DSSA Update

Costa Rica – March, 2012

Goals for today

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

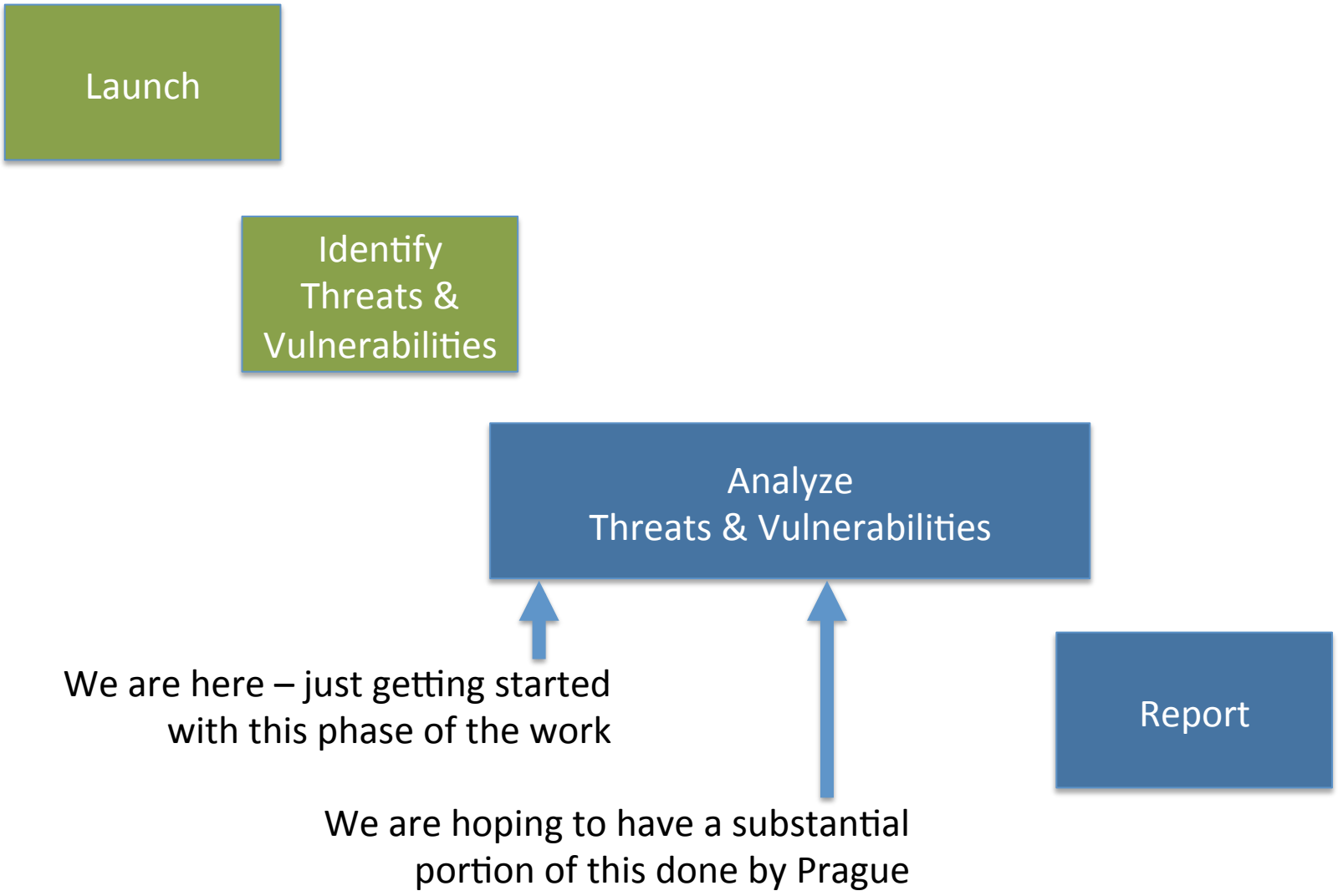
Goals and Objectives

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)

Where we are…

Approach and status



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)
  - It's available in English

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 we feel it may be useful to pursue one or two deeper, narrower analyses of specific threats once our "survey" work is complete

Where we're going

Analysis phase – based on NIST methods

Assess threat sources and events

Threat sources – broad range of impact, high capability, strong intent, targeting the DNS?
Threat events – relevant to the DNS?

Assess vulnerabilities and predisposing conditions

Vulnerabilities – severe?
Predisposing conditions – pervasive?

Determine likelihood

High likelihood that a threat-event will be initiated?
High likelihood that a threat-event will result in an adverse impact?

Determine level of impact

Broad harm/consequence from a threat-event – operations, assets, individuals, other organizations, world?
Severe impact of a threat-event?

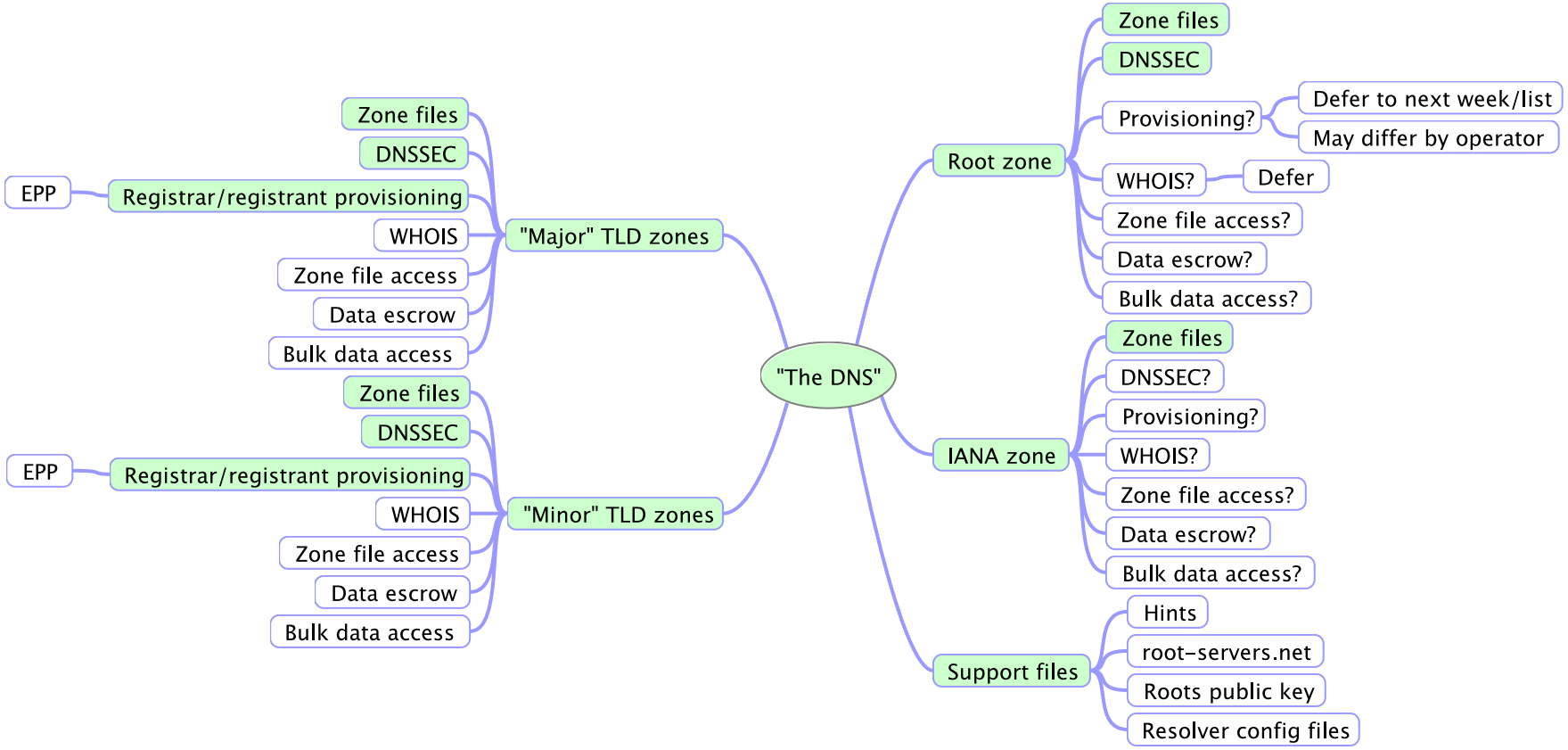
Determine risk

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

Activity since Singapore

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

Architecture



Non-adversarial threat **events**

(Question: relevance to “the DNS”)

