DNS Security and Stability Analysis Working Group (DSSA)

*DSSA Update*

*Toronto – October, 2012*
Context

STRATEGIC
Cross-community collaboration

LONG-TERM

IMMEDIATE

EDGE
“Regional” or “segment” focus

GLUE

CORE

Ecosystem-wide

Need: Provider or organization-focused risk
Need: coordination, fast response

TACTICAL
DNS providers are at the forefront

Framework

Creating RISK to users and providers of the DNS – a combination of the nature of the impact and the likelihood that its effects will be felt

Risk Scenario Topic List

Gaps in policy, management, or leadership splits the root
“Reductive” forces (security, risk-mitigation, control through rules, etc.) splits the root
Widespread natural disaster brings down the root or a major TLD
Attacks exploiting technical vulnerabilities of the DNS bring down the root or a major TLD
Inadvertent technical mishap brings down the root or a major TLD

Research & Analysis
Standards, Tools, Techniques
Education, Training, Awareness
Technology Selection, Deployment & Management
Operational & Technical Practices and Controls

Security Management/Leadership
Risk Planning
Risk Assessment

Glue
Regional or segment focus
Constituencies

Core
Ecosystem-wide Collaborative
Governance
Steering

Coordination
Sharing

Edge (internal)
Within the organization

Edge (external)
Cross-organizational

Incident Response
Event Monitoring
Compliance Monitoring
Technology Selection, Deployment & Management
Operational & Technical Practices and Controls

Need:
models, tools, support, direction

http://toronto45.icann.org/node/34225
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.
The DSSA has:

- Established a cross-constituency working group
- Clarified the scope of the effort
- Developed a protocol to handle confidential information
- Built a risk-assessment framework
- Developed risk scenarios
- Documented this work in a report
Since Prague:

• Refined and consolidated
• Launched public-comment cycle

Still to come (if needed)

• Refine the methodology
• Introduce the framework to a broader audience
• Complete the risk assessment
Methodology

Creating RISK to users and providers of the DNS – a combination of the nature of the impact and the likelihood that its effects will be felt.
STRATEGIC
Cross-community collaboration

Risk Scenarios

LONG-TERM

Ecosystem-wide

Gaps in policy, management, or leadership splits the root

“Reductive” forces (security, risk-mitigation, control through rules, etc.) splits the root

Widespread natural disaster brings down the root or a major TLD

Attacks exploiting technical vulnerabilities of the DNS bring down the root or a major TLD

Inadvertent technical mishap brings down the root or a major TLD

IMMEDIATE

“Regional” or “segment” focus

Need: coordination, fast response

TACTICAL

DNS providers are at the forefront

Need: models, tools, support, direction

Provider or organization-focused risk

EDGE

CORE

GLUE

Risk Scenario
Topic List
Roles and context

- **Glue**
  - Regional or segment focus
  - Constituencies

- **Core**
  - Ecosystem-wide
  - Collaborative

- **Steering**
  - Governance

- **Sharing**
  - Coordination

- **Doing**
  - Delivery

- **Incident Response**
  - Event Monitoring

- **Compliance Monitoring**
  - Risk Assessment
  - Risk Planning

- **Security Management/Leadership**

- **Risk**

- **Technology Selection, Deployment & Management**

- **Operational & Technical Practices and Controls**

- **Research & Analysis**

- **Standards, Tools, Techniques**

- **Education, Training, Awareness**

- **Edge (internal)**
  - Within the organization

- **Edge (external)**
  - Cross-organizational
Question: Who is doing what?

- Backend registry providers
  - Security Team
  - ICANN SOs and ACs
- ccTLD registries
- CERTs
- DNRMF
- DNS-OARC
- ENISA
- FIRST
- ISPs
- Network Operator Groups
  - NRO
  - RSAC
  - SSAC
  - And ???
- gTLD registries
- IANA
- ICANN

Research & Analysis
- Standards, Tools, Techniques

Edge (internal)
- Within the organization
- Education, Training, Awareness

Edge (external)
- Cross-organizational
- Technology Selection, Deployment & Management
- Operational & Technical Practices and Controls

Glue
- Regional or segment focus Constituencies
- Governance
- Steering
- Coordination
- Sharing
- Delivery
- Doing
- Incident Response

Core
- Ecosystem-wide Collaborative

Security Management/Leadership
- Risk Planning
- Risk Assessment
- Compliance Monitoring
- Event Monitoring

Educa<on, Training, Awareness
- Standards, Tools, Techniques

Standards, Tools, Techniques
- Risk Planning
- Risk Assessment
- Compliance Monitoring
- Event Monitoring
Approach: a data-gathering worksheet

Goal: complete the map of DNS SSR functions and participants for our report - and provide a foundation for a “gaps and overlaps” analysis.
Approach: Coordinate DSSA and DNSRMF

DNRMF scope – Risk Management Framework

1) Build scenarios
   - Identify threats
   - Describe predisposing conditions

2) Identify gaps
   - Analyze controls
   - Determine likelihood
   - Determine risk

3) Evaluate risk
   - Analyze
   - Determine likelihood
   - Determine risk

DSSA scope – risk assessment

Assess

Risk Planning

Mitigate

Assume the risk
Avoid the risk
Transfer the risk
Limit the risk

Monitor

Compliance and Activity-Monitoring
Refine and consolidate

ID roles – gaps & overlaps

Public comment

Gather comments and feedback

Revise report and obtain AC/SO endorsement

Obtain community feedback and incorporate those suggestions into the RM framework

Determine whether separate DSSA risk-assessment effort is needed

Establish community-based portion of RM launch project

Align/Integrate DNSRMF and DSSA findings/methods/leadership

Select DNS risk-management framework consultant and launch DNSRMF project

Complete DNS risk-management framework

Launch the project to establish the RM function and complete one “cycle”
How you can help

• Comment on our Phase I report

• Fill out one of our “Gaps & Overlaps” worksheets

• Comment on our plans going forward

https://community.icann.org/x/4AB5