|  |  |  |
| --- | --- | --- |
| C:\Users\ponder\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\BDT-25th_anniversary_2017-Logo_411959-3_transparent.png | **World Telecommunication DevelopmentConference 2017 (WTDC-17)****Buenos Aires, Argentina, 9-20 October 2017** | C:\Users\ponder\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\BDT-25th_anniversary_2017-Logo_411959-1_transparent.png |
|  |  |
| PLENARY MEETING | **Document WTDC-17/36-E** |
|  | **8 September 2017** |
|  | **Original: Spanish** |
| Brazil (Federative Republic of)/Mexico |
| proposals for the work of the conference |
|  |
|  |
| **Priority area:**Study group Questions**Summary:**Modification to ITU-D Study Question 3/2 – Securing information and communication networks: Best practices for developing a culture of cybersecurity**Expected results:**Brazil and Mexico invite all delegations at WTDC-17 to consider this document when discussing the revision of Study Question 3/2, addressing both its substance and its wording.**References:**Question 3/2 |

STUDY GROUP 2

**MOD** B/MEX/36/1

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 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, national infrastructure, public and private services, all are increasingly managed through some information and communication network, 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 with a major positive impact in economic and social areas brought about by all players exercising an effect on privacy, 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 information and communication technology (ICT);

b) cybersecurity remains a concern of all and there is thus a need to assist countries, in particular developing countries, 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 need for national, regional and international action along with a multistakeholder approach to build a global culture of cybersecurity that includes national coordination, appropriate national legal infrastructures, watch, warning and recovery capabilities, government/industry partnerships, and outreach to civil society and consumers;

e) 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";

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

g) 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;

h) the 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);

i) ITU was requested by WSIS (Tunis, 2005), in its agenda for the implementation and follow-up, to be the lead facilitator/moderator for Action Line C5 (Building confidence and security in the use of ICTs);

j) UNGA Resolution 70/125, the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society, states that building confidence and security in the use of information and communications technologies should be a priority, especially given growing challenges, including the abuse of such technologies for harmful activities from harassment to crime to terrorism, and should be consistent with human rights;

k) according to the WSIS+10 Statement on the Implementation of WSIS Outcomes, governments and all relevant stakeholders are aware of the need for greater collaboration to address the problems of confidence, security, privacy and personal data protection, safety and trust in the use of ICTs;

l) WTDC Resolution 45 (Rev. Dubai, 2014) supported the enhancement of cybersecurity among interested Member States;

m) Resolution 130 (Rev. Busan, 2014 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;

n) Resolution 50 (Rev. Hammamet, 2016) of the World Telecommunication Standardization Assembly (WTSA) 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;

o) the conclusions and recommendations in ITU-D Study Group 2's final report on Question 3/2, to consider in the next study a study cycle on evolving and emerging threats beyond spam and malware;

p) there have been various efforts to facilitate the improvement of network security, such as 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 in the relevant programme; and, in certain cases, by experts across the globe;

q) 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;

r) spam continues to be a serious concern, although evolving and emerging threats must be studied;

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

# 2 Question or issues for study

a) Foster the integrity of ICT systems, this being essential for their ongoing development;

b) discuss approaches and best practices for evaluating the impact of spam within a network, as well as evolving and emerging threats, and provide the necessary measures and guidelines, including mitigation techniques, legislation and regulatory measures that developing countries can use, taking into account existing standards and available tools;

c) provide information on current cybersecurity challenges that service providers, regulatory agencies and other relevant parties are facing;

d) continue to gather national experiences from Member States relating to cybersecurity, privacy and child online protection and to identify and examine common themes within those experiences, using that information to devise guidelines enabling Member States to develop effective mechanisms for security and privacy in the digital environment;

e) analyse the cyberthreat challenges facing IoT, artificial intelligence and other emerging technologies, and measures to address those challenges;

f) discuss perspectives and best practices regarding the protection of privacy and personal data;

