DSSA Update

Costa Rica – March, 2012

Goals for today

- Update you on our progress
- Raise awareness
- Solicit your input

Charter: Goals and Objectives

Report to participating SO's and AC's on:

- Actual level, frequency and severity of threats to the DNS
- Current efforts and activities to mitigate these
- Gaps in the current response to DNS issues
- Possible additional risk mitigation activities that would assist in closing those gaps

Unpacking some terms

Our charter speaks to "Threats"

Threat-events (what happens) should not be confused with:

- **Adverse impacts -** that may result
- **Vulnerabilities -** that allow them to happen
- **Predisposing conditions -** that influence adverse impact once they're under way
- **Controls and mitigation** – that reduce likelihood and impact
- **Threat-sources –** which exploit vulnerabilities to initiate them

Activity since Dakar

- The working group has:
  - Developed a protocol for handling confidential information
  - Selected, and begun to tailor, a methodology to structure the remaining work
  - Begun the detailed analysis of the risk assessment

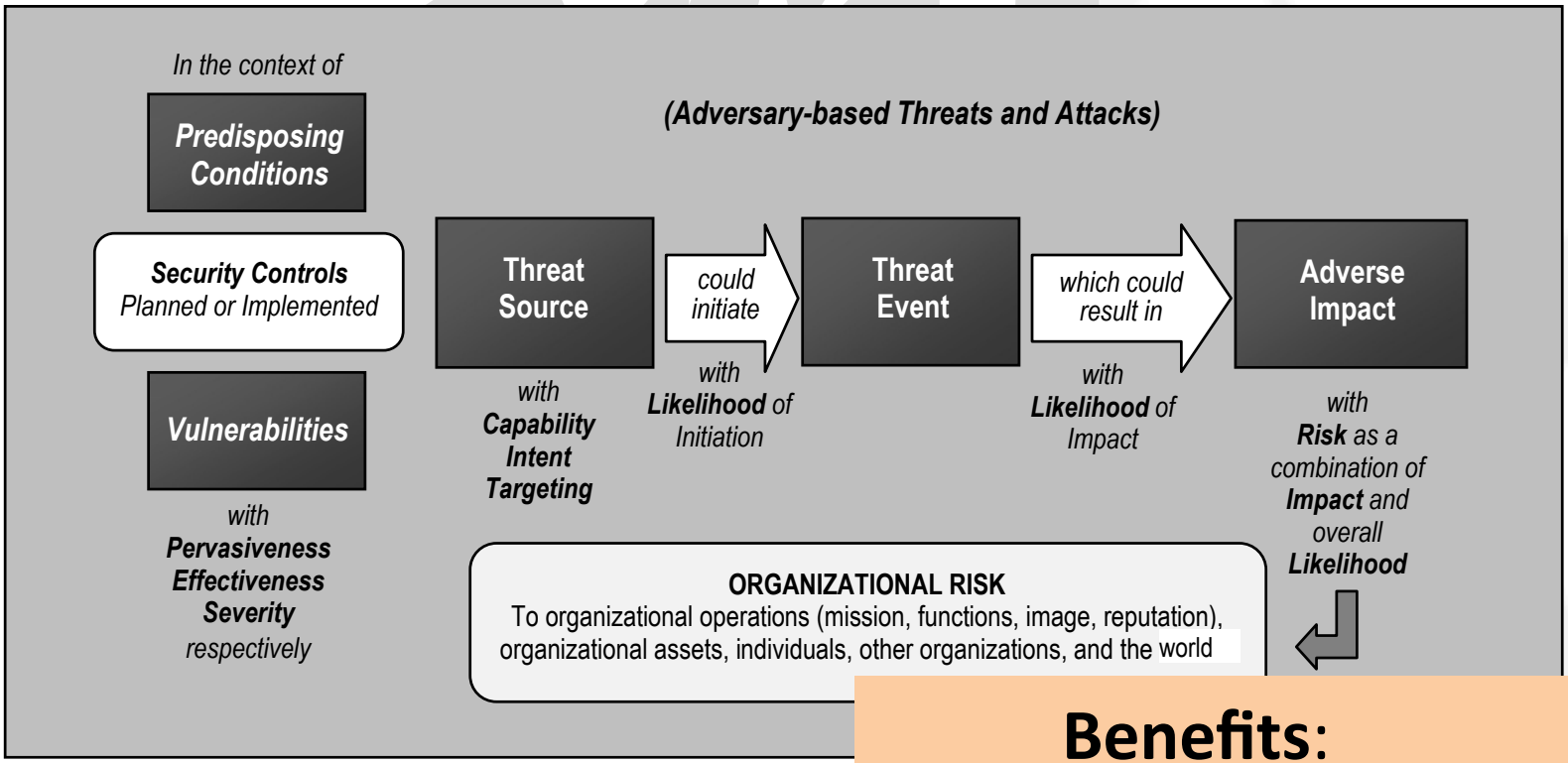
Methodology – NIST 800-30

Rationale

- Using a predefined methodology will save time and improve our work product
- Reviewed several dozen alternatives
- We selected this one because it's:
  - Available at no cost
  - Actively supported and maintained
  - Widely known and endorsed in the community
  - Reusable elsewhere in ICANN

Methodology – NIST 800-30

Example – Adversarial Risk Model



Benefits:

- Consistent terminology
- Shared model
