Culture of cybersecurity: from policies to practice

ITU Regional Cybersecurity Forum for Europe and CIS

Sofia, Bulgaria
07-09 October 2008

Professor Solange Ghernaouti-Hélie - University of Lausanne
Cybersecurity for information economy

- **Cybersecurity culture** deals with key economic, legal, and social issues related to information security
  - in order to contribute to helping countries get prepared
    - to face issues and challenges linked to information and communication technologies (ICT) deployment, uses and misuses
A large range of issues ...

- At the crossroads of technological, legal, sociological, economic, and political fields
  - Cybersecurity is an interdisciplinary domain by nature

- Depending on the country
  - it must reflect the vision, the culture and the civilization of a nation
  - as well as meeting the specific security needs of the local context in which it is introduced
A large range of issues ...

- Educational efforts and investments need to be made to educate and train all the members of the information society
  - from decision makers to citizens
  - including children and older people

- Specific actions should be taken at a national level
  - to raise or build cybersecurity capacities of various members
  - in order to be able to deal with national and international cybersecurity issues
Awareness is not enough

- Awareness is not enough
  - to empower the end-user in a way that he or she would be able to adopt a safe and responsible behaviour when dealing with ICT technologies

- Specific educational programmes should be effective and available
  - for each kind of stakeholder
    - policy makers, justice and police professionals, managers, information technology professionals, end-users
## Building blocks

### Cybersecurity culture

<table>
<thead>
<tr>
<th>Training</th>
<th>Policy makers</th>
<th>Justice Police Professionals</th>
<th>Managers</th>
<th>ICT professionals</th>
<th>Acceptable practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>End-users</td>
</tr>
</tbody>
</table>

### Effective cooperation
Answering a global challenge by a local answer

- Any global strategy to develop a cybersecurity culture
  - has to be adapted to local needs

- When developing cybersecurity culture, one of the main challenges is to identify correctly what are
  - the global & international issues
  - the local specific needs for a cybersecurity culture
Strategic answer and political will

- Promoting a culture of cybersecurity that will touch the entire population needs to rely upon
  - an appropriate political vision and will
  - and efficient private and public partnerships
- There are no real theories or methodologies related to:
  - How to design, to communicate, to validate or to control the adequacy of a cybersecurity culture

  - Evaluating the effectiveness of cybersecurity culture, from policies and guidelines to practice, is very difficult
A need for private and public partnerships

- If the public and private sectors do not support such initiatives together as soon as possible
  - there will be a long term negative effect on economic development and the ability to ensure the security of goods and people
A question of responsibility

○ “Awareness: Participants should be aware of the need for securing information systems and networks and what can be done to enhance security”

○ “Responsibility: All participants are responsible for the security of information systems and networks”

● It will also contribute to avoiding building security based on fear
  ● Fear is a selling argument when dealing with security issues but is not always rational and does not lead to the best investments and efficiency in security
Basic recommendations

- **Educate** the end-user

- **Increase** public awareness to enhance users’ behaviour in respect of security

- **Give** to the end-user the tools and means required to be responsible

- **Design** an end-user-centric security model within a given technical and legal framework whereby the user can decide what is judicious based on his own resources
Defense in deep

- Education contributes to developing a layer of defence in deep security approach and is the cornerstone of the information society.

- Education constitutes a real human capacity challenge that governments have to face.
Human capacity building

- Capacity building includes
  - **Human resource development**
    - The process of equipping individuals with the understanding, skills and access to information, knowledge and training that enable them to perform effectively

- Every citizen should:
  - **Understand** the cyberthreats for the end-user
    - viruses, spam, identity theft, fraud, swindle, privacy offence, …
    - and their impacts
  - **Understand** how to adopt a security behaviour for a safe use of ICT resources
  - **Be able to** promote a cybersecurity culture based on well recognized good practices;
Concluding words …

- With the **Global Cybersecurity Agenda**, ITU proposes a unique framework to consider cybersecurity issues in a holistic and systemic approach,
  - a unique model to deal with the global challenges of building confidence and security into the use of ICT that takes into consideration awareness and education issues
Concluding words

- Promoting a culture of cybersecurity
  - contributes to building a safe and inclusive information society

- Considering cybersecurity education is a long term approach which is efficient for a sustainable information society
Thank you for your attention