|  |  |
| --- | --- |
| **Document Title:** | **Draft RESOLUTION GSC-16/11: (GTSC) Cybersecurity (Reaffirmed)** |
| **Source:** | GTSC-9 |
| **Contact:** | Wayne Zeuch (ATIS) |
| **GSC Session:** | Closing Plenary |
| **Agenda Item:** | 3.9 |

|  |
| --- |
| **RESOLUTION GSC-16/11: (GTSC)Cybersecurity (Reaffirmed)** |

The 16th Global Standards Collaboration meeting (Halifax, 31 October – 3 November 2011)

## Recognizing:

1. the crucial importance of the information and communications infrastructure to practically all forms of social and economic activity, and the need for everyone to assume their role in contributing to its security on an ongoing basis;
2. that the legacy Public Switched Telephone Network (PSTN) has a level of inherent security properties because of its hierarchical structure and built-in management systems;
3. that the converged legacy networks and IP networks are therefore potentially more vulnerable to intrusion if adequate care is not taken to integrate security requirements into the planning and design as early as possible;
4. that the type and number of cyber attacks in terms of worms, viruses, malicious intrusions and thrill-seeker intrusions is on the increase;
5. that new cyber attacks such as phishing, pharming, malware distributed via the web, and botnets are emerging and spreading rapidly;
6. that the source of attack or spoofed IP address used by attackers need to be identifiable;
7. that ITU-T Recommendation X.1205 “*Overview of Cybersecurity*” provides a definition, description of technologies, and network protection principles;
8. that ITU-T Recommendation X.805 provides a systematic framework for identifying security vulnerabilities that together with many new security-related deliverables from the ITU and the Participating Standards Organizations (PSOs) can assist risk assessment and the development of mechanisms to mitigate the risks;
9. that the ITU-T and ISO/IEC JTC 1 already has a significant body of published materials and ongoing work that is directly relevant to this topic, that needs to be taken into account and integrated;
10. that the UN World Summit on the Information Society identified the ITU as the facilitator and moderator for its Action Line C5 (Building confidence and security in the use of ICTs);
11. that the Global Cybersecurity Agenda (GCA) of the ITU promotes international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the use of ICTs;
12. that the World Telecommunication Standardization Assembly (Johannesburg, 2008) revised WTSA Resolution 50 on Cybersecurity, which underlined the vigorous activity and interest in the development of security standards and Recommendations in ITU-T Study Group 17 and in other standardization bodies, including the Global Standards Collaboration (GSC) group, as well as Resolution 52 (Countering and combating spam) (Johannesburg, 2008) which, *inter alia*, highlighted the need to address the problems associated with spam including its use for the dissemination of unsolicited software;
13. that the ITU World Telecommunication Policy Forum (Lisbon, 2009) adopted Opinion 4 entitled *Collaborative strategies for creating confidence and security in the use of ICTs*, which underlined the critical importance of international, regional and national cooperation in developing effective strategies to mitigate cyber threats, including spam;
14. that the ITU-D approved a 2010 report under Question 22/1, *Securing information and communication networks: best practices for developing a culture of Cybersecurity,* and the W2010 WTDC approved a revised Question 22/1 for 2011-2014, and Resolution 45, *Mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam;*
15. that *Cybersecurity, ICT applications and IP-based network-related issues* is one of the priority domains of Programme 2 of the Hyderabad Action Plan adopted by the 2010 World Telecommunication Development Conference (WTDC-10), along with a revision to ITU-D Study Question 22/1: Securing information and communication networks: Best practices for developing a culture of cybersecurity;
16. that amendments to WTDC RESOLUTION 45 (Rev. Hyderabad, 2010), *Mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam*, were adopted which highlight the importance of close collaboration between the work of the Telecommunication Development Sector and the Telecommunication Standardization Sector;
17. the need for national, regional and international strategies and initiatives to be harmonized to the extent possible to avoid duplication and to optimize the use of resources;
18. that cooperation and collaboration among organizations addressing security issues can promote progress and contribute to building and maintaining a culture of cybersecurity;
19. that achieving most of the above requirements is highly dependent on the development of global cooperative and collaborative strategies, taking advantage of activities and initiatives being undertaken on an international, regional and national basis, for the exchange of information; and
20. that cybersecurity metrics (e.g., parameters that may be used domestically within a corporation, or organization etc. in cybersecurity indices) could be helpful.

## Resolves:

To encourage Participating Standards Organizations (PSOs) and Observer Organizations of the Global Standards Collaboration (GSC) on an ongoing basis to:

1) evaluate existing and evolving new standards and Recommendations, and especially signaling and communications protocol standards and Recommendations with respect to their robustness of design and potential for exploitation by malicious parties to interfere destructively with their deployment in the global information and communications infrastructure;

1. consider using ITU-T Recommendations, including X.805 and X.1205, ISO/IEC products/standards and other relevant deliverables from the ITU and PSOs as a framework for assessing networks and protocols for security vulnerabilities and to share experiences;
2. recognize the importance of ITU-T Recommendations which can be used to facilitate secure transport and service interconnection;
3. raise awareness within their areas of operation and influence of the need to protect information and communications systems against the threat of cyber attack;
4. promote global, consistent, interoperable and measurable processes for sharing information through the development of collaborative and cooperative strategies including ITU and other international, regional and national organizations and entities involved in cybersecurity activities;
5. work with the ITU and others to develop standards or guidelines to protect against botnet attacks, malware distributed via the web and facilitate tracing the source of an attack;
6. work with the ITU and others to contribute to guidelines and best practices (e.g., self-assessment tool[[1]](#footnote-1)) in building a culture of cyberscurity, e.g., the Korean experience with cybersecurity indices;
7. supply updated information on their security standards work for inclusion in the “*ICT Security Standards Roadmap*”[[2]](#footnote-2)*,* a database of security standards hosted by the ITU-T;
8. request ITU, in building upon the information base associated with the “*ICT Security Standards Roadmap*” and the ITU-D efforts on cybersecurity, to prepare, with PSO assistance, an inventory of national, regional and international initiatives and activities to promote, to the maximum extent possible, the worldwide harmonization of strategies and approaches in this critically important area; and
9. work towards a cybersecurity information exchange framework which on a global basis,  
   provides for the reduction of threats, risks, and vulnerabilities by a) structuring cybersecurity information for exchange purposes, b) identifying and discovering  
   cybersecurity information and entities, c) requesting and responding with cybersecurity  
   information, d) exchanging cybersecurity information over networks, and e) trusted  
   cybersecurity information exchanges.

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

1. The ITU National Cybersecurity/CIIP Self-Assessment Tool is an initiative by the ITU-D to assist ITU Member States who wish to elaborate on their national approach for cybersecurity and critical information infrastructure protection (CIIP). [↑](#footnote-ref-1)
2. <http://www.itu.int/ITU-T/studygroups/com17/ict/index.html> [↑](#footnote-ref-2)