# NIS Standardisation – ENISA view

Dr. Steve Purser

Brussels, 19th September 2017

European Union Agency for Network and Information Security

# Instruments For Improving Cybersecurity

- Policy makers have a number of instruments at their disposal for improving cybersecurity:
  - International treaties and agreements
  - EU legislation and national legislation
  - Policy statements and strategy
  - Standards
  - Good practices
  - Awareness raising and training
- It is important to choose the right instrument for the right problem.
- Standards are well suited to problems that require a normalised approach and are stable in time.

# The Importance of Standards (1)

- Improving efficiency and effectiveness of key processes.
  - Standardised procedures of are critical importance in cross-border and cross community communication.
  - Standard Operating Procedures are key to the EU response mechanism to cyber incidents.
  - Where industry is concerned, standards such as ISO 27001 encourage the adoption of standard organisational structures.
- Facilitating systems integration and interoperability
  - Security products need to interoperate in different environments.
  - Many security weaknesses occur at the interface of different technologies or products.
  - Needs to be balanced against risk of creating a single target.

# The Importance of Standards (2)

- Enabling different products or methods to be compared in a meaningful manner.
  - Standardisation of testing methods makes it possible to compare security products in a meaningful manner.
  - Example : level of compatibility of cryptographic modules with the FIPS 140-2 standard.
- Providing a means for users to assess new products or services.
  - Standards increase the level of transparency of the product or service to the end user.
- Structuring the approach to deploying new technologies or business models.

# The Importance of Standards (3)

- Simplification of complex environments.
  - The complexity of real-life systems is one of the biggest barriers to achieving coherent security solutions.
  - Standards help reduce complexity, reducing the number of special cases that a security solution has to take account of.
  - Techniques such as ‘defence in depth’ provide a mitigation for the problem of the standardised target….
- Promoting economic growth.
  - The use of open standards encourages information exchange between developers and is likely to result in greater competition between product developers.

# Standardisation Challenges

- ## Organisational challenges
  - The number of SDOs and the number of published standards has increased, which can be a source of confusion to end users.
  - This issue is not restricted to the area of standards….

- ## Areas of standardisation
  - standardisation activities in the area of NIS tends to be driven by areas of work that lay in line with the core interests of service providers.
  - There is no single, continuous “line of standards” related to cyber security, but rather a number of discrete areas which are the subject of standardisation.
  - What does a cyber security standard look like?

- ## Lack of awareness
  - In many areas, customers still do not demand open standards.

# Standardisation Challenges

- Lack of agility
  - Standards move slowly, ICT moves fast….
  - Good Practice might be a precursor to standards.
- Competing sets of standards
  - The great thing about standards is that there are so many to choose from….
  - Public key Infrastructure (PKI) for instance often uses a combination of standards : X.509 (ITU), PKIX (IETF), PKCS (RSA) standards….
- Economic considerations
  - Proprietary standards often result in wasted resources.
  - Companies with a dominant position have few incentives to adopt interoperable standards,

# ENISA & Standardisation

## Legislation

- Regulation 460/2004: "the Agency shall [..] track the development of standards for products and services on network and information security"
- Regulation 526/2013, "Support research and development and standardisation, by: facilitating the establishment and take-up of European and international standards for risk management and for the security of electronic products, networks and services"
- NIS Directive: “ENISA, [..] shall draw up advice and guidelines regarding the technical areas [..] as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered”

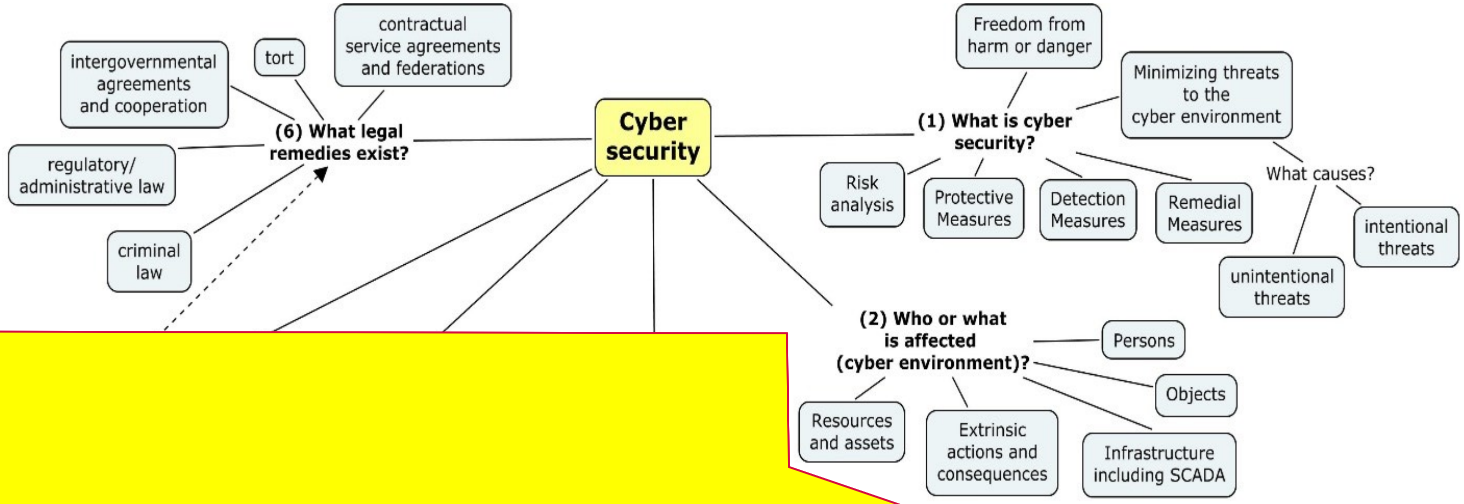
## Cooperation agreements:

