|  |  |  |
| --- | --- | --- |
| INTERNATIONAL TELECOMMUNICATION UNION **TELECOMMUNICATION STANDARDIZATION SECTOR**  STUDY PERIOD 2009-2012 | | **Joint Coordination Activity on Accessibility and human Factors (JCA-AHF)** |
|  | | **Doc. 134** |
| **English only**  **Original: English** |
| **Source:** | JCA-AHF Convener | |
| **Title:** | Report of the Rapporteur Group meeting on Question 22-1/1  (report submitted by the Rapporteur for Question 22-1/1, Second Meeting of ITU-D Study Group 1 Geneva, 5-9 September 2011) | |

This document is submitted for information.

|  |  |  |
| --- | --- | --- |
| Telecommunication Development Sector  Study Groups | |  |
| Second Meeting of ITU-D Study Group 1 | |  |
| Geneva, 5-9 September 2011 | |  |
|  | |  |
|  | | Document 1/REP/17(Rev.1)-E |
| 25 September 2011 |
| Original: English |
|  | | For action |
| Question 22-1/1: Securing information and communication networks: best practices for developing a culture of Cybersecurity | | |
| SOURCE | Rapporteur for Question 22-1/1 | |
| TITLE | Report of the Rapporteur Group meeting on Question 22-1/1  (Geneva, 8 September 2011) | |
|  | | |

1. Adoption of the agenda

The agenda [1/OJ/18 (Rev.1)](http://www.itu.int/md/D10-SG01-OJ-0018/en) was adopted with minor modifications.

1. Review of the main conclusions of the previous meeting

Document [1/58](http://www.itu.int/md/D10-SG01-C-0058/) was presented by Mr James Ennis (United States), Rapporteur for Question 22-1/1. It contains a summary of the discussions and decisions made during the previous Rapporteur Group meeting, and the work to be conducted for the study period. The meeting accepted the report.

1. Study of relevant input documents, including Liaison Statements (if any)

In numerical order, the following documents were presented.

Document [1/69](http://www.itu.int/md/D10-SG01-C-0069/en) presented by Mali introduced an overview of cybercrime targeting persons with disabilities. The contribution shows how the access and constant evolution of new information technologies are improving our lives, but also are exposing vulnerable people such as children, persons with disabilities, senior citizens and women to be victims of cybercrime. To reduce the negative effect of the misuse of ICTs, Mali proposes several measures such as legislation, training, agencies, sub-regional integration and cybersecurity technologies. Action: This document provides a basis for a joint contribution to the next meeting which will examine in more detail the special cybersecurity issues facing persons with disabilities. A number of countries agreed to participate in the development of such a contribution.

Document [1/75](http://www.itu.int/md/D10-SG01-C-0075/en) submitted by Viable France (France), provided an overview on how cybercrime is targeting persons with disabilities and other vulnerable persons. In particular the contribution highlighted the measures adopted by the European Union though the European Commission, and UNAPEI, a French association for persons with disabilities. These measures (legislation, training, agencies, sub-regional integration and Cybersecurity technologies) have to be made to make cybercriminals “visible” in order to dissuade them and fight cyberthreats. Action: This document provides a basis for a joint contribution to the next meeting which will examine in more detail the special cybersecurity issues facing children with disabilities. A number of countries agreed to participate in the development of such a contribution.

Document [1/93](http://www.itu.int/md/D10-SG01-C-0093/en) was presented by Brazil and it described the Tentacles Project as a new way to combat cybercrimes. Created by the Brazilian Federal Police Department, the project aims to combat bank frauds, through a radical change of investigation methods and routines: rapid exchange of bank fraud information, with the substitution of physical media (paper) by electronic means, as well as the development of a national bank fraud database and cross-checking data received gathered through the use of modern tools of analysis and police intelligence. Early results have shown that the chosen path is the correct one and that the implementation of projects of Structure and Training will lead to the eventual achievement of all the desired objectives and goals. Action: For inclusion in the compendium.