NATE-10	Disrupts a "major" zone file (.COM/.NET/.UK/.DE etc.)
NATE-20	Disrupts a "lesser" zone file (that is not outsourced to a major provider)
NATE-30	Root zone -- is published incorrectly
NATE-40	Root zone -- is not published
NATE-50	Disrupts the IANA zone file
NATE-60	Disrupts DNSSEC from a "Major" DNSSEC provider
NATE-70	Disrupts DNSSEC for a TLD zone
NATE-80	Disrupts Critical DNS support files
NATE-90	Disrupts provisioning systems between registries and registrars (the result being that registrars can't add/change/delete zones from the TLD)

Scale: Table E-4 -- Relevance to the organization

- 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 -- N/A -- Not currently applicable

Non-adversarial threat **sources**

(Question: what is the range of impact?)

NATS - 10	Configuration errors by privaleged users
NATS - 20	Business failure of a key provider
NATS - 30	Nation state -- interventions with accidental or unintended consequences
NATS - 40	Key storage, processing or network hardware failure
NATS - 50	Key networking or operating-system software failure
NATS - 60	General-purpose application software failure
NATS - 70	Mission-specific software failure (WHOIS, EPP/ RPP, Billing)
NATS - 80	Root scaling
NATS - 90	Natural disaster (flood, tsunami, earthquake
NATS - 100	Widespread telecommunications infrastructure failure
NATS - 110	Widespread power infrastructure failure

Scale: Table D-6 -- Range of impact

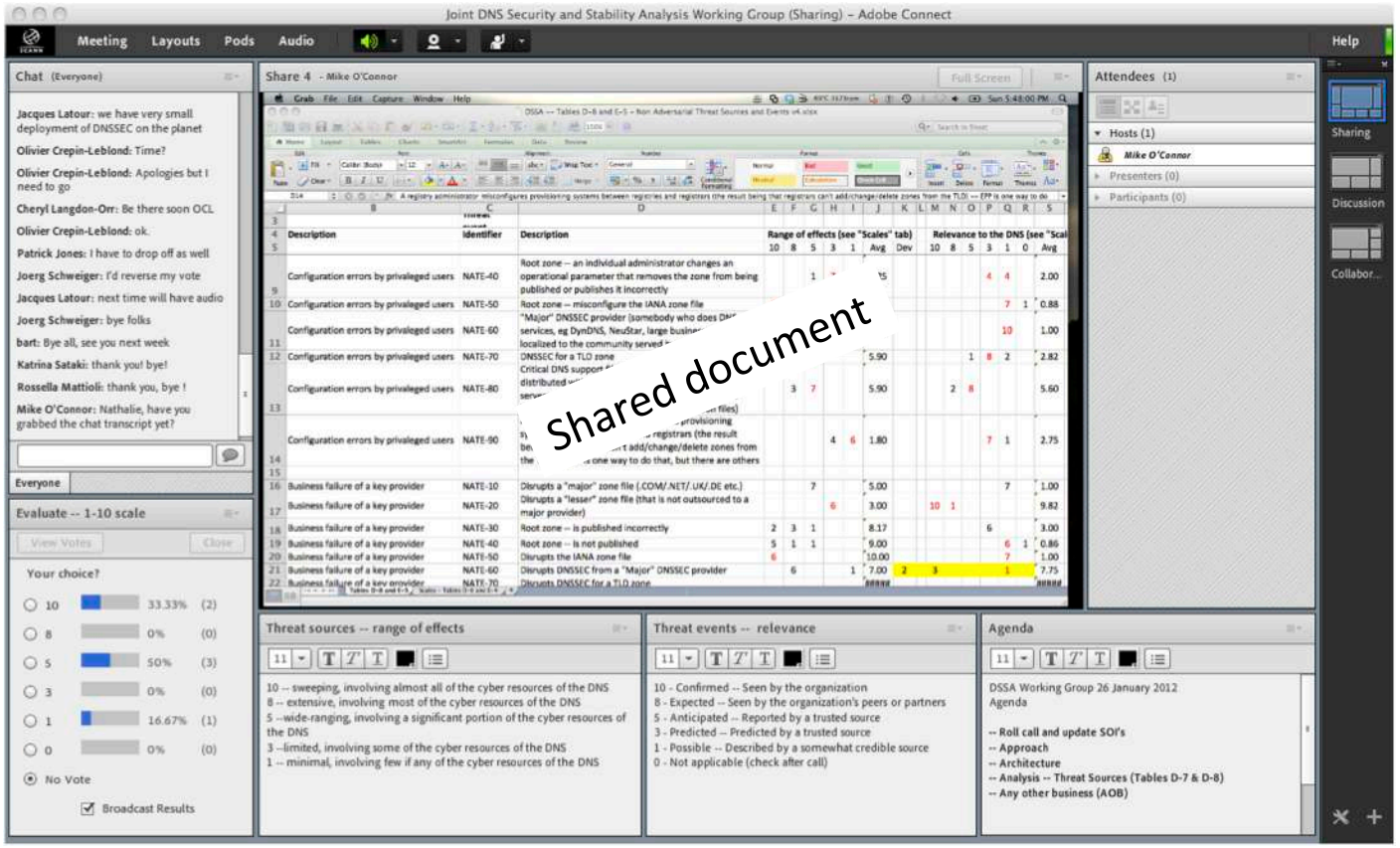
- 10 -- sweeping, involving almost all of the cyber resources of the DNS
- 8 -- extensive, involving most of the cyber resources of the DNS
- 5 --wide-ranging, involving a significant portion of the cyber resources of the DNS
- 3 --limited, involving some of the cyber resources of the DNS
- 1 -- minimal,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

