MOD

QUESTION 3/2

Securing information and communication networks: Best practices for developing a culture of cybersecurity

1 Statement of the situation or problem

The use of telecommunications and information and communication technologies (ICTs) has been invaluable in fostering development and social and economic growth globally. However, despite all the benefits and uses these technologies offer, there are risks and threats to security.

From personal finances to business operations, from national critical infrastructure and essential services to private ones, all transactions are increasingly managed through information and communication networks, making them more vulnerable to some form of attack.

In order to build trust in the use and application of telecommunications/ICTs for applications and content of all kinds, especially those having a major positive impact in economic and social areas where all players exert an effect on the protection of personal data, network security and the actual network user, close collaboration is required between national authorities, foreign authorities, industry, academia and users.

Based on the foregoing, securing information and communication networks and developing a culture of cybersecurity have become key in today's world for a number of reasons, including:

a) the explosive growth in the deployment and use of ICTs;

b) cybersecurity remains a matter of concern of all, and there is thus a need to assist countries, in particular developing countries[1], to protect their telecommunication/ICT networks against cyberattacks and threats;

c) the need to endeavour to ensure the security of these globally interconnected infrastructures if the potential of the information society is to be achieved;

d) the growing recognition, at the national, regional and international levels, of the need to develop and promote best practices, standards, technical guidelines and procedures to reduce vulnerabilities of and threats to ICT networks;

e) the need for national action and regional and international cooperation to build a global culture of cybersecurity that includes national coordination, appropriate national legal infrastructures, watch, warning and recovery capabilities, public-private partnerships and outreach to civil society and consumers;

f) the requirement for a multistakeholder approach to effectively make use of the variety of tools available to build confidence in the use of ICT networks;

g) United Nations General Assembly (UNGA) Resolution 57/239, on creation of a global culture of cybersecurity, invites Member States "to develop throughout their societies a culture of cybersecurity in the application and use of information technology";

---

[1] These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition.

h) UNGA Resolutions 68/167, 69/166 and 71/199, on the right to privacy in the digital age, affirm, *inter alia*, "that the same rights that people have offline must also be protected online, including the right to privacy";

i) best practices in cybersecurity must protect and respect the rights of privacy and freedom of expression as set forth in the relevant parts of the Universal Declaration of Human Rights, the Geneva Declaration of Principles adopted by the World Summit on the Information Society (WSIS) and other relevant international human rights instruments;

j) the WSIS Geneva Declaration of Principles indicates that "A global culture of cybersecurity needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies", the Geneva Plan of Action encourages sharing best practices and taking appropriate action on spam at national and international levels, and the Tunis Agenda for the Information Society reaffirms the necessity for a global culture of cybersecurity, particularly under Action Line C5 (Building confidence and security in the use of ICTs);

k) ITU was requested by WSIS (Tunis, 2005), in its agenda for implementation and follow-up, to be the lead facilitator/moderator for Action Line C5 (Building confidence and security in the use of ICTs), and relevant resolutions have been adopted by the Plenipotentiary Conference, the World Telecommunication Standardization Assembly (WTSA) and the World Telecommunication Development Conference (WTDC);

l) UNGA Resolution 70/125 adopted the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the WSIS outcomes;

m) the WSIS+10 statement on the implementation of WSIS outcomes, and the WSIS+10 vision for WSIS beyond 2015, adopted at the ITU-coordinated WSIS+10 high-level event (Geneva, 2014) and endorsed by the Plenipotentiary Conference (Busan, 2014), which were submitted as an input into the UNGA's overall review on the implementation of WSIS outcomes;

n) WTDC Resolution 45 (Rev. Baku, 2025) supports the enhancement of cybersecurity among interested Member States;

o) Resolution 130 (Rev. Bucharest, 2022) of the Plenipotentiary Conference resolves to continue promoting common understanding among governments and other stakeholders of building confidence and security in the use of ICTs at the national, regional and international level;

p) WTSA Resolution 50 (Rev. New Delhi, 2024) highlights the need to harden and defend information and telecommunication systems from cyberthreats and cyberattacks, and continue to promote cooperation among appropriate international and regional organizations in order to enhance exchange of technical information in the field of information and telecommunication network security;