- ISO SC27 (Liaison), ETSI (MoU), CEN CENELEC (Collaboration agreement)
- ETSI TISPAN on CIIP, ESI on eID, CLOUD on cloud certification, CEN CENELEC on smart grids, ISO SC 27 in the area of privacy

# Current landscape of standardisation

- Cybersecurity areas covered by standardization
  - Security feature provision
    - Provision of sector/technology specific security features.
  - Security assurance
    - Common Criteria (ISO 15408)
    - Ongoing work in 3GPP
  - Security threat sharing
    - Sharing of threat information, current attack patterns, software vulnerabilities
  - Organisational management for secure operations
    - ISO 27000 series
- Challenges from EU perspective
  - Lack of consistent strategy towards standards
  - Recognized shortcomings of the current approach
  - Need establishing a small number of key initiatives at EU level
  - Improve coordination between EU funded R&D and SDOs

# New context – NIS Directive



Cyber security

(1) What is cyber security?

Freedom from harm or danger

Minimizing threats to the cyber environment

What causes?

intentional threats

unintentional threats

Risk analysis

Protective Measures

Detection Measures

Remedial Measures

(2) Who or what is affected (cyber environment)?

Persons

Objects

Resources and assets

Extrinsic actions and consequences

Infrastructure including SCADA

(6) What legal remedies exist?

intergovernmental agreements and cooperation

tort

contractual service agreements and federations

regulatory/ administrative law

criminal law

Focus of the Directive

# Priorities for standardisation related to NIS Directive

- Close the gaps and simplify the standards for NIS that enable interoperability of event reporting and information sharing
  - Reach consensus on
    - Architectures, interfaces, and information exchange expressions
    - Standards and specifications
  - Develop a means for Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) to fit into the NIS Directive model and architecture
  - Develop means for Public Electronic Communication Networks or Publicly Available Electronic Communication Service Providers (under Framework Directive) and Trust Providers to fit into the NIS Directive model and architecture
  - Develop additional border gateway defence and threat exchange standards for one Essential Service (Digital Infrastructure Internet Exchange Points)
  - Develop a means for virtualised infrastructures and services to fit into the NIS Directive model and architecture

# Recommendations (2014)

- The Commission and the Member States should continue to encourage vendors to agree on the use of open standards and to encourage both private and public sector organisations to include references to these standards in procurement processes.
- Member States should consider including the subject of standardization in national cyber security strategies. Emphasis should be given to improving the coordination between policy and operational levels and enhancing the role of public private partnerships in the standardisation process.
- Member States should encourage National Regulatory Authorities to make greater use of open standards as point of reference in the process of enforcing regulations.

# Recommendations (2014)

- Public institutions involved in the funding of research and development should identify consistent sets of standards for different research areas. Where appropriate, publicly funded research should require compliance with these standards.

- Standards Development Organisations should work together to identify ways of speeding up the standards development process for cyber security related standards. This might be achieved by a ‘fast track’ mechanism.

- The Commission and the Member States should support the EU-wide certification scheme outlined in the new ENISA mandate proposal allowing end users to verify that services or products upon which they rely comply with security standards (2017).

# Trending Issues

- New trust models to ensure supply chain integrity
- Baseline requirements for IoT security and privacy, including mandatory reference levels for trusted IoT solutions and minimal requirements
- Adaptation of the framework for interoperability testing to new IoT requirements
- Future standards for scalability of security controls have to anticipate and meet the needs of different risk levels.
- Baseline security certification (“lightweight” certification) for ICT products
- Better coordination of work performed by ESOs

# Thank you!

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu