Attack & Contingence Response Planning for ccTLD .CR
A practical case for a small ccTLD

Luis Espinoza

NIC-Internet Costa Rica

lespinoz@nic.cr

ICANN 35

Sydney, Australia 21-26 June 2009

Agenda

About NIC-Internet Costa Rica

ACRP Workshop in Mexico

ACRP Process at NIC-CR

Findings

Conclusions

About NIC-CR

The ccTLD administration is delegated to ANC (National Academy of Sciences of Costa Rica)

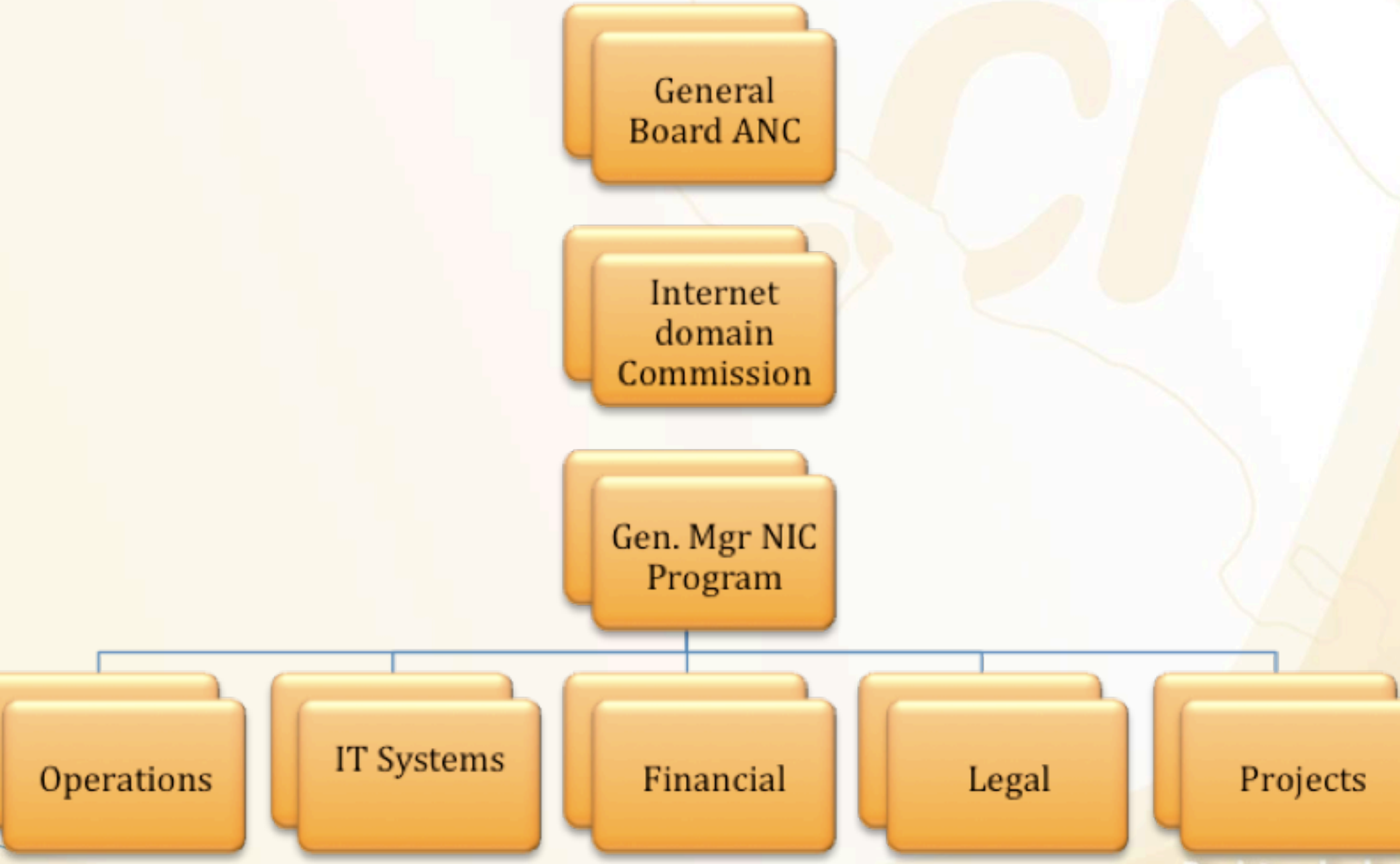
NIC-CR is a Program of ANC.

9 persons permanent staff.

Services by outsourcing: Legal, Systems Development, Communication, Accounting, etc.

Number of domains registered: 11731

NIC-CR Organigram



ACRP Workshop
Mexico City 26-28 Feb 2009

ACRP Process

ACR Plan Process - Review

ACRP Process at NIC-CR

Work Team

Check list for NIC-CR

Project Initiation Checklist

Project Initiation Checklist			
Gather the following documents / information:			
Organization Chart			OK
Existing Plans	Disaster Recovery Plan		Partial
	Business Continuity Plan		NO
	Information Backup / Archive Plan		Partial
	Fire Evacuation Plan		NO
	Other: Strategic Plan		Partial
Emergency Contact Information	Business / Technical Staff		Partial
	Emergency Services (Fire, Police, Medical)		No documented
	Key Stakeholders (Commissioners, Board Members, Government Representatives, ...)		Not up to date
	Suppliers / Vendors (Equipment, Personnel, Facilities)		Not up to date
Facility Maps and Floor Plans			
Documented Procedures	Offsite Storage		Yes
	Evacuation		Partial
	Health and Safety Reporting		No
	Operations and Administrative Procedures		Yes
	Data / Information Security (includes Protection of Privacy Information)		Partial
IT System Information	Network Topology / Diagrams		Not up to date
	Inventory / System Configurations (make/model/specs of IT systems; software version numbers)		Yes
Maintenance / Service Level Agreements			No
Industry Regulations / Guidelines			RFC 1591, UDRP, etc

Challenges

The strategic planning is project oriented, then it doesn't include definition of strategic objectives formally.

Many things are not documented.

Very busy people with operative tasks.

No high-level expert in Risk or Strategic Planning, but the knowledge from Mexico's workshop.

ACRP Action Plan

Skip all introduction. Go directly to the forms.

Deduct Business Objectives from projects planned and interview with administrative staff.

Scope: create a baseline Plan, no too detailed, no too comprehensive.

Presents results in short time.

Findings

Electricity Poles

Major threats

Transcription errors in zone files.

Database corruption in the NIC Portal System.

Cables manipulation at telecom room.

Atmospheric phenomena cuts the power.

Car crashes to the electricity poles.

To do

Develop the Plan following the guide from worksho

Present the Plan to the Domain Commission for approval.

Train, test and maintain the Plan.

Conclusions

We must response to Conficker threat without a Pl
developed, using common sense and some
experience. But is better to have a plan.

In a small ccTLD, there is no time or budget for
sophisticated and complex plans, should be
something very practical.

During the ACRP process, we create awareness
about to have a plan for contingency and incident
response.

uestions?

commons

Attribution 3.0 Unported

You are free:

to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

Under the following conditions:

Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

With the understanding that:

Waiver — Any of the above conditions can be **waived** if you get permission from the copyright holder.

Other Rights — In no way are any of the following rights affected by the license:

- Your fair dealing or **fair use** rights;
- The author's **moral** rights;
- Rights other persons may have either in the work itself or in how the work is used, such as **publicity** or privacy rights.

Notice — For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to this web page.

This is a human-readable summary of the Legal Code (the full license).

Registro de don