How we work

(design credit -- CLO)

Live chat

Voting



Participants

Definitions

Agenda

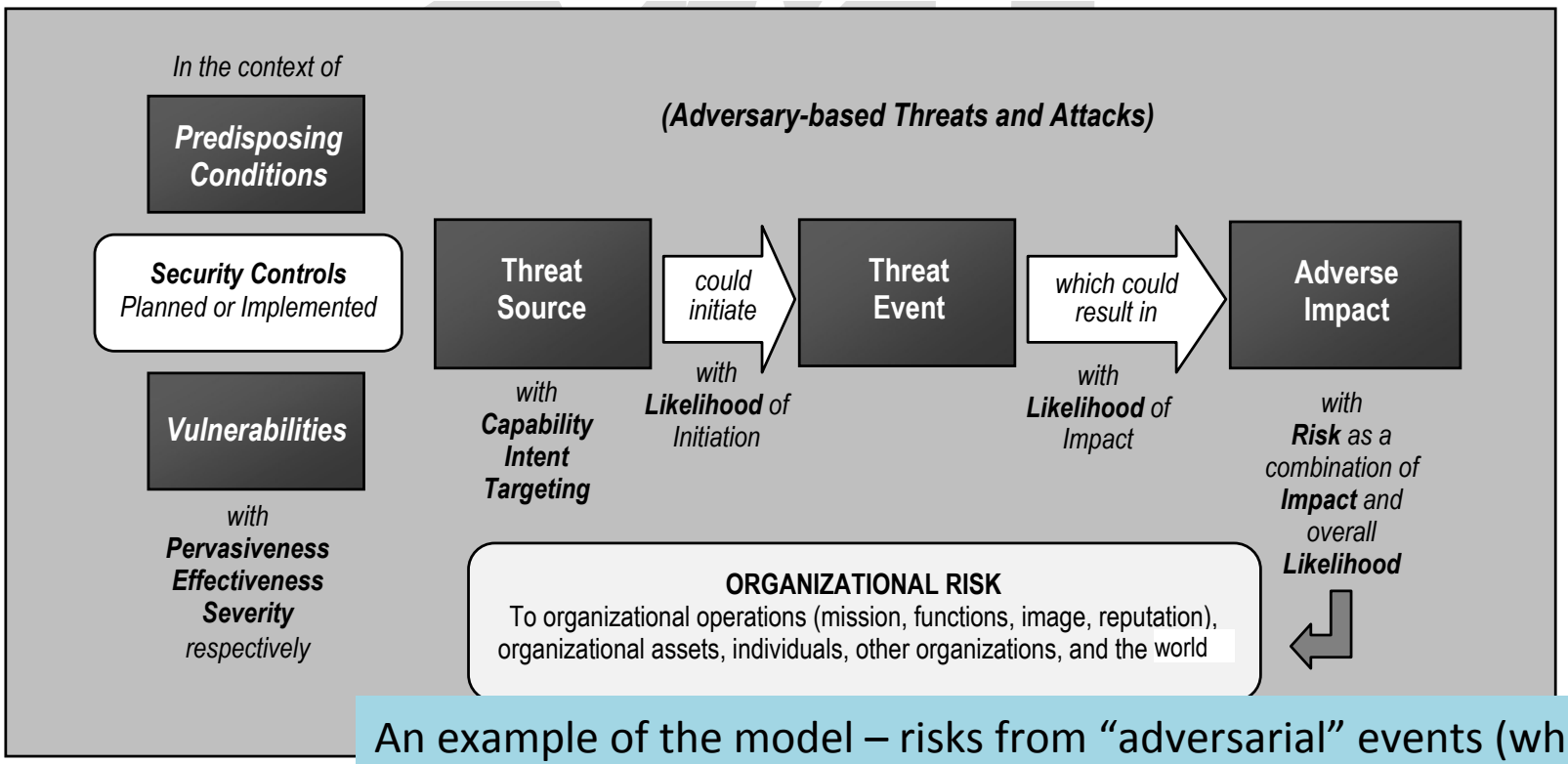
Questions?