- Structured work
- Sample deliverables

Where we are…

Approach

Launch

Identify Threats & Vulnerabilities

Analyze Threats & Vulnerabilities

Report

We are here – getting started with this phase of the work

We are hoping to have a high-level version of this done by Prague

Where we are…

Status

- 43 weeks (or 43 hours) in
- We've developed substantial (and reusable)
  - **Data**
  - **Methods**
- Given our **resources**, pick any 2 of 3 going forward
  - **Detail** (identify vs. analyze high-risk scenarios)
  - **Speed** (6 months vs. 36)

Where we are…

Determinations – Threat events and level of impact

Level of Impact:

In the worst case there would be broad harm/consequence/ impact to operations, assets, individuals, other organizations and the world if any of these threat-events occur. And in all cases there would be significant problems for registrants and users in the zone.

Threat events:

- Zone does not resolve
- Zone is incorrect
- Zone security is compromised

Where we are…

Determinations – **Nature of impact**

- Damage to a critical infrastructure sector
- Damage to trust relationships or reputation
- Harm to individuals
- Harm to assets
- Harm to operations

Where we are going

- **Vulnerabilities** – severe and widespread?
- **Predisposing conditions** – pervasive?
- **Controls and mitigation** – effective and deployed?

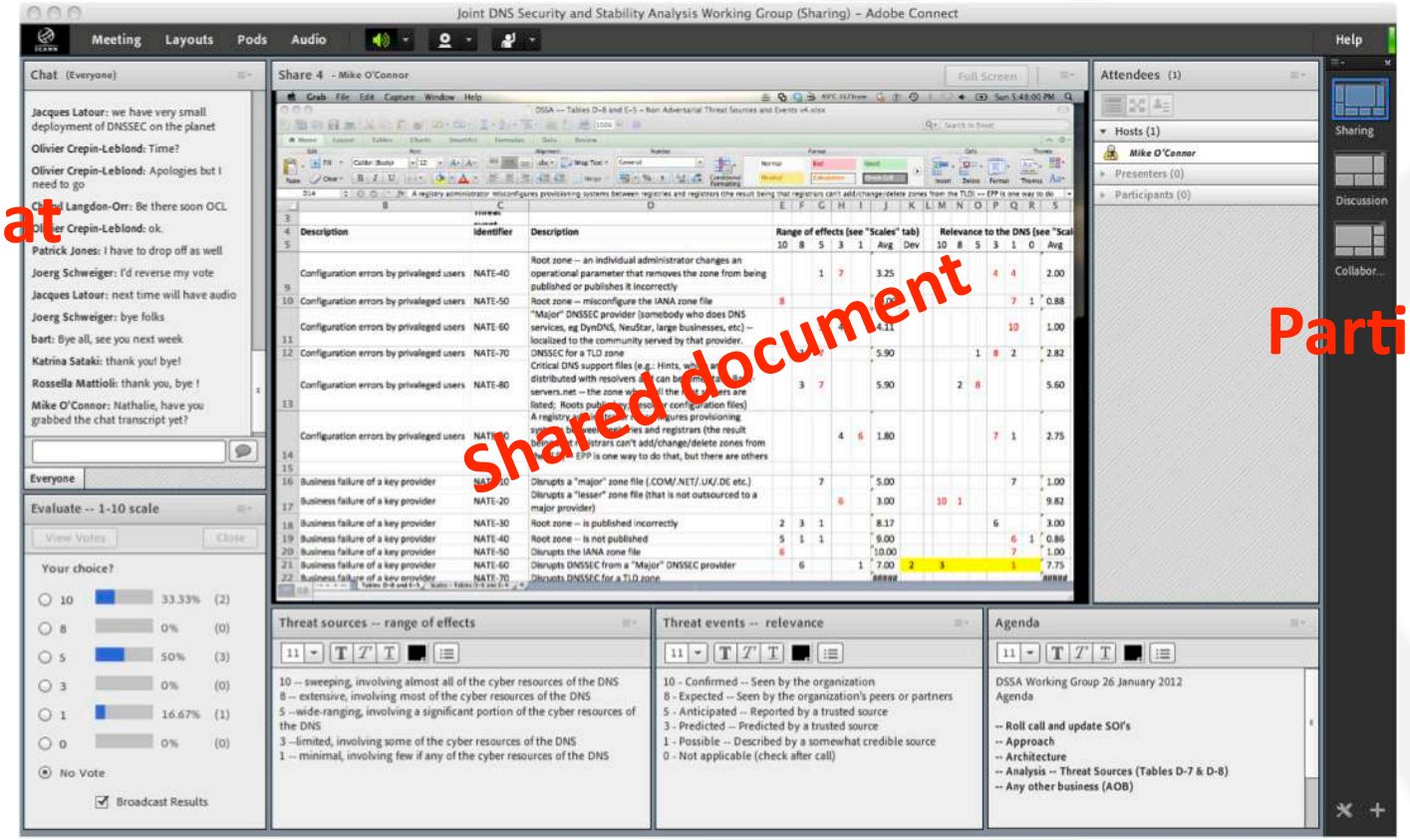
- **Threat sources** – how broad is range of impact, what are their capabilities, how strong is their intent, are they targeting the DNS?
- **Initiation** – what is the likelihood that a threat-event will happen?