Document [1/100 + Annex](http://www.itu.int/md/D10-SG01-C-0100/en), presented by the USA, contains Best Practices of Cybersecurity: Public-Private Partnerships. It proposes principles of sound public-private partnerships, their role in security risk management, a framework for building successful partnerships and examples of the action of public-private partnerships. These partnerships are also helpful to promote greater security awareness and facilitate the exchange of technical expertise. The United States has built a public-private partnership model that provides a solid foundation for its national critical information infrastructure security program. The contribution shows how public-private partnerships are expanded beyond national borders and geographic boundaries, strategic and operational outcomes relationships will strengthen national-level security capabilities. Action: For consideration and approval at the next meeting as text for the final report. The question was raised as to whether this material could be translated into French for non-English speaking readers. The BDT said that some of it could be translated.

Document [1/101 + Annex](http://www.itu.int/md/D10-SG01-C-0101/en), anticipating the United States’s contribution to the Spring 2012 to the Rapporteur Group meeting on Questions 22-1/1, proposes and outline of a training course which covers two aspects of CSIRTs: Building a National Computer Security Incident Management Capability and Managing a National Computer Security Incident Response Team with Critical Success Factors. Action: Noted.

Document [1/107](http://www.itu.int/md/D10-SG01-C-0107/en) submitted by the People's Republic of China introduced an international practice (advantages, challenges and problems) in the area of mobile phone Real Name Registration (RNR) and how China is ready to enforce the rule in two steps: the first one, started in September 2010, requested all mobile operators to adopt new contracts with consumers. In this contract new subscribers are asked to voluntarily provide the necessary real name information to complete registration procedure. The second stage is beginning from new RNR regulations taking effect, which is planned for existing non-real name users to take 3 years to accomplish supplement registration. Action: For inclusion in the compendium.

Document [1/113 + Annex](http://www.itu.int/md/D10-SG01-C-0113/en), introduced by Morocco, contains the revised version of the contribution on a “National Cybersecurity Management System: Framework – Maturity Model – Responsibilities and Implementation Guide” as a National Roadmap for Global Cybersecurity for discussion in Question 22-1/1. This document superceded documents [1/114 + Annex](http://www.itu.int/md/D10-SG01-C-0114/en) and [1/102](http://www.itu.int/md/D10-SG01-C-0102/en) which made it unnecessary to present these documents. Action: For consideration and approval at the next meeting as text for the final report.

Document [1/116 + Annex](http://www.itu.int/md/D10-SG01-C-0116/en), an overview on Cloud Computing and Security High Level, was introduced by AT&T, United States. As an outcome of the previous meeting in May on Question 22-1/2, AT&T had been asked by the Rapporteur, considering the participant’s interest in the subject, to provide a deeper presentation with additional details on cloud security. There were many questions. Action: it was suggested that Q22-1/1 should consider developing best practices regarding cloud security.

Document [1/119 + Annex](http://www.itu.int/md/D10-SG01-C-0119/en) was presented by the BDT Focal Point for Question 22-1/1. It provides an update on some of the key activities that BDT is undertaking in the field of cybersecurity, in line with recent ITU developments, and how these activities (including the collaboration with EC project, MoU with UNODC, technical assistance for the establishment of CIRT, update on the national elaboration of the Cybersecurity Strategy Guide and the ITU IMPACT endevour) would contribute to the work of Q22-1/1.

Document [1/INF/33](http://www.itu.int/md/D10-SG01-INF-0033/en), was introduced by Republic of Korea and it shared a Smart Mobile Security Strategy and their Implications. As mobile devices have become an integral part of our lives, people are encountering cyber threats. The Korean Government established various collaborative platforms for smartphone and mobile security countermeasures and announced the Mobile Information Security Strategy in December 2010. With these pre-emptive countermeasures on possible security threats, Korea expects to minimize the future social cost. And also by establishing secure and reliable mobile service environment, citizens’ quality of life would be raised. Action: For inclusion in the compendium.

