Promoting a Culture of Cybersecurity

ITU West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP

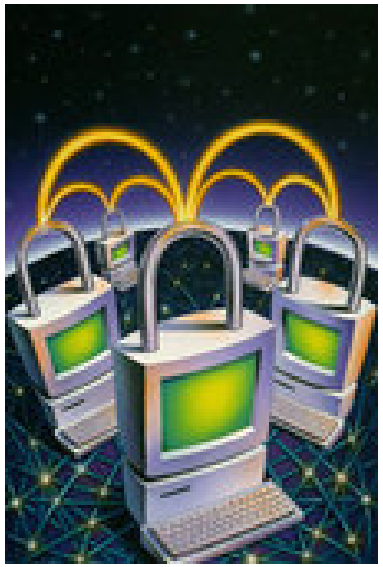
27-29 November 2007

Christine Sund
<christine.sund(at)itu.int>

ICT Applications and Cybersecurity Division
Telecommunication Development Sector (ITU-D)
International Telecommunication Union

Introduction to Promoting a Culture of Cybersecurity

- Societies are increasingly dependent on information and communication networks that span the globe
- Continuing changes in the use of ICT, systems networks, and the entire IT environment:
  - Increasingly powerful PCs
  - Converging technologies
  - Widespread use of the Internet have replaced what were modest, stand-alone systems in predominantly closed networks
  - Change in the way information is exchanged
  - Increasing interconnectivity
- The need for a national comprehensive action plan that addresses technical, legal and policy issues, combined with regional and international cooperation is growing



Nature and Scope of Cybersecurity Around the World

Countries see cybersecurity as:

- a technical, network or information technology issue, or
- a developmental issue because ICT services need secure and reliable networks, or
- an economic issue relating to maintaining business continuity or economic advantage, or
- a law and enforcement issue to deal with cybercrime and criminalizing the misuse of ICTs, or
- a national security issue relating to critical information infrastructure protection (CIIP).

Any international road map for cybersecurity must address all these different national perspectives.

All stakeholder groups have a role to play in promoting a global **culture of cybersecurity**.

UN Resolutions (57/239 & 58/199) Related to a "Culture of Security"

- **UN Resolution 57/239** (2002) on the "Creation of a global culture of cybersecurity"
- Identifies nine elements for creating a global culture of cybersecurity:

a) Awareness
b) Responsibility
c) Response
d) Ethics
e) Democracy
f) Risk Assessment
g) Security Design and Implementation
h) Security Management
i) Reassessment

- **UN Resolution 58/199** (2004) further emphasized "promotion of a global culture of cybersecurity and protection of critical information infrastructures"
  - Recognizes the growing importance of information technologies for the promotion of socio-economic development and the provision of essential goods and services
  - Notes the increasing links among most countries' critical infrastructures and that these are exposed to a growing number and a wider variety of threats and vulnerabilities that raise new security concerns

UN Resolution (57/239)
Elements for Creating a Culture of Security

a) Awareness: Participants should be aware of the need for security of information systems and networks and what they can do to enhance security;

b) Responsibility: Participants are responsible for the security of information systems and networks in a manner appropriate to their individual roles. They should review their own policies, practices, measures and procedures regularly, and should assess whether they are appropriate to their environment;

c) Response: Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective cooperation to prevent, detect and respond to security incidents. This may involve cross-border information-sharing and cooperation;

d) Ethics: Given the pervasiveness of information systems and networks in modern societies, participants need to respect the legitimate interests of others and recognize that their action or inaction may harm others;

UN Resolution (57/239)
Elements for Creating a Culture of Security

e) Democracy: Security should be implemented in a manner consistent with the values recognized by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency;

f) Risk Assessment: All participants should conduct periodic risk assessments that identify threats and vulnerabilities; are sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications; allow determination of the acceptable level of risk; and assist in the selection of appropriate controls to manage the risk of potential harm to information systems and networks in the light of the nature and importance of the information to be protected;

g) Security Design and Implementation: Participants should incorporate security as an essential element in the planning and design, operation and use of information systems and networks;

UN Resolution (57/239)
Elements for Creating a Culture of Security

h) Security Management: Participants should adopt a comprehensive approach to security management based on risk assessment that is dynamic, encompassing all levels of participants' activities and all aspects of their operations;

i) Reassessment: Participants should review and reassess the security of information systems and networks and should make appropriate modifications to security policies, practices, measures and procedures that include addressing new and changing threats and vulnerabilities.

