Capacity building and other topics will come
- Training material setup to deliver training services to MSs that don’t have a strategy
- Evaluation of a NCSS: working deeper on the specific KPIs, the goal is to offer a checklist the MSs can use

2nd ENISA National Cyber Security Conference

RĪGA 2014

EUROPEAN CAPITAL OF CULTURE

13th of May in Riga

Save the date!!

Questions?

Thank you for your attention

For more information visit: http://www.enisa.europa.eu

Follow ENISA: