A strategy for a secure information society – Dialogue, partnership and empowerment - COM(2006) 251

Implementation progress

Gerard.Galler@ec.europa.eu

European Commission

DG Information Society & Media

Unit INFSO/A3: Internet; Network & Information Security

NISSG 18.1.2007

Challenges of the Information Society

TECHNICAL dimension

SOCIAL dimension

TRUSTWORTHY, SECURE & RELIABLE ICT

ECONOMIC dimension

LEGAL dimension

The challenges for stakeholders

- **Public Administrations**
  - to address the security of their own networks and **serve as** an **example of best practice** for other players

- **Private sector enterprises**
  - to **address NIS as an asset and an element of competitive advantage** an not as a “negative” cost

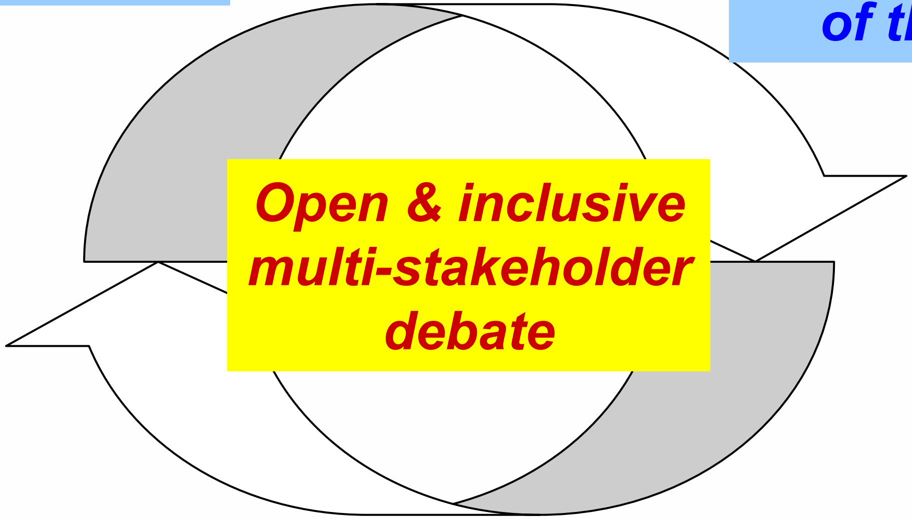
- **Individual users**
  - to understand that **their home systems are critical** for the overall “security chain”

European Commission
Information Society and Media

Strategy

DIALOGUE
structured and multi-stakeholder

PARTNERSHIP
greater awareness & better understanding of the challenges



Open & inclusive multi-stakeholder debate

EMPOWERMENT
commitment to responsibilities of all actors involved

A. Dialogue

- ***"Benchmarking"* national NIS-related policies**
  - Comparing to learn and to transfer **best practices to improve awareness** among SMEs & individual users to **strengthen their capability** to counter NIS risks
  - public administrations shall act **as 'intelligent' users & serve as an example for best practice** drivers (-> eID)

- **Structured multi-stakeholder dialogues**
  - where to **strike the balance** between security & protection of fundamental rights (PET, TCP)
  - develop a **sector-specific policy for the ICT** sector to enhance the security and the resilience of information and communication networks (CIIP)
  - **Business Summit** to stimulate industry **commitment** to implement a culture of security in industry (see C. Empowerment)
  - Seminar to raise security awareness & strengthen trust of end-users

B. Partnerships

- **Improve knowledge of the problem**
  - **ENISA** to develop a trusted partnership with Member States and stakeholders to create a **data collection framework** to collect EU-wide data on security incidents and consumer confidence

- **Establish strategic platform**
  - fostering a strategic relationship between governments, businesses and research community to deliver **data on trends in ICT security**

- **Support response capability**
  - ENISA to examine feasibility of a **European information sharing and alert system** (including a multi-lingual security portal)

C. Empowerment

- **Invite Member States to:**
  - Proactively participate in the proposed *benchmarking* exercise of national NIS policies;
  - Promote, in cooperation with ENISA, **awareness campaigns on the virtues, benefits and rewards of adopting effective security technologies**, practices and behaviour;
  - Leverage the roll-out of e-Gov services to **communicate and promote good security practices** that could then be extended to other sectors;
  - Stimulate the development of **network and information security programmes** as part of higher education curricula.

C. Empowerment (2)

- **Invite private sector stakeholders to take initiatives to:**
  - Develop an appropriate **definition of responsibilities for SW producers and ISPs** in relation to the provision of adequate and auditable security. Need for **standardised processes** meeting commonly agreed **security standards and best practice rules**.
  - Promote **diversity, openness, interoperability, usability and competition as key drivers for security.**
  - Stimulate actual **deployment** of security-enhancing products, processes and services.
  - **Disseminate good security practices** for network operators, service providers and SMEs**.**

European Commission
Information Society and Media

C. Empowerment (3)

- **Invite private sector stakeholders to take initiatives to:**
  - Promote **training programmes in the business sector**, in particular for SMEs, to provide employees with the knowledge and skills to implement security practices.
  - **Work towards affordable security certification schemes** for products, processes and services (in particular with respect to **privacy**).
  - Involve the **insurance sector** to develop **risk management tools and methods** for ICT-related risks. Foster a culture of risk management (in particular in SMEs).

Research: FP7–ICT: Secure, dependable & trusted infrastructures

- **Call 1** (opening 22.12.06, **closing 8.5.07**), Budget: 90 M€
  - Security and resilience in network **infrastructures**
    - Scalable, context-aware, secure & resilient architectures & technologies
    - Real-time detection and recovery against intrusions and failures
  - Security & trust in dynamic & reconfigurable **service** architectures
  - **Trusted computing** infrastructures
  - Security & dependability in the **engineering** of SW and service
  - **Identity** Management and **Privacy** enhancing tools
  - Coordination & Support Activities

- **Call 2 (2H2007):**
  - New paradigms and experimental facilities
  - Protection of **critical infrastructures** (joint call with FP7-Security)

- Information Day: 26.2.07, Brussels
- See http://cordis.europa.eu/ist/trust-security/index.htm

INFSO internal implementation roadmaps

1. Critical information infrastructures protection
2. International cooperation
3. R&D
4. Dialogues
    1. Benchmarking MS policies on awareness raising & trust strengthening - Seminar
    2. Dialogue on Trusted Computing
    3. Dialogue on PET
    4. Dialogue on eID
    5. Business event (commitment)
5. Partnerships
    1. ENISA: a. Data collection framework, b. Study on information sharing and alert system
    2. Data on ICT security market
6. Empowerment (STD, Certification, business, MS)
7. Report on implementation