



Pacific Islands CERT (PacCERT)

Updates & Current Status

Outlines

- **Background**
- **Where we are now !!!**
- **The challenge of establishing a regional CERT in this region**

Background

- **Early 2007 - Various groups in Fiji and the region saw the need for a CERT for Pacific Island countries**
- **Feb 2010 - The Working Group met and discussed and developed the Business Plan for PacCERT**
- **June 2010 - ICT Ministerial meeting held in Tonga endorsed the Business Plan**

Background

- The Ministerial meeting also endorsed for USP, Japan-Pacific ICT Centre to host PacCERT
- March 2011 - The Ministerial meeting in Noumea also requested ITU and shareholders to consider funding this initiative
- Nov 2011 - PacCERT was in operation



PacCERT - Vision



**“Make the Pacific Islands Countries
safer in the global Internet
community”**



PacCERT - Mission



“The Pacific community, like the rest of the world, is connected to and dependent on the Internet. Internet security and safety of each member state is essential for sustainable future growth.

PacCERT was established to facilitate, coordinate and monitor activities related to cyber security to secure fast and effective response to cyber security and threats”



Pacific Islands CERT

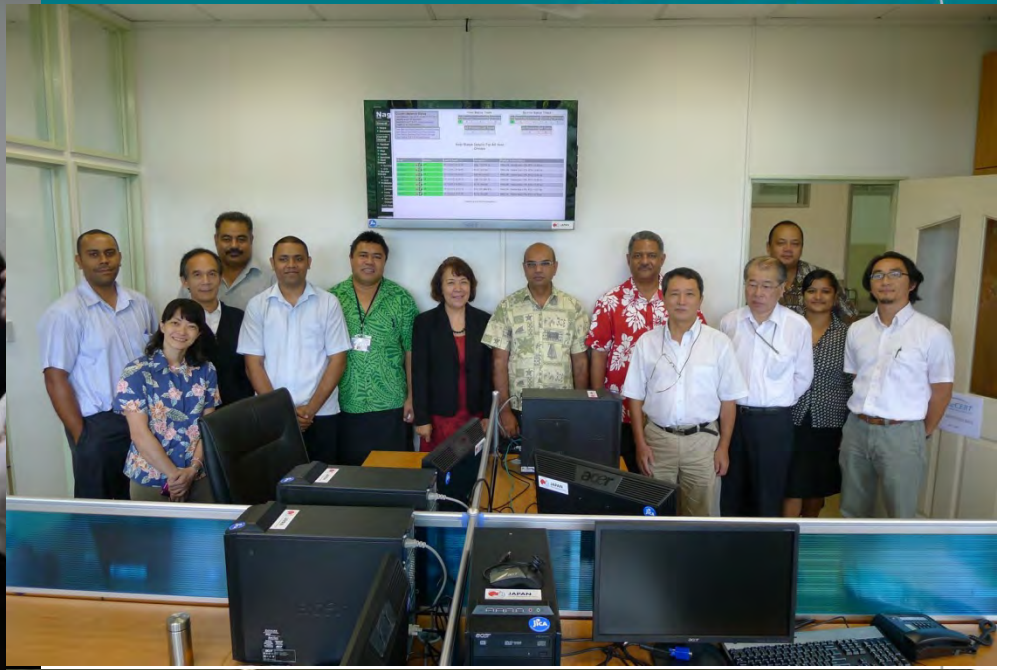


PacCERT - Goal

- **To raise ICT and cyber security awareness**
- **To ensure that Pacific Island countries response to Internet threats is appropriate and timely**
- **To build the Information Security capacity and expertise of Pacific Island countries**
- **To support establishment of National CERTs within the Pacific**
- **To work closely with the governments and industries to secure information and communication infrastructure**

Expected Services

- **Incident Handling and Response**
 - **Coordination Centre to Handle Incidents**
- **Analysis of Malicious Code and Advise Members**
- **Log Analysis and Dissemination of Information to Members**
- **Provide Awareness, Training and Education**
- **Security Survey**
- **Cybercrime Legislation**
- **Outreach Programme**



BRAVIA



Document | Graph | Kmldata | RawData | > Google Earth | > SYSTEM SETTING

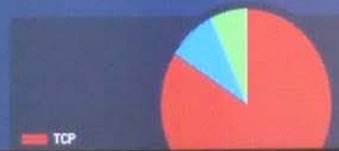
1 July 2012 / 04:00:00



ALL

Mode [Icons] Map world Data Day/Week Date 2012-07-01 Speed Faster Ctrl [Pause]

Protocol Share Graph



Scan Packet Graph



Top5 Port Count Graph



Current Status

- **The operational functions of PacCERT have been suspended since 31st Dec 2014.**
 - **No staffing since both Manager and Technical Staff left because of no funds**
 - **The office space and equipment are still there**
- **Board**
 - **The PacCERT Board is still working on models and strategies**

Challenging Issues

- **With more submarine cables made available in this region and high bandwidth, PICs are more vulnerable and at higher risk of cyber attacks**
- **Awareness – Lack of in-depth user awareness in this region on ICT and Security generates vulnerabilities**
- **Expertise – experts are in great demand, but availability is short**
- **Cyber Security – Deal with it or Dealing individually**
- **Cost of establishing a National CERT may be too high for some**

Challenging Issues

- **Costs of training is high**
- **Lack of technical skills and knowledge on how to deal with Cyber Security**
- **Scale and speed of response to threat warrants a layered approach within the countries and regionally**
- **Cybersecurity issues in one country affect other nations, thus needing coordination**
- **Lack of standards around Policy & Regulation dealing with Cybersecurity**

Future of PacCERT

- **The question is whether the Pacific Regional still need to have PacCERT**
- **Funding ?????**
- **Sustainability**
- **Governance**

Malo