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

Adversarial Risk Model



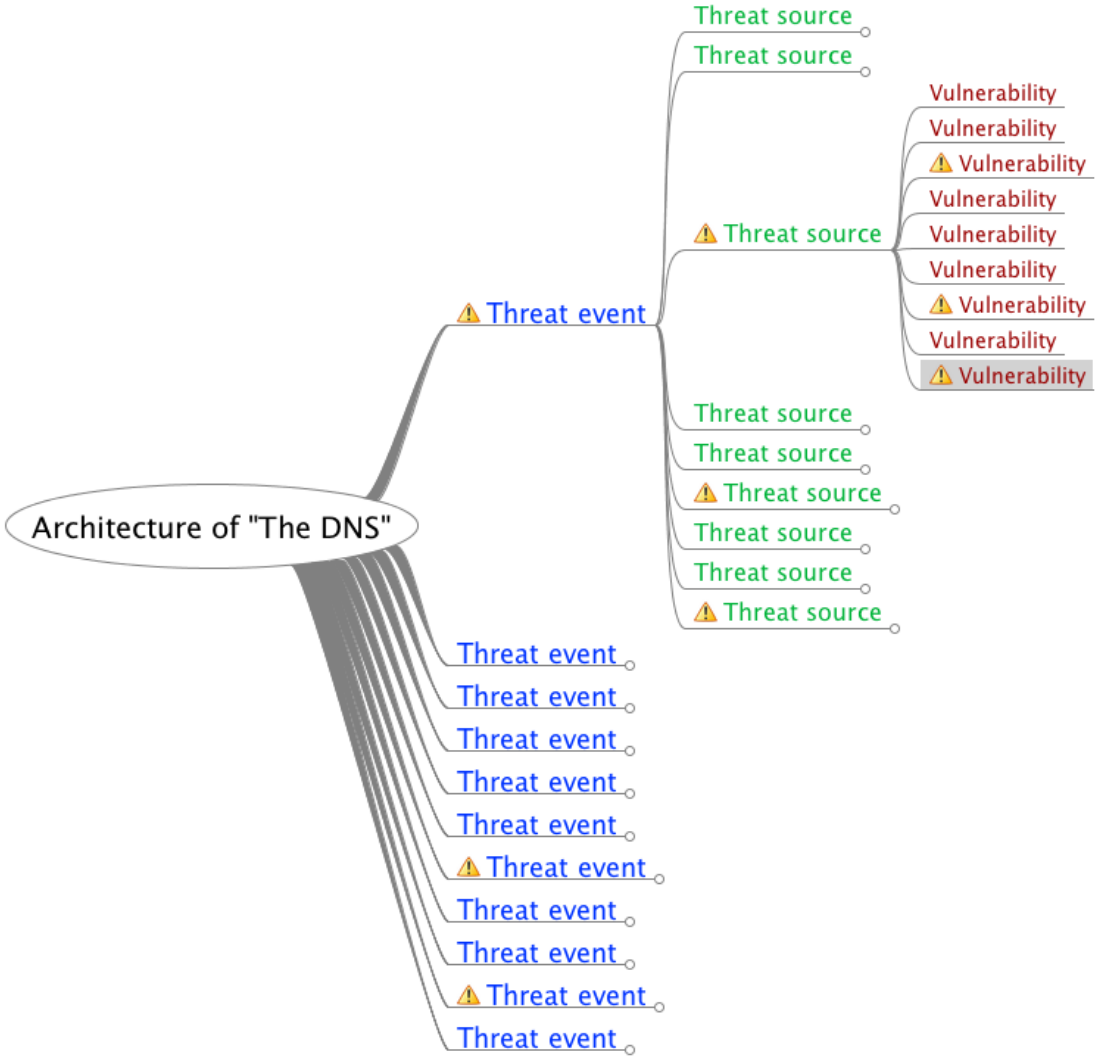
An example of the model – risks from "adversarial" events (which differs from "non-adversarial" threats such as errors, accidents, etc.)

