Australian Government
Department of Broadband, Communications and the Digital Economy

Australian Government Cyber-security Activities in the Pacific

Daniel Wells

International Branch

Department of Broadband, Communications and the Digital Economy

Overview

- Australia's engagement with the Pacific
- DBCDE and AusAID anti-spam legislative project for the Pacific
- Pacific CERT initiative
- Next steps

Engagement with the Pacific

- DBCDE manages the Australian Government's engagement with PICs in terms of telecommunications capacity building activities.

- Promote liberalised telecommunications markets and the adoption of best practice regulatory environments.

Engagement with the Pacific cont.

- Regional and international fora:
  - ITU, Asia Pacific Telecommunity, Asia Pacific Economic Cooperation, Pacific Islands Telecommunications Association, Pacific Island Forum Secretariat

- Goal – assist policy makers & regulators through capacity building projects to improve access, security & governance in the telecommunications sector.

Engagement with the Pacific cont.

- Cyber security focus, coordinated across key regional & international organisations.
- For example:
  - APT/ITU/PITA Joint Regulatory Forum for the Pacific Island countries (Fiji , July 2006);
  - APT/ITU/PITA Workshop on Principles of Cyber legislation for the Pacific Island countries (New Zealand, March 2007); and
  - Regional workshop on Frameworks for cybersecurity and critical Information Infrastructure protection, (Vietnam, August 2007) APEC TEL work (malware, SPSG)

Engagement with the Pacific cont.

- PIFS Taskforce on Regional Approaches to ICTs in the Pacific
- The World Bank

Anti-spam Legislative Project

- Strengthening Spam Legislation, Enforcement and Cooperation Regimes in the Pacific project.

- Collaboration between DBCDE and AusAID, with support from the Australian Communications & Media Authority

Anti-spam Legislative Project cont.

Three parts:

– Develop, in collaboration with participating PICs, anti-spam legislation specific to each country, using Australia's *Spam Act* as a model;

– Build local enforcement capacity; and

– Participation in a network of international enforcement agencies.

Anti-spam Legislative Project cont.

- Builds on earlier work in Tonga & the Cook Islands

- Legislation is at various stages in participating PICs

Anti-spam Legislative Project cont.

Pacific Anti-spam Enforcement workshop

1. Identify enforcement authorities

2. Enforcement mechanisms

3. Public awareness campaigns

4. Domestic cooperative arrangements

Anti-spam Legislative Project cont.

5. International cooperative arrangements
6. Capacity building requirements

Anti-spam Legislative Project cont.

Pacific Anti-spam Enforcement workshop

Action Items

1. Enforcement Grouping linked to PITA Meetings

2. Direct ACMA/DBCDE engagement with Enforcement Grouping

Anti-spam Legislative Project cont.

3. Identify & share awareness raising & education materials

4. PICs to review Legislation if necessary

5. PICs participation in international anti-spam fora

6. Dialogue with ACMA & DBCDE

Pacific CERT Initiative

- What, why, who and how?

- What?

  – Computer Emergency Response Team = CERT

    - Provide a coordinated approach to informing key stakeholders of the latest cyber-threats; and

    - Assist in developing coordinated responses to these threats

Pacific CERT Initiative cont.

- Why?
  - CERTs are a crucial part of a broader e-security strategy.
  - Inform key stakeholders in the ICT community about the latest e-security threats.

Pacific CERT Initiative cont.

- Who?
  - DBCDE, ITU, AusCERT, SOPAC, PICISOC.
- How?
  - Through Australia's contributions to the ITU & in collaboration with AusCERT, a scoping study into the creation of a Pacific CERT will be undertaken.

Future Projects

- Grateful for your views
  - Priorities
  - Specific activities
  - daniel.wells@dbcde.gov.au

Thank you