q) there have been various efforts to facilitate the improvement of network security, including the work of Member States and Sector Members in standards-setting activities in the ITU Telecommunication Standardization Sector (ITU-T) and in the development of best-practice reports in ITU-D; by the ITU secretariat in the Global Cybersecurity Agenda (GCA); and by ITU-D in its capacity-building activities under the relevant programme; and, in certain cases, by experts across the globe;

r) governments, service providers and end users, particularly in least developed countries (LDCs), face unique challenges in developing security policies and approaches appropriate to their circumstances;

s) reports detailing the various resources, strategies and tools available to build confidence in the use of ICT networks and the role of international cooperation in this regard are beneficial for all stakeholders;

t) cybersecurity issues including spam and malware continue to be a serious concern, although evolving and emerging threats must also be studied; and

u) the need for simplified test procedures at basic level for security testing of telecommunication networks to promote a security culture.

2 Questions or issues for study

Discuss approaches and share experiences on how to promote cybersecurity and cyber resilience for the telecommunications/ICTs sector, including:

a) Cybersecurity public policies and regulations that apply to the telecommunications/ICT sector, including obligations, measures, and assurance practices.

b) Specific measures, initiatives and projects to improve the cybersecurity and cyber resilience of small and medium telecommunications service providers.

c) How ITU Membership is addressing the cybersecurity challenges and opportunities of the new and emerging telecommunications/ICT technologies and services in the sector, such as Artificial Intelligence applications.

3 Expected output

a) Three output reports to the membership on the issues identified in § 2 above that will be delivered during the cycle in a staggered manner, and guidelines developed based on those reports.

b) Holding ad hoc sessions, seminars and workshops, including invited experts from outside ITU membership to share knowledge, information and best practices concerning the topics identified as issues for study in item 2. These activities are to be collocated as far as possible with meetings of ITU-D Study Group 2 or of the rapporteur group for the Question.

4 Timing

This study is proposed to last four years, with output reports to be delivered 12, 24 and 36 months.

5 Proposers/sponsors

ITU-D Study Group 2, APT, ATU, CEPT and CITEL.

6 Sources of input

1) Member States and Sector Members

2) Relevant ITU-T and ITU-R study group work

3) Relevant outputs of international and regional organizations

4) Relevant non-governmental organizations concerned with the promotion of cybersecurity and a culture of security

5) Surveys, online resources

6) Experts in the field of cybersecurity

7) Global Cybersecurity Index (GCI)

8) Other sources, as appropriate

7 Target audience

Target audience	Developed countries	Developing countries
Telecom policy-makers	Yes	Yes
Telecom regulators	Yes	Yes
Service providers/operators	Yes	Yes
Manufacturers	Yes	Yes
Academia	Yes	Yes

a) Target audience

National policy-makers and Sector Members, and other stakeholders involved in or responsible for telecommunication/ICT cybersecurity activities, especially those from developing counties.

b) Proposed methods for implementation of the results

The study programme focuses on gathering information and best practices. It is intended to be informative in nature and can be used to raise awareness of cybersecurity issues in Member States and Sector Members and to draw attention to the information, tools and best practices available, the results of which may be used in conjunction with BDT-organized ad hoc sessions, seminars and workshops.

8 Proposed methods of handling the Question or issue

The Question will be addressed within a study group over a four-year study period and will be managed by a rapporteur and vice-rapporteurs. This will enable Member States and Sector Members to contribute their experiences and lessons learned with respect to cybersecurity.

9 Coordination and collaboration

Relevant study Questions under both ITU-D Study Groups 1 and 2. as well as ITU-T, in particular ITU-T Study Group 17, which is responsible for developing international standards to enhance confidence, security, and trust in the use of telecommunications/ICTs.

Coordination with other relevant organizations and agencies. Given the existing level of technical expertise on the issue in these groups, they should be given the opportunity to comment and provide input documents as appropriate.

10 BDT programme link

The BDT programme under the ITU-D priority ''Inclusive and secure telecommunications/ICTs for sustainable development'' shall facilitate exchange of information and make use of the output, as appropriate, to satisfy programme goals and the needs of Member States.

11 Other relevant information

As may become apparent within the life of the Question.