Benefits:

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

Problem: the evaluation per NIST methodology does not scale

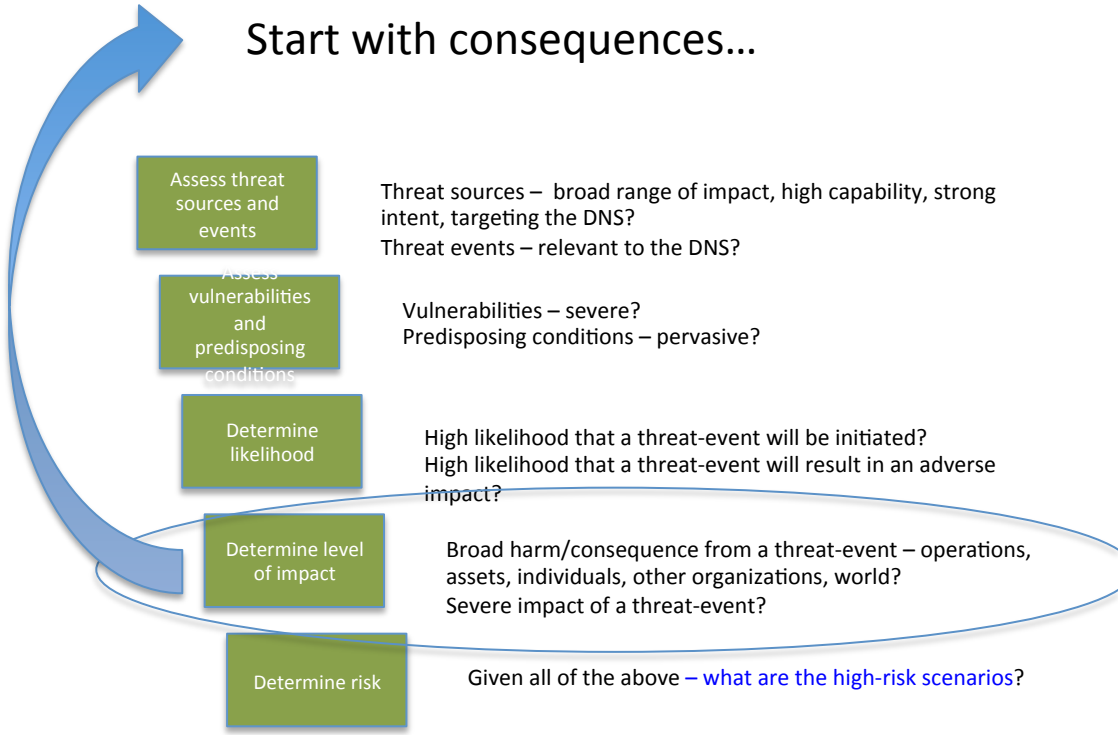
It's all about choices



- 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

Possible solution: re-sequence the work

- Start with consequences
- Evaluate the severity
- Concentrate on the most severe (e.g. loss of trust in DNS)
- Evaluate only those branches of the threat tree that lead to those outcomes



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