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 respective participating SO's and AC's on:

- Actual level, frequency and severity of threats to the DNS
- Current efforts and activities to mitigate these threats to the DNS
- Gaps (if any) in the current response to DNS issues
- Possible additional risk mitigation activities that would assist in closing those gaps (if considered feasible and appropriate by the WG)

Unpacking some terms

Our charter speaks to “Threats”

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

- **Adverse impact -** things that may result from the threat-event
- **Vulnerabilities -** things that allow it to happen
- **Predisposing conditions -** things that help prevent it from happening
- **Adversarial threat-sources –** people initiating it
- **Non-adversarial threat-sources** - non-adversarial events that initiate it
- **Controls and mitigation -** actions to reduce likelihood and impact

Activity since Singapore

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

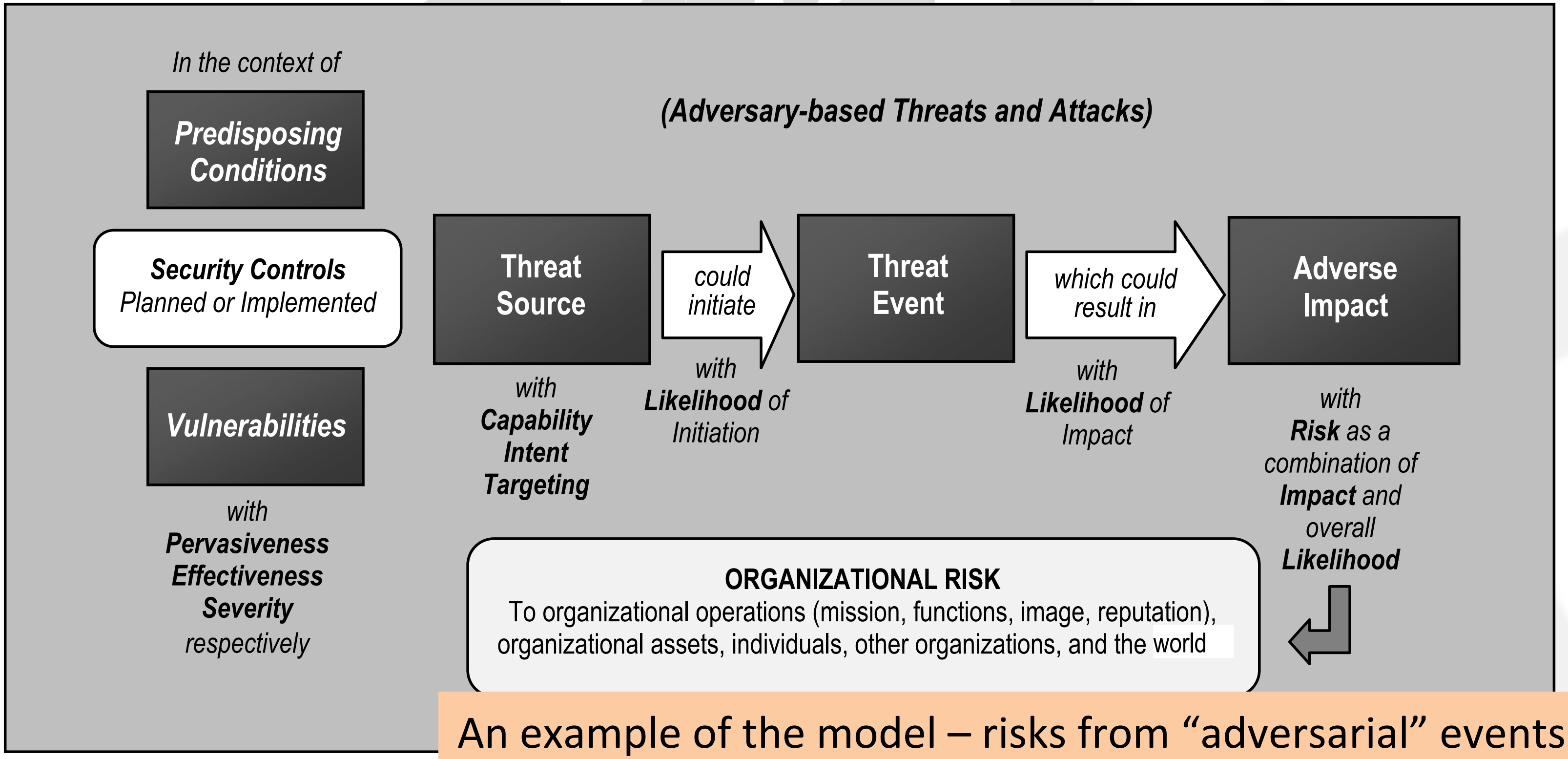
Methodology – NIST 800-30

Rationale

- The DSSA realized that using a predefined methodology would save time and improve our work product
- We selected NIST 800-30 after reviewing several dozen alternatives
- The reasons we selected this one include:
  - It's available at no cost
  - It's being actively supported and maintained
  - It's widely known and supported in the community
  - It's likely to be consistent with the needs of other parts of ICANN (and thus our pioneering may produce something that can be "repurposed" elsewhere in the organization)