UN Resolutions (57/239 & 58/199) Related to a "Culture of Security"

- **UN Resolution 57/239** (2002) on the "Creation of a global culture of cybersecurity"
- Identifies nine elements for creating a global culture of cybersecurity:
  - Awareness
  - Responsibility
  - Response
  - Ethics
  - Democracy
  - Risk Assessment
  - Security design and implementation
  - Security management
  - Reassessment
- **UN Resolution 58/199** (2004) further emphasized "promotion of a global culture of cybersecurity and protection of critical information infrastructures"
  - Recognizes the growing importance of information technologies for the promotion of socio-economic development and the provision of essential goods and services
  - Notes the increasing links among most countries' critical infrastructures and that these are exposed to a growing number and a wider variety of threats and vulnerabilities that raise new security concerns

The Role of Government

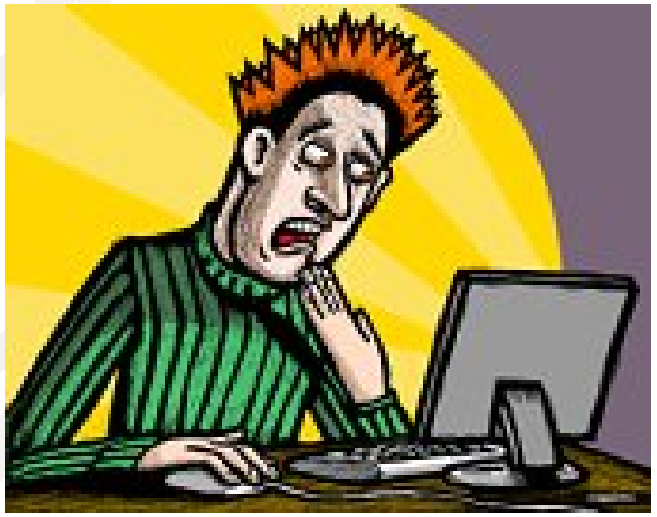
- Governments are responsible for ensuring that their citizens are protected
  - Protecting a country includes protecting its ICT infrastructures
- Governments have the central task of coordinating and implementing a national cybersecurity strategy
  - Ensuring that the national policy is flexible and adaptive
  - Coordinating responsibilities across authorities and government departments
- Governments are responsible for creating new (or adapting existing) legislation to criminalize the misuse of ICT, to curb abuses and to protect consumer rights
- Governments to **lead** national, regional, international cooperation activities
  - To protect national infrastructures effectively, national strategies must be matched with an international approach
  - Frameworks for cooperation that expand across national jurisdictions, with the sharing of skills, knowledge, and experience, are essential

The Role of the Private Sector and Industry

- As the owners and operators of most of the ICT and critical infrastructures, private sector entities have a central role to play in cybersecurity
- Private sector technical expertise and involvement are paramount in the development and implementation of national cybersecurity strategies
- Early warning and rapid response are key to protecting business assets, and in many countries, the private sector is typically the first to assess technological changes and threats
- Private sector participation in building a culture of security through involvement in relevant technical security forums or standards-development organizations is key

The Role of Individuals, Civil Society and Academia

- Cybersecurity is at its core a shared responsibility
- Governments and businesses must help people obtain information on how to protect themselves — and thus the community at large
- With the right tools readily accessible, each participant in the Information Society is also responsible for being alert and protecting themselves



Key Drivers for a Culture of Security in Some Countries

- Two main drivers which support the development of a culture of security at the national level:
  - Implementation of e-Government applications and services
  - Protection of national critical information infrastructures (CII)
- Privacy as an indirect driver for the development of a culture of security

Source: OECD 2005 Survey on Practical Initiatives to Promote a Culture of Security

Commonalities in Cybersecurity Approaches Taken by Countries

- In developing and implementing national policies for a culture of security, governments have been seen to adopt:
  - A multi-disciplinary and multi-stakeholder approach
  - A high-level governance structure
- International cooperation for fostering a culture of security
  - It is important that countries are involved in international networks and cooperation activities in the different areas essential for cybersecurity (legislation, enforcement, watch, warning and incident response, standards development, etc.)

Source: OECD 2005 Survey on Practical Initiatives to Promote a Culture of Security

Focus Areas in OECD Countries

Areas of high attention:

- Combating cybercrime
- Creating National CERTs/CSIRTs (Computer Emergency Response Teams/Computer Security Incident Response Teams)
- Engaging in cyber-security awareness raising activities
- Fostering education

Areas with less attention:

- Research and development
- Evaluation and assessment
- Outreach to small and medium sized enterprises (SMEs)

Source: OECD 2005 Survey on Practical Initiatives to Promote a Culture of Security

Links and Material

- Information on activities undertaken by ITU in the area of cybersecurity can be found at: www.itu.int/cybersecurity/
- ITU Cybersecurity Gateway (an easy-to-use information portal on national and international initiatives worldwide) can be found at: www.itu.int/cybersecurity/gateway/
- Information on ITU Global Cybersecurity Agenda (GCA) can be found at: www.itu.int/gca/
- ITU Development Sector (ITU-D) resources and activities related to cybersecurity can be found at: www.itu.int/itu-d/cyb/cybersecurity/
- The ICT Security Standards Roadmap produced by the ITU Standardization Sector (ITU-T) is accessible at: www.itu.int/ITU-T/studygroups/com17/ict/
- ITU Plenipotentiary Resolution 130: "Strengthening the role of ITU in building confidence and security in the use of information and communication technologies" (Antalya, 2006), can be found at: www.itu.int/osg/spu/cybersecurity/pgc/2007/docs/security-related-extracts-pp-06.pdf

Thank You for Your Attention!

For additional information do not hesitate to contact me at: christine.sund(at)itu.int

International Telecommunication Union

Helping the World Communicate