ENISA EU Threat Landscape

24th February 2015

Dr Steve Purser
ENISA Head of Department

Agenda

- ENISA – Areas of Activity
- Key Policy Statements
- The EU Cyber Security Strategy
- The Proposal for an NIS Directive
- National Cyber Security Strategies
- Economic Considerations

ENISA Activities

Recommendations

Policy Implementation

Mobilising Communities

Hands on

Agenda

- ENISA – Areas of Activity
- Key Policy Statements
- The EU Cyber Security Strategy
- The Proposal for an NIS Directive
- National Cyber Security Strategies
- Economic Considerations

Key Policy Documents

- The new ENISA Regulation (EU) No 526/2013.
- The Cybersecurity Strategy of the EU
- The proposal for NIS directive
- Council Conclusions on the Cybersecurity Strategy
- Directive on ECIs
- The CIIP Action Plan
- Commission Communication on Critical Information Infrastructure Protection
- Electronic Communications Regulatory Framework

Key Policy Documents

- Review of the Data Protection Framework.
- Commission Regulation on the measures applicable to the notification of personal data breaches
- Regulation on electronic identification and trusted services for electronic transactions in the internal market
- European cloud computing strategy
- …..

Policy Considerations : ETL 2014

- Europe, in its role as a world leader in data privacy, should continue with setting up the standards in this area.
- Building expertise in cyber-security and resilience of Cyber Physical Systems is an economic opportunity for Europe.
- Current revelations regarding certain national security agencies have increased fragmentation risks for the internet.
- Surveillance has a negative impact to the trust in the internet where end users are concerned.
- Breach notification needs to be put on a wider basis via corresponding regulations in various areas/sectors, eventually covering end-user impact
- New, sophisticated attacks make the development of new detection methods and new security controls necessary.

Agenda

- ENISA – Areas of Activity
- Key Policy Statements
- The EU Cyber Security Strategy
- The Proposal for an NIS Directive
- National Cyber Security Strategies
- Economic Considerations

Strategic Priorities

- The Five strategic objectives of the strategy are as follows:
  - Achieving cyber resilience
  - Drastically reducing cybercrime
  - Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)
  - Developing the industrial and technological resources for cybersecurity
  - Establishing a coherent international cyberspace policy for the European Union and promote core EU values.

ENISA explicitly called upon.

Achieving Cyber Resilience

- Introduces ENISA and explains the policy on NIS.
- Makes reference to articles 13a & 13b.
- Introduces the legislative proposal.
- Stresses the importance of the following:
  - The establishment of a cybersecurity culture to enhance business opportunities and competitiveness.
  - Reporting significant incidents to the national NIS competent authorities.
  - Exchange of information between National NIS competent authorities and other regulatory bodies.
  - Recognises that exercises at EU level are essential to simulate cooperation among the MS and the private sector.

Achieving Cyber Resilience

- The Commission asks ENISA to:
  - Assist the Member States in developing strong national cyber resilience capabilities.
  - Examine in 2013 the feasibility of Computer Security Incident Response Team(s) for Industrial Control Systems (ICS-CSIRTs) for the EU.
  - Continue supporting the Member States and the EU institutions in carrying out regular pan-European cyber incident exercises.
- In terms of raising awareness:
  - Propose in 2013 a roadmap for a "Network and Information Security driving licence".
  - Support a cybersecurity championship in 2014, where university students will compete in proposing NIS solutions.

Developing Resources

- There is a risk that Europe becomes excessively dependent on ICT and on security solutions developed outside its frontiers.
- Hardware and software components used in critical services and infrastructure must be trustworthy, secure and guarantee the protection of personal data.
- In order to mitigate this risk, the strategy proposes two action areas:
  - Promoting a Single Market for cybersecurity products.
  - Fostering R&D investments and innovation.

Single Market for Products

- A high level of security can only be ensured if all in the value chain make security a priority.
- The strategy aims to increase cooperation and transparency about security in ICT products:
  - It calls for the establishment of a platform to identify good cybersecurity practices across the value chain.
- COM will support the development of security standards and assist with EU-wide voluntary certification schemes.
  - Cloud computing and data protection.
  - critical economic sectors - Industrial Control Systems, energy and transport infrastructure.

R&D and Innovation

- R&D should fill technology gaps in ICT security and prepare for the next generation of security.
- The Horizon 2020 Framework Programme for Research and Innovation was launched in 2014:
  - There are specific objectives for trustworthy ICT as well as for combating cyber-crime.
- Specific attention will be drawn at EU level to optimising and better coordinating various funding programmes.
- ENISA could also play a valuable role here:
  - Providing advice on how to align H2020 research with cyber security policy objectives.
  - Improving the interaction between H2020 initiatives and industry representatives.