Methodology – NIST 800-30

Example – Adversarial Risk Model



In the context of

Predisposing Conditions

Security Controls
Planned or Implemented

Vulnerabilities

with
Pervasiveness
Effectiveness
Severity
respectively

(Adversary-based Threats and Attacks)

Threat Source

with
Capability
Intent
Targeting

could initiate

with
Likelihood of
Initiation

Threat Event

which could result in

with
Likelihood of
Impact

Adverse Impact

with
Risk as a
combination of
Impact and
overall
Likelihood

ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the world

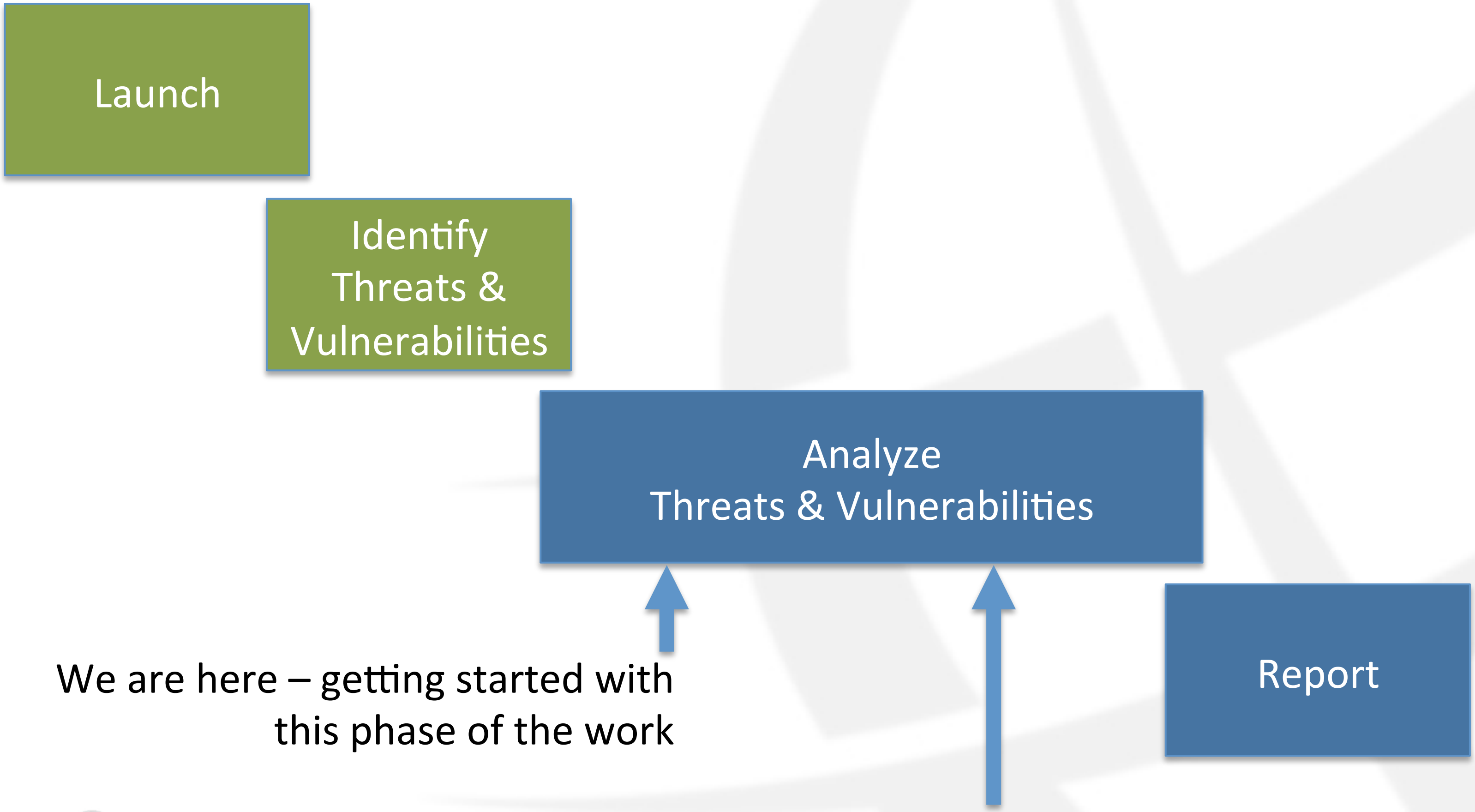
An example of the model – risks from “adversarial” events (which differs from “non-adversarial” threats such as errors, accidents, etc.)

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

- We’ve been at this for 43 weeks
- 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)
  - **Accuracy**

Where we are…

Analysis phase – based on tailored NIST methods

Assess threat events

We have concluded that there are three threat-events:

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

Determine 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.**

Determine nature of impact

- Damage to or incapacitation of a critical infrastructure sector.
- Relational harms (damage to trust relationships or reputation)
- Harm to individuals (Injury or loss of life, damage to image or reputation)
- Harm to assets (physical facilities, information systems, networks, information assets)
- Harm to operations, e.g.:
  - Inability to perform current missions/business functions.
  - Direct financial costs.
  - Harms (e.g., financial costs, sanctions) due to noncompliance with laws, contracts or regulations.

Where we are going

Analysis phase – based on tailored NIST methods

Assess vulnerabilities, controls and predisposing conditions

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

Determine likelihood

- **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?

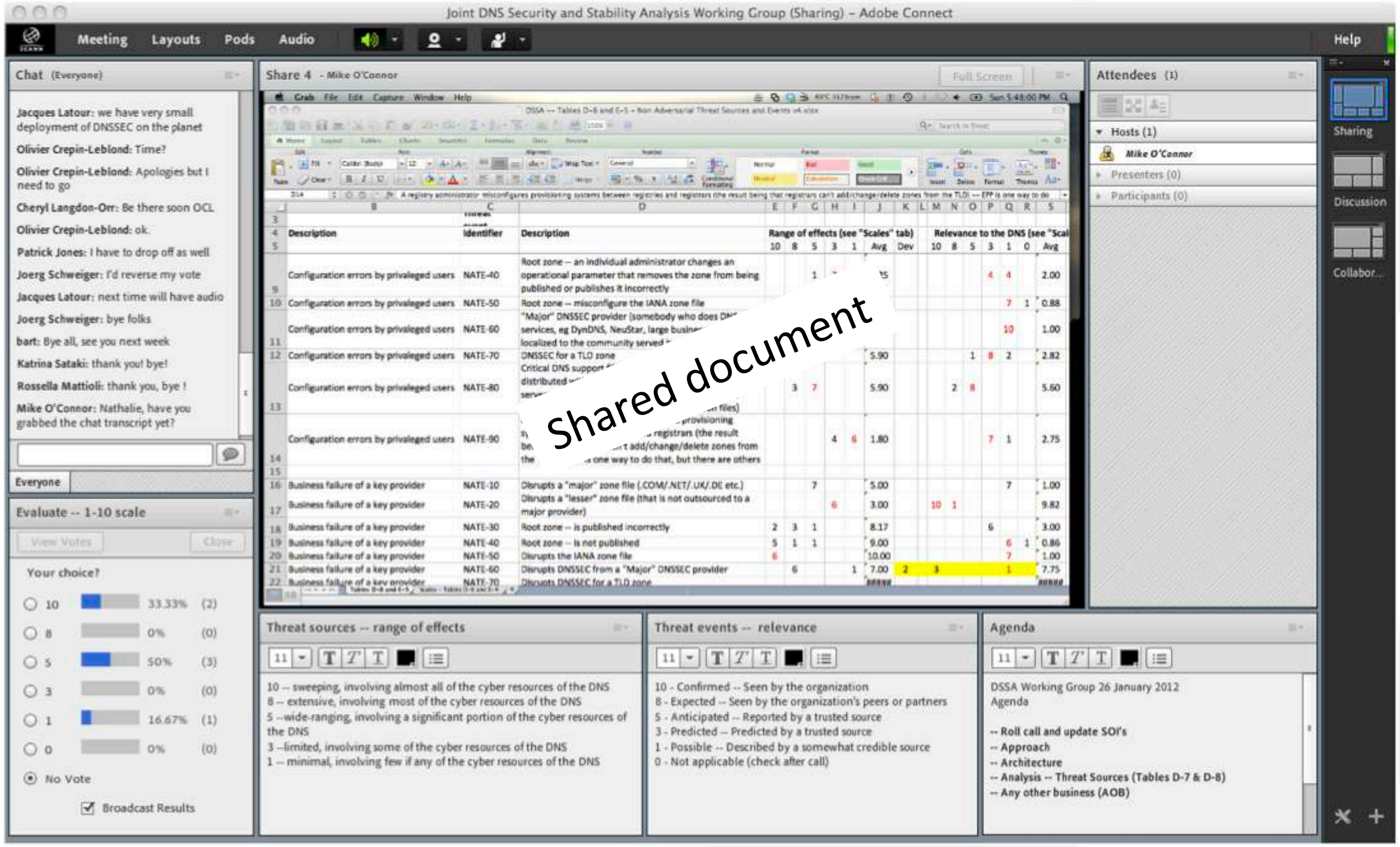
Determine risk

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

Questions?

How we work

(design credit -- CLO)



Joint DNS Security and Stability Analysis Working Group (Sharing) – Adobe Connect
Meeting
Layouts
Pods
Audio
Help

Live chat

Chat (Everyone)

Jacques Latour: we have very small deployment of DNSSEC on the planet

Olivier Crepin-Leblond: Time?

Olivier Crepin-Leblond: Apologies but I need to go

Cheryl Langdon-Orr: Be there soon OCL

Olivier Crepin-Leblond: ok

Patrick Jones: I have to drop off as well

Joerg Schweiger: I'd reverse my vote

Jacques Latour: next time will have audio

Joerg Schweiger: bye folks

bart: Bye all, see you next week

Katrina Sataki: thank you! bye!

Rossella Mattioli: thank you, bye !

Mike O'Connor: Nathalie, have you grabbed the chat transcript yet?

Polling

Evaluate -- 1-10 scale

Your choice?

○	10	33.33%	(2)
○	8	0%	(0)
○	5	50%	(3)
○	3	0%	(0)
○	1	16.67%	(1)
○	0	0%	(0)
●	No Vote		

☑ Broadcast Results

Share 4 - Mike O'Connor

DSSA -- Tables D-8 and E-5 – Non Adversarial Threat Sources and Events v4.xlsx

D14: A registry administrator misconfigures provisioning systems between registries and registrars (the result being that registrars can't add/change/delete zones from the TLD) -- EPP is one way to do

Shared document

	B	C	D	E	F	G	H	I	J	K	M	N	O	P	Q	R	S
3		Threat event															
4	Description	Identifier	Description	Range of effects (see "Scales" tab)							Relevance to the DNS (see "Scal						
5				10	8	5	3	1	Avg	Dev	10	8	5	3	1	0	Avg
9	Configuration errors by privaleged users	NATE-40	Root zone -- an individual administrator changes an operational parameter that removes the zone from being published or publishes it incorrectly			1	7		[illegible]5					4	4		2.00
10	Configuration errors by privaleged users	NATE-50	Root zone -- misconfigure the IANA zone file												7	1	0.88
11	Configuration errors by privaleged users	NATE-60	"Major" DNSSEC provider (somebody who does DN[illegible] services, eg DynDNS, NeuStar, large busine[illegible] localized to the community served [illegible]												10		1.00
12	Configuration errors by privaleged users	NATE-70	DNSSEC for a TLD zone						5.90				1	8	2		2.82
13	Configuration errors by privaleged users	NATE-80	Critical DNS support [illegible] distributed [illegible] serv[illegible] [illegible]n files)		3	7			5.90			2	8				5.60
14	Configuration errors by privaleged users	NATE-90	[illegible] provisioning sy[illegible] registrars (the result be[illegible]'t add/change/delete zones from the [illegible] one way to do that, but there are others				4	6	1.80					7	1		2.75
15																	
16	Business failure of a key provider	NATE-10	Disrupts a "major" zone file (.COM/.NET/.UK/.DE etc.)			7			5.00						7		1.00
17	Business failure of a key provider	NATE-20	Disrupts a "lesser" zone file (that is not outsourced to a major provider)				6		3.00		10	1					9.82
18	Business failure of a key provider	NATE-30	Root zone -- is published incorrectly	2	3	1			8.17					6			3.00
19	Business failure of a key provider	NATE-40	Root zone -- is not published	5	1	1			9.00						6	1	0.86
20	Business failure of a key provider	NATE-50	Disrupts the IANA zone file	6					10.00						7		1.00
21	Business failure of a key provider	NATE-60	Disrupts DNSSEC from a "Major" DNSSEC provider		6			1	7.00	2	3				1		7.75
22	Business failure of a key provider	NATE-70	Disrupts DNSSEC for a TLD zone						#####								#####

Participants

Attendees (1)

- Hosts (1)
  - *Mike O'Connor*
- Presenters (0)
- Participants (0)

Threat sources -- range of effects

10 -- sweeping, involving almost all of the cyber resources of the DNS
8 -- extensive, involving most of the cyber resources of the DNS
5 --wide-ranging, involving a significant portion of the cyber resources of the DNS
3 --limited, involving some of the cyber resources of the DNS
1 -- minimal, involving few if any of the cyber resources of the DNS

Threat events -- relevance

10 - Confirmed -- Seen by the organization
8 - Expected -- Seen by the organization's peers or partners
5 - Anticipated -- Reported by a trusted source
3 - Predicted -- Predicted by a trusted source
1 - Possible -- Described by a somewhat credible source
0 - Not applicable (check after call)

Agenda

DSSA Working Group 26 January 2012
Agenda

-- Roll call and update SOI's
-- Approach
-- Architecture
-- Analysis -- Threat Sources (Tables D-7 & D-8)
-- Any other business (AOB)

Definitions

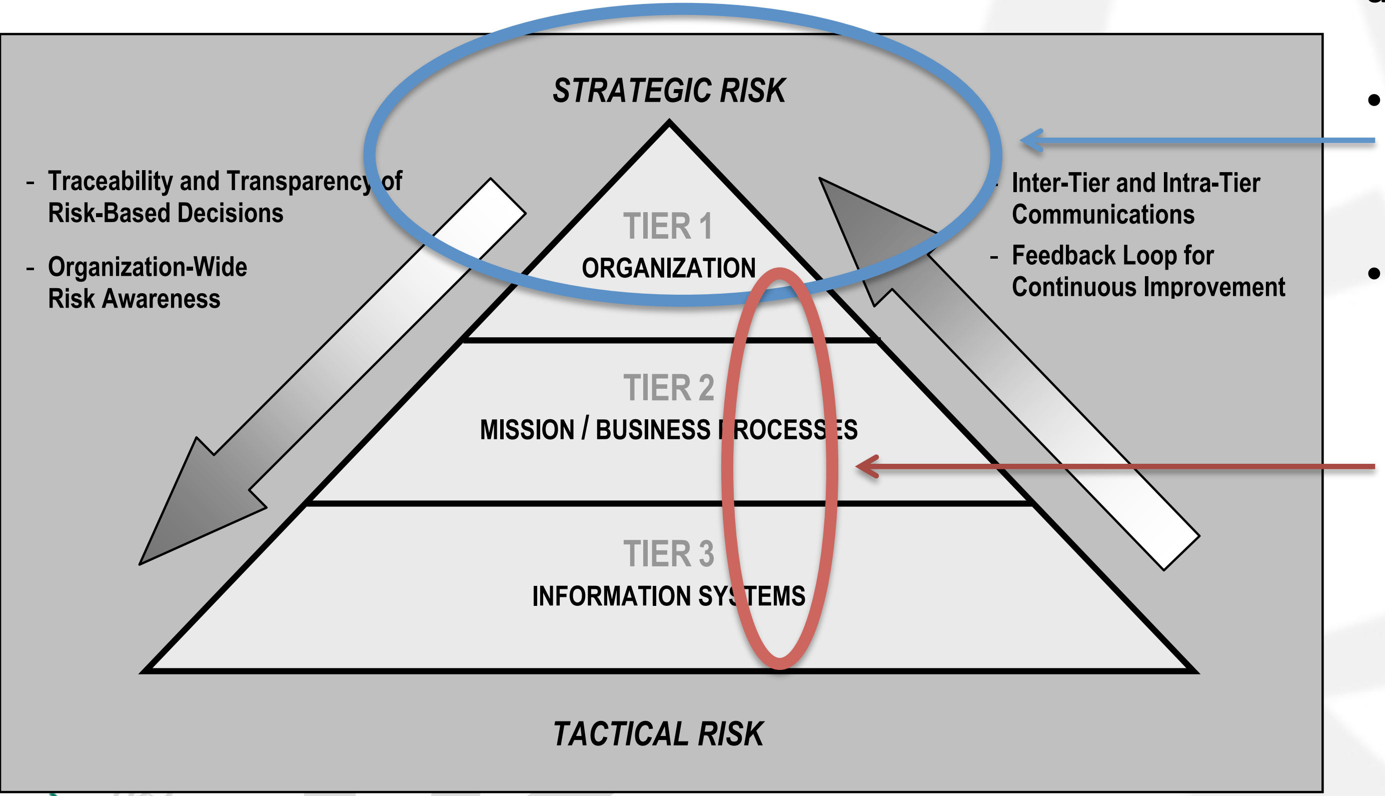
Agenda

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

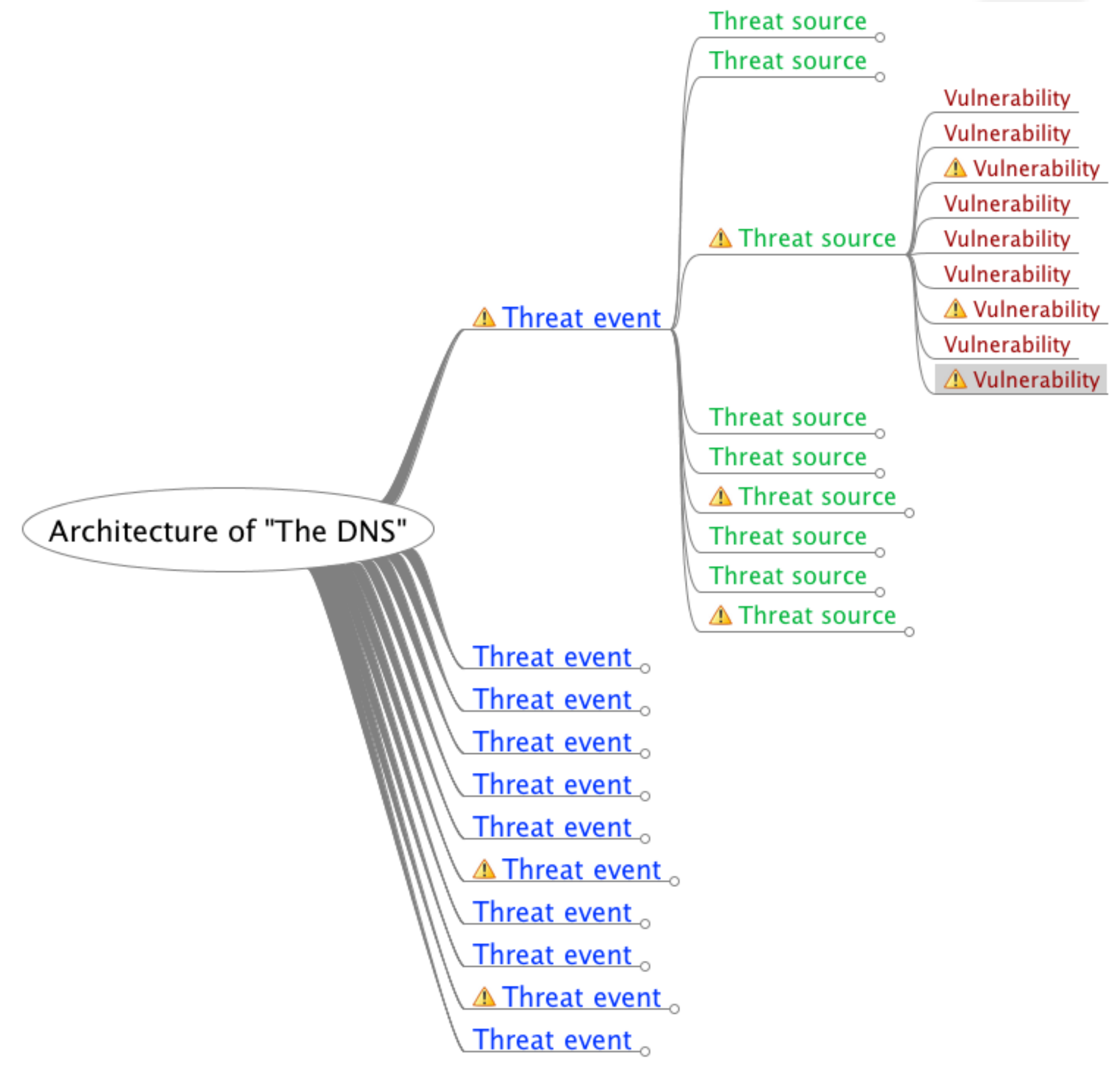
Risk Management Hierarchy


STRATEGIC RISK
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement

The methodology presumes a tiered approach to the work

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

Problem: the evaluation per NIST methodology does not scale



Architecture of "The DNS"