- Given all of the above – **what are the high-risk scenarios?**

Questions?

How we work

(design credit -- CLO)



Live chat

Shared document

Participants

Polling

Definitions

Agenda

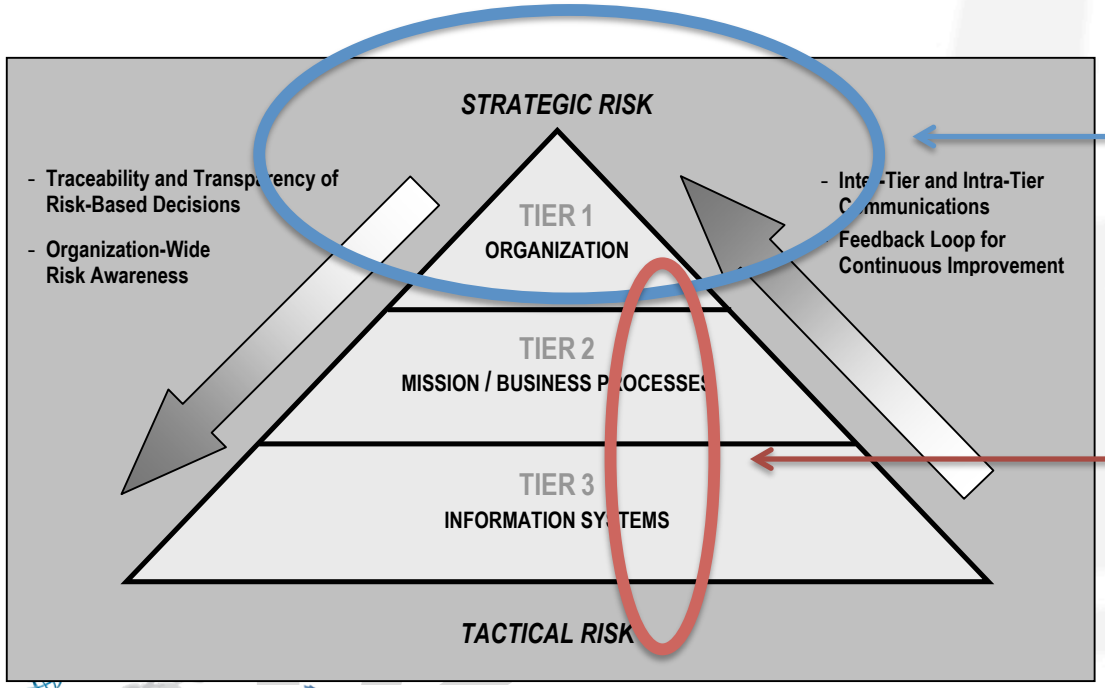
Charter: Background

At their meetings during the ICANN Brussels meeting the At-Large Advisory Committee (ALAC), the Country Code Names Supporting Organization (ccNSO), the Generic Names Supporting Organization (GNSO), the Governmental Advisory Committee (GAC), and the Number Resource Organization (NROs) acknowledged **the need for a better understanding of the security and stability of the global domain name system (DNS)**. This is considered to be of **common interest** to the participating Supporting Organisations (SOs), Advisory Committees (ACs) and others, and should be preferably **undertaken in a collaborative effort.**