Developing Resources

- The Commission asks ENISA to:
  - Develop, in cooperation with relevant stakeholders, technical guidelines and recommendations for the adoption of NIS standards and good practices in the public and private sectors.
    - The Agency is working closely with COM, the standards organisations and the CSCG.
  - Collaborate with Europol to identify emerging trends and needs in view of evolving cybercrime and cybersecurity patterns so as to develop adequate digital forensic tools and technologies.
    - ENISA is currently represented on the EC3 Programme Board.

Further Involvement of ENISA

- Although ENISA is not explicitly mentioned in the other strategic priorities, there is clearly a role for the Agency.
- The EU Internal Security Strategy explains how ENISA should collaborate with the recently established EU Cyber Crime Centre.
- We have a role in creating a strong culture of NIS throughout the EU.
- This can only be achieved by bringing communities together and ensuring that information on NIS is shared between such communities in an appropriate manner.

Agenda

- ENISA – Areas of Activity
- Key Policy Statements
- The EU Cyber Security Strategy
- The Proposal for an NIS Directive
- National Cyber Security Strategies
- Economic Considerations

The Legislative Proposal

- Key points are as follows:
  - Will help establish common minimum requirements for NIS at national level.
  - Requires Member States to designate national competent authorities for NIS, set up a competent CERT and adopt a national NIS strategy and a national NIS cooperation plan.
  - Explains the role of the CERT EU regarding the EU institutions, agencies and bodies.
  - Requires the establishment of coordinated prevention, detection, mitigation and response mechanisms.
  - Requires the private sector to develop, at a technical level, its own cyber resilience capacities and share best practices across sectors.

The Legislative Proposal - Opportunities

- The legislative proposal correctly leaves a lot of room for HOW articles are implemented.
- An example is provided by Article 1:

1. This Directive lays down measures to ensure a high common level of network and information security (hereinafter referred to as "NIS") within the Union.

- ENISA will work together with the Member States and the private sector to identify the optimal implementation strategies.
- This is the approach we used for Article 13a.

Agenda

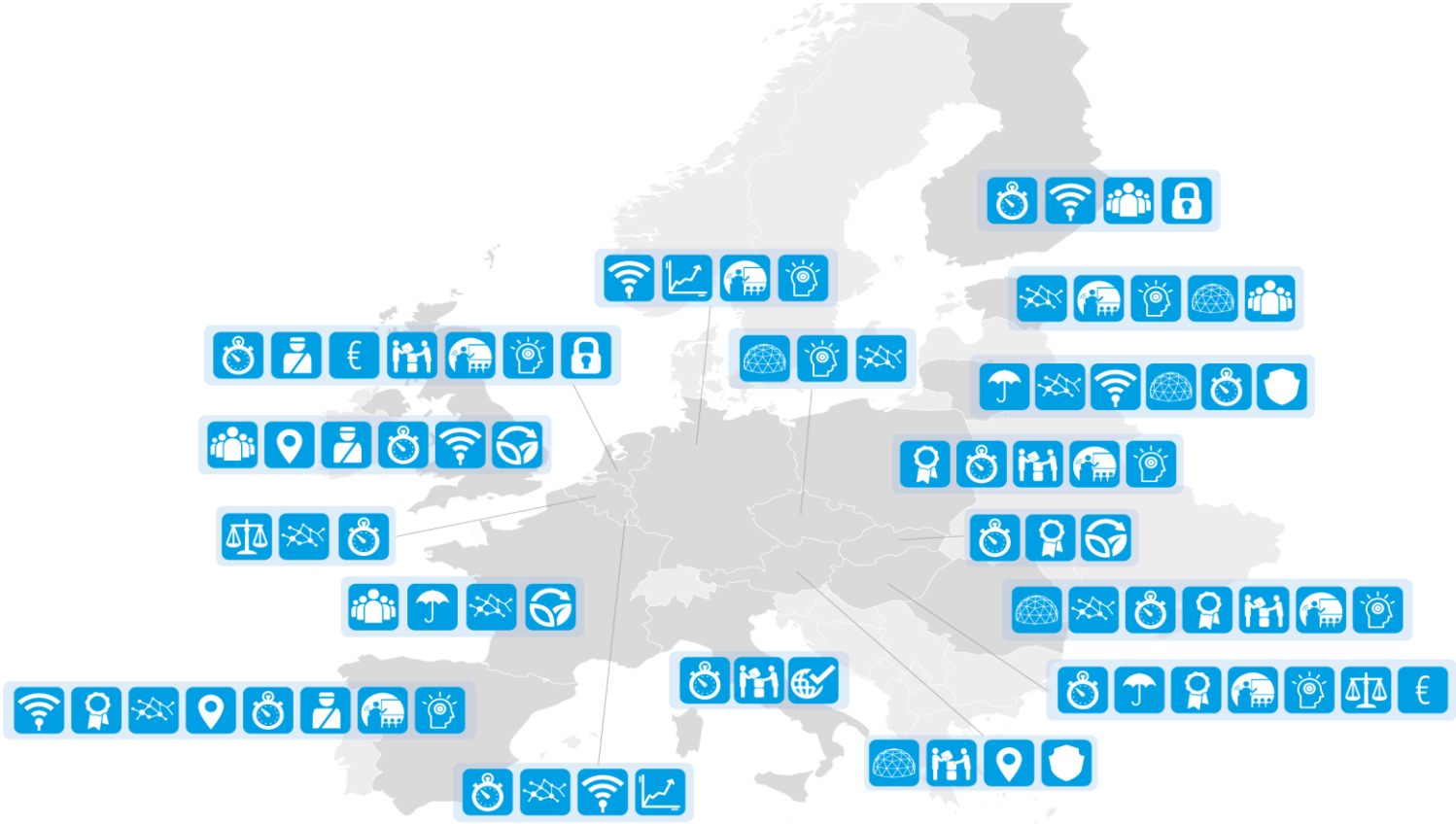
- ENISA – Areas of Activity
- Key Policy Statements
- The EU Cyber Security Strategy
- The Proposal for an NIS Directive
- National Cyber Security Strategies
- Economic Considerations

National Cyber Security Strategies in the EU

19 EU MS have a strategy

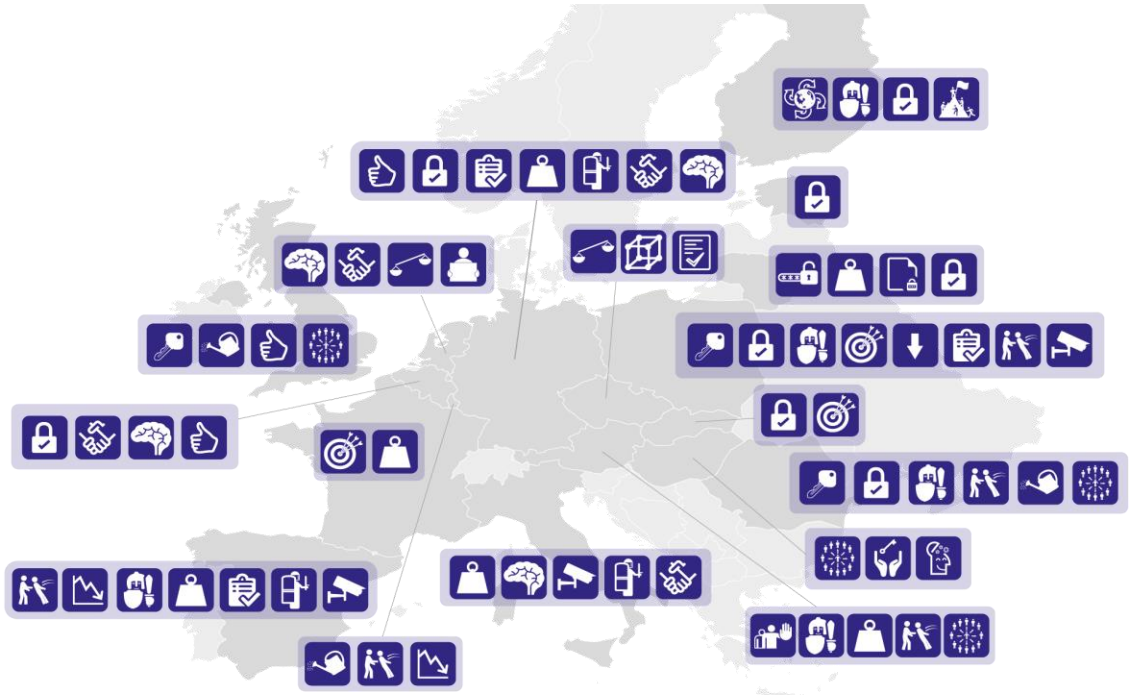
Source: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