⚠ Threat event

Threat source

Threat source

⚠ Threat source

Vulnerability

Vulnerability

⚠ Vulnerability

Vulnerability

Vulnerability

Vulnerability

⚠ Vulnerability

Vulnerability

⚠ Vulnerability

Threat source

Threat source

⚠ Threat source

Threat source

Threat source

⚠ Threat source

Threat event

Threat event

Threat event

Threat event

Threat event

⚠ Threat event

Threat event

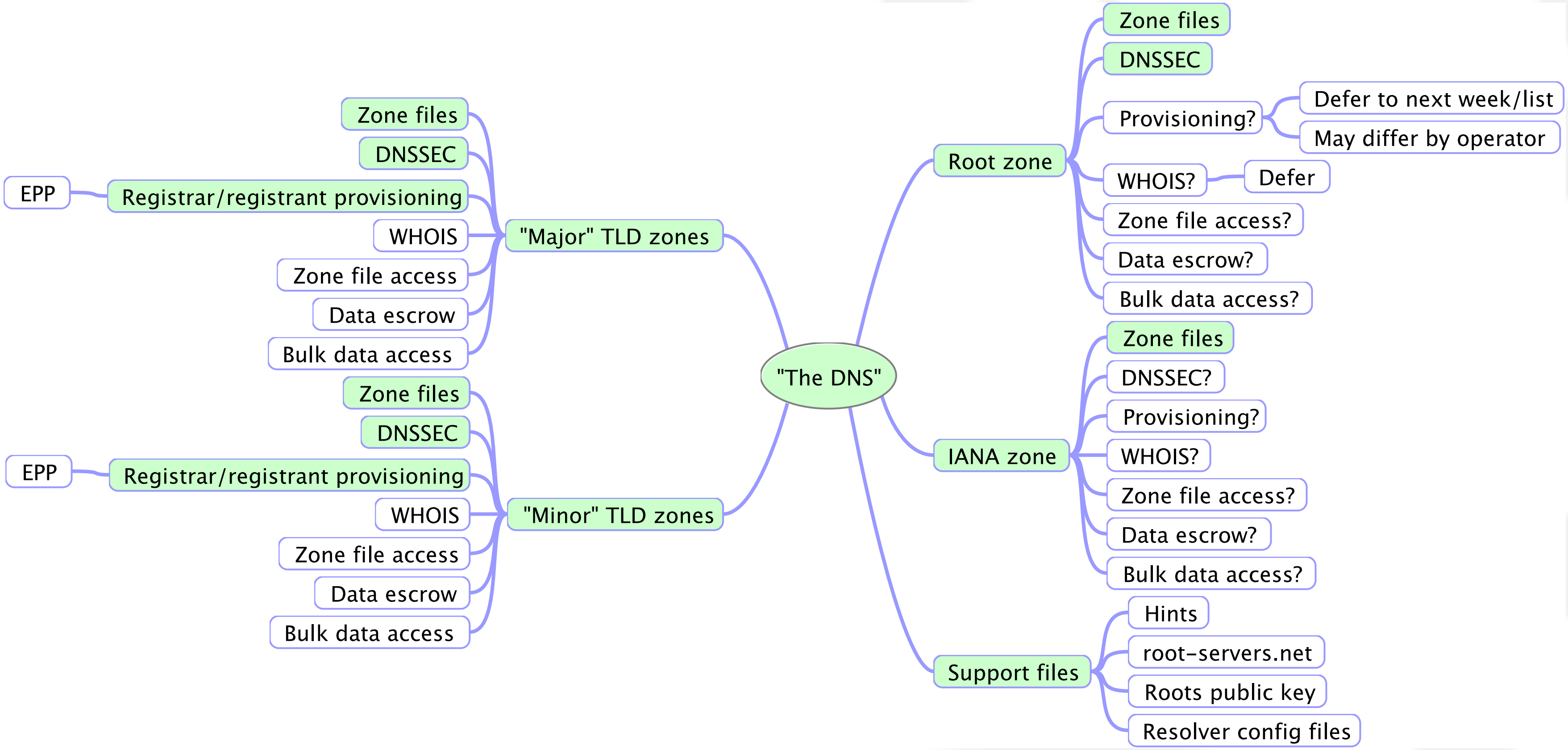
Threat event

⚠ Threat event

Threat event

- 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

Architecture



"The DNS"

"Major" TLD zones
- Zone files
- DNSSEC
- Registrar/registrant provisioning
  - EPP
- WHOIS
- Zone file access
- Data escrow
- Bulk data access