g) promote awareness-raising and capacity-building for users regarding the protection of data, privacy and cybersecurity;

h) provide a compendium of relevant, ongoing cybersecurity activities being conducted by Member States, organizations, the private sector and civil society at the national, regional and international levels, in which developing countries and all sectors may participate, including information gathered under c) above;

i) examine specific needs of persons with disabilities, in coordination with other relevant Questions;

j) examine ways and means to assist developing countries, with the focus on LDCs, in regard to cybersecurity-related challenges;

k) foster cooperation between the players involved with a view to holding ad hoc sessions, seminars and workshops to share knowledge, information and best practices concerning effective, efficient and useful measures and activities to enhance cybersecurity, increase confidence and protect data and network integrity, taking into consideration existing and potential risks for ICTs, using outcomes of the study, to be collocated as far as possible with meetings of Study Group 1 or of the rapporteur group for the Question;

l) work in collaboration with the relevant ITU‑T study groups and other standards-developing organizations (SDOs), as appropriate, and taking into account available information and material in these entities;

m) develop guidelines to facilitate the establishment of measures at national, regional and international level to combat spam;

n) gather national experience on regulation and/or policies implemented by telecommunication regulatory authorities to foster confidence and security in the use of telecommunications/ICTs.

# 3 Expected output

1 Reports to the membership on the issues identified in § 2 a) to n) above. The reports in question will reflect that secure information and communication networks are integral to building of the information society and to the economic and social development of all nations. Cybersecurity challenges include potential unauthorized access to, destruction of and modification of information transmitted on ICT networks, as well as countering and combating spam. However, the consequences of such challenges can be mitigated by increasing awareness of cybersecurity issues, establishing effective public-private partnerships and sharing successful best practices employed by policy-makers and businesses, and through collaborating with other stakeholders.

 In addition, a culture of cybersecurity can promote trust and confidence in these networks, stimulate secure usage, ensure protection of data and privacy while enhancing access and trade, and enable nations to better achieve the economic and social development benefits of the information society.

2 Educational materials for use in workshops, seminars, etc.

3 Accumulation of knowledge, information and best practices on effective, efficient and useful measures and activities to enhance cybersecurity in developing countries resulting from ad hoc sessions, seminars and workshops.

4 Recommendations to make it easier for members to establish relevant ways to increase confidence and security in the use of ICTs.

# 4 Timing

This study is proposed to last four years, with preliminary status reports to be delivered on progress made after 12, 24 and 36 months.

# 5 Proposers/sponsors

ITU‑D Study Group 1; Arab States; Inter-American proposal; Japan; Islamic Republic of Iran.

# 6 Sources of input

a) Member States and Sector Members

b) Relevant ITU‑T and ITU‑R study group work

c) Relevant outputs of international and regional organizations

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

e) Surveys, online resources

f) Experts in the field of cybersecurity

g) Global Cybersecurity Index (GSI)

h) Other sources, as appropriate.

# 7 Target audience

| Target audience | Developed countries | Developing countries[[1]](#footnote-1)1 |
| --- | --- | --- |
| 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 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 for Member States and Sector Members of the issues of cybersecurity 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 (with submission of interim results), 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

Coordination is required with ITU‑T, on security, in particular Study Group 17 which is responsible for building confidence and security in the use of information and communication technologies, as well as other relevant organizations, including FIRST, IMPACT, APCERT, OAS CICTE, OECD, APEC, RIRs, NGOs, M3AAWG, UCENET and others. Given the existing level of technical expertise on the issue in these groups, all documents (questionnaires, interim reports, draft final reports, etc.) should be sent to Study Group 17 for comment and input prior to being submitted to the full ITU‑D study group for comment and approval.

# 10 BDT programme link

The BDT programme under Output 3.1 of Objective 3 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

–

\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. 1 These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition. [↑](#footnote-ref-1)