Methodology – NIST 800-30

Risk Management Hierarchy

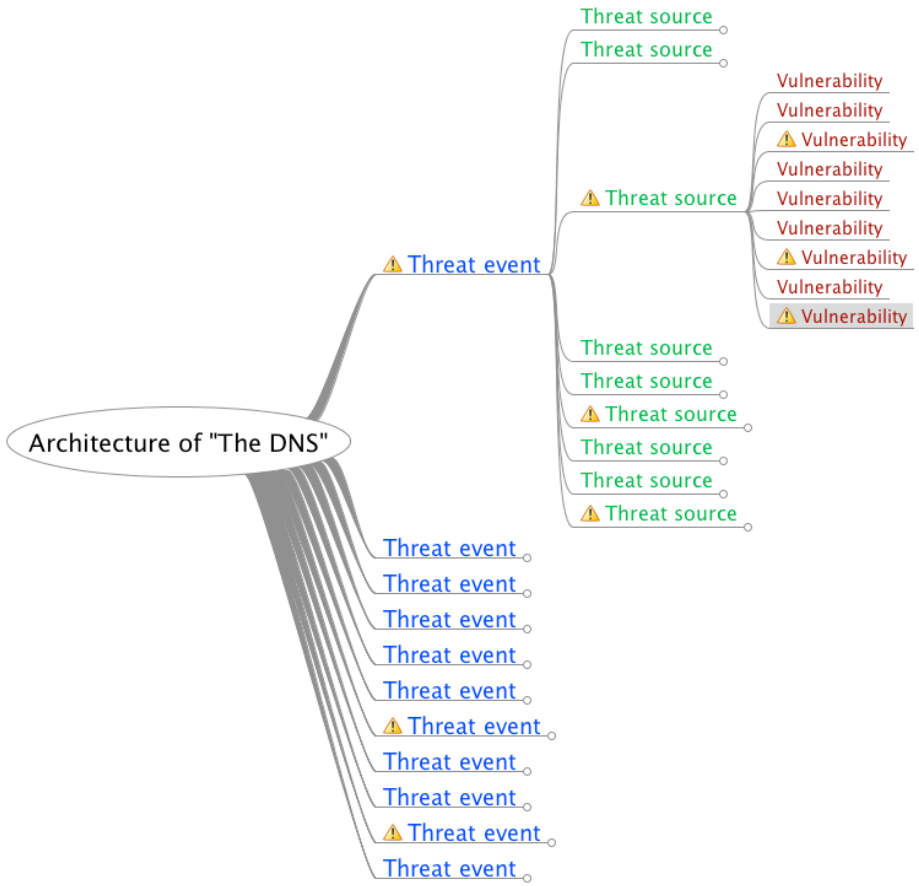
The methodology presumes a tiered approach to the work



- DSSA is chartered to look at the broadest, most general tier
- However it may be useful to pursue one or two deeper, narrower analyses of specific threats once the "survey" work is complete

Problem: the evaluation per NIST methodology does not scale

It's all about choices



- Threat tree could easily grow to over 1000 permutations
- Prune the tree along the way, in order to focus on the highest risks
- Leave a framework that can be used to address:
  - New things
  - Changes
  - Greater detail

Confidential information

Note: Sensitivity, attribution **and release to public** are determined by info-provider	**Sensitive**		**Not sensitive**
Not attributed to source (transmitted through trusted 3rd party or summaries of Type 1 developed by sub-group)	Type 2: Distributed to sub-groups only. (Info-providers determine ultimate distribution)	Info-provider authorizes release	Type 3: Distributed to DSSA and public ("sanitized" info from sub-groups and other non-attributed information)
Attributed to source	Type 1: Distributed to sub-groups only (under NDA, most-protected)	Confidential info must never pass through this path. This is the exposure of information we're trying to prevent.	Type 4: Distributed to DSSA and public