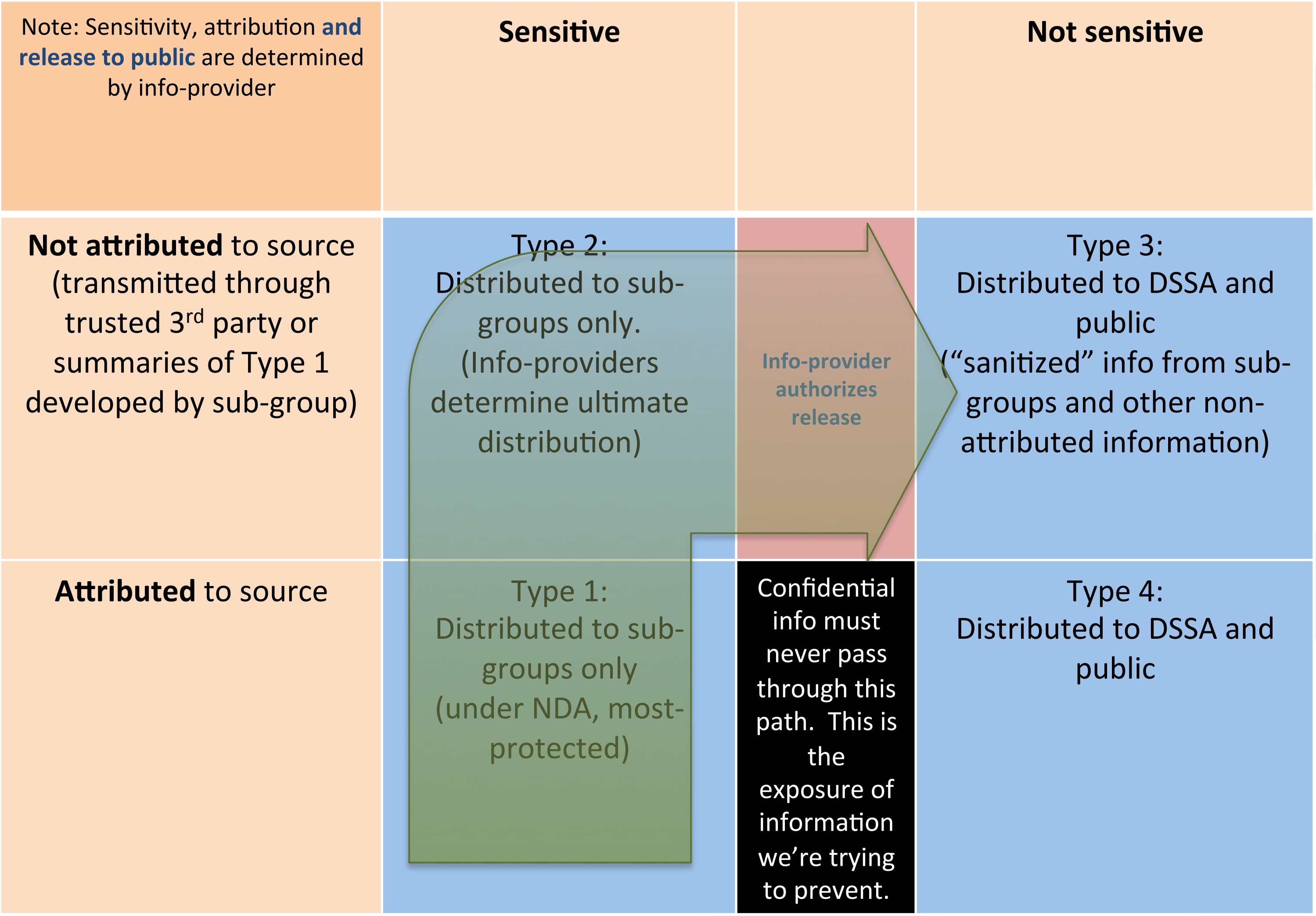
"Minor" TLD zones
- Zone files
- DNSSEC
- Registrar/registrant provisioning
  - EPP
- WHOIS
- Zone file access
- Data escrow
- Bulk data access

Root zone
- Zone files
- DNSSEC
- Provisioning?
  - Defer to next week/list
  - May differ by operator
- WHOIS?
  - Defer
- Zone file access?
- Data escrow?
- Bulk data access?

IANA zone
- Zone files
- DNSSEC?
- Provisioning?
- WHOIS?
- Zone file access?
- Data escrow?
- Bulk data access?

Support files
- Hints
- root-servers.net
- Roots public key
- Resolver config files

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