Background Theme 4(a)
Cybersecurity

Pacific ICT Ministerial Forum: Connecting the Unconnected

17 February 2009, Tonga
Pacific Circumstances

- Little legislation specific to cybersecurity
- Some countries (e.g. New Zealand, Australia, Kiribati, Tonga) have taken steps to address cybersecurity
- Little effort on set up of Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT)
- Issue of telecommunication fraud i.e. Blocking and Hijacking
  
  *(WTSA-08 Res 61 “Misappropriation of international telecommunication numbering resources”)*)
Global Cybersecurity Agenda (GCA)

Building confidence and security in the use of ICTs

Global Cybersecurity Agenda

Five Pillars [Legal Measures, Technical and Procedural Measures, Organizational Structure, International Cooperation, Capacity Building]

Toolkits

- ITU National Cybersecurity/CIIP Self-Assessment Tool
- ITU Botnet Mitigation Toolkit
- Toolkits on the establishment of CERTs/CSIRTs
- “Understanding Cybercrime: A Guide for Developing Countries”
- ITU Toolkit for Cybercrime Legislation
Chile Online Protection (COP)

- Identifying risks for children/young people in cyberspace
- Creating awareness of the risks through multiple channels
- Developing tools to help governments, industry, educators, and relevant organisations minimize the risks
On-going Efforts

- Australian-supported “Anti-Spam Legislation Project”

- Feasibility Study on establishment of the PacificCERT

- ITU harmonization of legal frameworks e.g.
  - Assist countries in promoting cybersecurity culture and establishing a sound legal framework
  - ITU Toolkit for Cybercrime Legislation
Ways Forwards

- Coordination and Cooperation at both national and international levels (e.g. government, industry, private sector, and users)

- Implementation of a national strategy for cybersecurity and critical information infrastructure protection requires a comprehensive approach

- Promoting a culture of cybersecurity

- PacificCERT
Thank You