enisa
European Network
and Information
Security Agency

A Strategy For ENISA

Steve Purser

Head of Technical Competence Department

Reasons For a New Strategy

- The current series of MTPs terminates in 2010.
- In parallel, a public consultation, organised by the Commission, invites all parties to provide their views of a future approach to NIS.
- In order to avoid a ‘gap’ in production, we needed to define a strategy now.
- This approach allows us to use 2010 as a transition year.

Our Vision

- Everybody is involved.
  - All actors understand the role they are expected to play and are sufficiently knowledgeable to perform this role.
- Actions performed by the different actors are mutually reinforcing.
  - This is the principle of defence in depth.
- The approach is sufficiently scalable and flexible to cope with rapidly evolving constraints.
  - Approaches that are too rigid and that cannot adapt to changes in the socio-economic environment will not survive.

The Challenges (I)

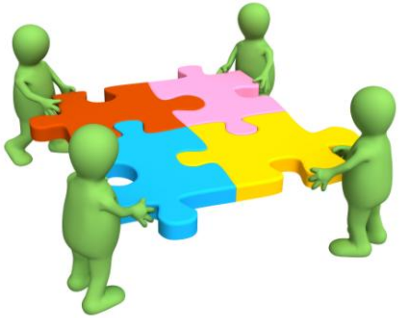
- Success requires going further than awareness – we must achieve active participation.
  - Active risk management must replace passive checklists.
  - The citizen should be comfortable with risk management in an electronic world – this is ‘electronic common sense’.
- The global approach must be economically viable.
  - Everyone should benefit from contributing - All actors must be able to achieve a sensible trade-off between opportunity and risk.

The Challenges (II)

- Methods and tools must reflect all the constraints.
  - It must be possible to achieve results with limited resources.
  - There is no “one size fits all”, a complete and coherent approach must offer solutions to organisations of all types and sizes.
- We must react quickly to change.
  - Established ideas must be regularly challenged.
  - New computing models, such as cloud computing, will require innovative approaches to security.

Coherence & Consistency

- The European approach to information security must be coherent across borders and consistent over time.
  - A coherent approach will ensure common minimal standards for protection and will prevent the development of a weakest link.
  - An approach that is consistent over time will allow progression to greater levels of maturity.
- This will require commitment to a strategic approach and coordination across Member States and communities.
  - It will be necessary to achieve a balance between the priorities of the individual actors and the priorities of the whole community.



The Role of ENISA (I)

- Collecting and analysing data at the European level.
- Making recommendations to the Commission and Member States on suitable policies and associated actions.
- Identifying and promoting best practices.
- Facilitating the flow of information related to information security between the different community actors.
- Bringing together actors from the public sector and private sector to resolve specific issues.
- Working together with Member States to ensure alignment and harmonisation of initiatives.

The Role of ENISA (II)

- ENISA assists Member States and the Commission in global issues that affect the European Community as a whole.
- This is an advisory role and the focus is on prevention and preparedness.
- ENISA does NOT have any operational responsibilities either within the EU institutional framework or with respect to Member States.

- ENISA has no special role in the security process protecting EU institutions.

The Priorities

- ENISA believes that the priorities for addressing the evolving challenges to information security at the EU level are:
  - The creation of a knowledgeable and proactive NIS community throughout Europe.
  - The development of secure infrastructure and services.
  - The establishment of a framework for managing identity, accountability and trust.
  - Ensuring an economically efficient approach to securing information systems.

The Proactive Community

- A European approach to security requires a strong level of commitment from all actors:
  - People need to be convinced of the need to act and capable of carrying out their role.
  - In order to effectively respond to the evolving threat environment, we need to be highly proactive.
- Many potential areas for development, including:
  - EU-wide campaigns targeting the citizen *as an end user*.
  - Improving our response to emerging risks.
  - Creative learning approaches, such as AI and serious games.

Secure Services

- Future services must benefit from true end-to-end security – including end user equipment.
  - We must move from secure infrastructure to secure services.
  - Modern information systems are highly complex and evolve rapidly – they are easy targets.
  - An architectural approach combining network security and end point security is needed to secure services end-to-end.
- Examples of how this may be achieved include:
  - Agreement on an architectural approach.
  - Tighter integration of security into the lifecycle.
  - Improved collection and analysis of data relating to security incidents.

Identity & Trust

- The notion of identity in global networks is evolving rapidly.
  - Core concepts are to some extent poorly defined.
  - Many of these concepts (e.g. Trust) could have a profound effect on the way in which services are secured in the future.
  - There is considerable scope for abuse and/or inappropriate use of personal information.
- Examples of activities include:
  - Facilitating knowledge transfer between the research community and those deploying infrastructure.
  - Fostering the use of privacy-enhancing technologies.
  - Development of guidelines for legislation.

Economic Efficiency (I)

- In order to achieve optimal results, Member States must be capable of balancing opportunities with risks.
  - Regulatory requirements should be aligned with business needs.
  - National policies should take account of the needs of companies and institutions of different types and sizes.
- Security approaches should be sufficiently robust to survive changes in the socio-economic environment, e.g. mergers & acquisitions.
- Best practices should reflect economic reality.

Economic Efficiency (II)

- Ways in which this challenge may be met include:
  - Studying the impact of national policies and recommending changes.
  - Identifying security practices that are sufficiently robust to survive major socio-economic changes.
  - Promoting risk management as an economic tool.
  - Promoting secure software development.

Thank You For Your Attention!

Questions?