Document [1/INF/46](http://www.itu.int/md/D10-SG01-INF-0046/en) on Cybersecurity in Developing Countries was contributed by the Democratic Republic of the Congo. The contribution showed how while it is important to access telecommunication networks, it is necessary to deploy IT infrastructures and cyber services that are reliable, maintainable, robust and secure, while respecting basic human rights and the rights of States. In particular, developing countries need to enter the information society without exposing themselves to excessive risk, building on the experience acquired in the developed countries and avoiding the danger that a new factor for their exclusion arises in the form of cybersecurity. In the case of the Democratic Republic of the Congo, for instance, it has no policy for protecting people, data or infrastructure. Action: for inclusion in the compendium.

Tanzania reported verbally on some cybersecurity developments in Tanzania. The Rapporteur thanked Tanzania and asked it to put this information in writing and submit it as a contribution to the next meeting so that it could be included in the compendium.

1. Review of the structure and content of the draft report.

The work plan identifies a number of deliverables (discussed in Agenda Item 5) for Q22-1/1. The draft reports that have been developed so far in Q22-1/1 are responsive to a number of these deliverables. At the next meeting in May, Q22-1/1 will be asked to adopt texts that have been developed on the following topics:

* A maturity model implementation guide for national administrations
* Best practices for building and managing a national CSIRT
* Best practices for Network Protection by Internet Service Providers
* Best practices for Cybersecurity Public-Private Partnerships

In addition, Brazil (Vice-Rapporteur Ms Vanessa Cravo) has said it would contribute a table of contents or outline on the compendium project.

Also, Oman (Vice-Rapporteur Ms Rozalin Al-Balushi), Tanzania (Vice-Rapporteur Ms Elizabeth Nzagi) and Côte D’Ivoire (Vice-Rapporteur Ms Fabienne Apetey) have agreed to lead an effort to develop a questionnaire to obtain information about cybersecurity awareness-raising projects that countries have developed.

1. Review of work plan for the study period

Document [1/38](http://www.itu.int/md/D10-SG01-C-0038/en), the work plan for Question 22-1/1, was reviewed by Mr James Ennis. He noted that the Question 22-1/1 is tasked with:

* producing a report or reports on best practices for a number of aspects of cybersecurity.
* deriving some course materials from these best practice materials.
* developing a compendium of the cybersecurity projects underway in different countries, based on the contributions that have been submitted and other information. Brazil (Vice-Rapporteur Vanessa Cravo) is the editor of this compendium. The Rapporteur asked if Brazil could produce an outline or table of contents for the compendium at the next meeting, classifying the contributions according to subject.
* conducting surveys to collect information of some of these topics, as appropriate.

1. Update on collaboration with other Questions in Study Groups 1 and 2 (if any) and with relevant BDT Programmes

It was recognized that the issue of cybersecurity needs of people with disabilities needs to be coordinated with Q20-1/1 on the telecommunication needs of persons with disabilities and some contributions were made that went to both Questions.

Similarly, the issue of security of cloud computing is closely related to the activities of Q19-2/1 which is considering the broad issue of implementation of IP in developing countries, including cloud computing.

Finally, issues of cybersecurity awareness in the public is related to the broader activities of Q18-2/1 dealing with consumers generally.

The BDT has an active program to provide assistance to developing countries in cybersecurity. It is intended that the reports of Q22-1/1 will be considered under as a source of material to be used in the BDT’s development activities.

1. Update on collaboration with other Sectors and Organizations

Collaboration has occurred with ITU-T through liaisons with Study Group 17 (network security) informing it about the contribution received from Brazil on Child on-line protection (COP)(Angels on the Net) and the reports that are being developed in Q22-1/1 on best practices in various cybersecurity areas. A response was received from SG17 about the COP activities underway in SG17.

Similar information was sent regarding the Brazilian project “Angels on the Net” via liaison to the ITU-T Council Working Group (CWG) on COP, which will consider it at its next meeting in October.

1. Approval of meeting output documents

The only output document from the meeting is the report of the meeting from the Rapporteur.

1. Place and date of the next Rapporteur Group meeting

The next meeting of the Rapporteur Group will be held between April 16 and May 11, 2012; the exact date has not yet been determined.

1. Any other business

None

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