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

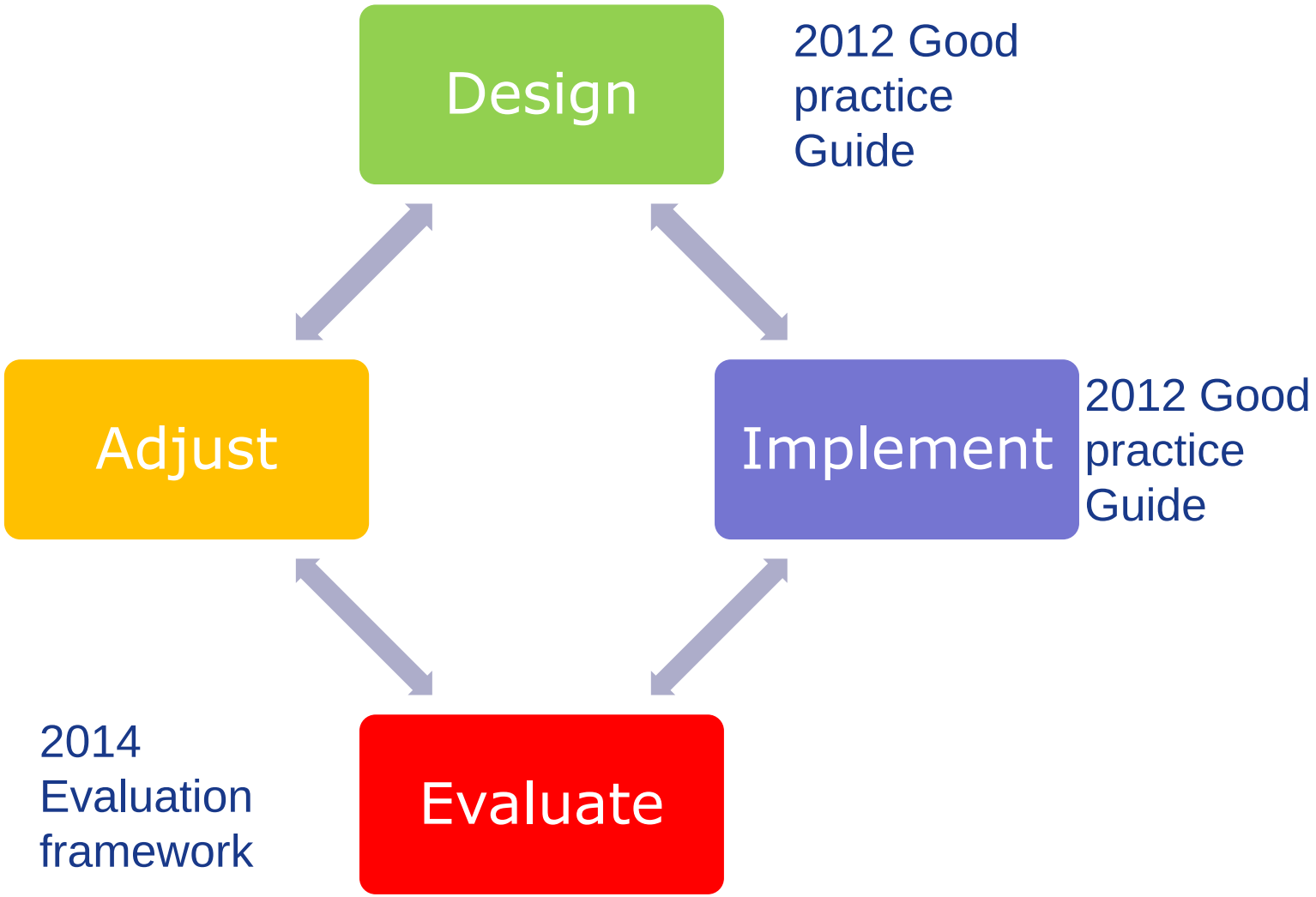
Public – private relations

- 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

ENISA doctrine: NCSS Lifecycle



Agenda

- ENISA – Areas of Activity
- Key Policy Statements
- The EU Cyber Security Strategy
- The Proposal for an NIS Directive
- National Cyber Security Strategies
- Economic Considerations

The Economic Challenge

- The EU approach to cyber security should be closely aligned with EU industrial policy.
- Good cyber security practice can contribute to EU economic development in two different ways:
  - By helping EU industry that provides products or services in information security to become more competitive.
  - By helping unrelated industries to achieve the appropriate level of security at minimal cost.
- Furthermore, cyber security may be a useful way of developing contacts with SMEs throughout the EU.
- ENISA is discussing these ideas with the Commission and with the private sector under the heading of Digital Sovereignty.

Using NIS to Support Growth

- ENISA promotes approaches to NIS that support economic growth, by:
  - Assisting operational communities in translating abstract policy statements into real-world operations.
  - Making lessons learned in one community available to other affected communities – promotion of best practice.
  - Ensuring that policy can be implemented in an economically efficient way by promoting economically efficient processes.
  - Identifying gaps and barriers to EU economic development that arise out of NIS issues.

Questions?

Follow ENISA: