DNS Security and Stability Analysis Working Group (DSSA)

DSSA Update
Prague – June, 2012
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
The DSSA will:

- Complete risk assessment
- Refine methodology
- Introduce framework to a broader audience
Scope: DSSA & DNRMF

The Board DNS Risk Management Framework working group

DNRMF scope – Risk Management Framework

1) Build scenarios
   - Identify threats
   - Identify vulnerabilities
   - Describe predisposing conditions

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

3) Evaluate risk
   - Evaluate risk
   - Determine risk

Risk Planning
- Assume the risk
- Avoid the risk
- Transfer the risk
- Limit the risk

Compliance and Activity-Monitoring

Assess
Mitigate
Monitor
Scope: DSSA & DNRMF

The DSSA is focusing on a subset of that framework

DNRMF scope – Risk Management Framework

1) Build scenarios
   - Identify threats
   - Describe predisposing conditions

2) Identify gaps
   - Analyze controls
   - Determine likelihood

3) Evaluate risk
   - Determine risk

Assess

Mitigate

Monitor

Risk Planning

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

Compliance and Activity-Monitoring

Scope: DSSA & DNRMF

The DSSA is focusing on a subset of that framework
Scope: DSSA in a broader context

DSSA is a part of a much larger SSR ecosystem that includes:

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

All other – including front-line mitigation...

Education, Training, Awareness

Monitoring

Risk Assessment

Risk Planning

Core
Ecosystem-wide
Collaborative

Edge
Organization-focused risk
Providers/Consumers

Glue
Regional or segment focus
Constituencies

Standards, Tools, Techniques
“Compound Sentence” Risk Assessment Framework

Based on NIST 800-30 standard

Tailored to meet unique ICANN requirements

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
“Compound Sentence” Risk Assessment Framework

An adversarial threat-source (with capability, intent and targeting),

OR...

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.
A non-adversarial threat-source (with a range of effects)...

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.
“Compound Sentence” Risk Assessment Framework

In the context of:

Predisposing conditions (with varying pervasiveness)...

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.
"Compound Sentence” Risk Assessment Framework

... Security controls (both planned and implemented), and...

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
“Compound Sentence” Risk Assessment Framework

Vulnerabilities (that range in severity)...

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.
“Compound Sentence” Risk Assessment Framework

... Could initiate (with varying likelihood of initiation)

a Threat Event which (with varying likelihood of impact) could result in...

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.
Adverse impacts (with varying severity and range)...

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.
All of which combined create 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.

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.
Findings: 5 Broad Risk Scenarios

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

LONG-TERM

Ecosystem-wide

“Regional” or “segment” focus

IMMEDIATE

GLUE

CORE

STRATEGIC
Cross-community collaboration

TACTICAL
DNS providers are at the forefront

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

Need: models, tools, support, direction

No. 44 - 24 - 29 JUNE 2012
Findings: 5 Broad Risk Scenarios

Gaps in policy, management or leadership splits the root

Risk Scenario Topic List

- “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

Need: coordination, fast response
Need: models, tools, support, direction
Provider or organization-focused risk
Findings: 5 Broad Risk Scenarios

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

- **Findings:** 5 Broad Risk Scenarios
  - "Reducive" forces (security, risk-mitigation, control through rules, etc.) splits the root
  - Long-term
    - GLUE
      - Need: provider or organization-focused risk
    - EDGE
      - Need: coordination, fast response
    - CORE
      - Need: models, tools, support, direction
  - Strategic
    - Cross-community collaboration
  - Risk Scenario Topic List
    - Gaps in policy, management, or leadership 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

- **Long-term**
  - **CORE**
  - **GLUE**
  - **EDGE**

- **Strategic**
  - Cross-community collaboration

- **Tactical**
  - DNS providers are at the forefront
Findings: 5 Broad Risk Scenarios

Widespread natural disaster brings down the root or a major TLD

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
- 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

Need: coordination, fast response
Need: models, tools, support, direction

Widespread natural disaster brings down the root or a major TLD
Findings: 5 Broad Risk Scenarios

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

- Attacks exploiting technical vulnerabilities of the DNS bring down the root or a major TLD
- 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
- Inadvertent technical mishap brings down the root or a major TLD

Risk Scenario Topic List:

- Attacks exploiting technical vulnerabilities of the DNS bring down the root or a major TLD
- 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
- Inadvertent technical mishap brings down the root or a major TLD
Findings: 5 Broad Risk Scenarios

Inadvertent technical mishap brings down the root or a major TLD

Reasons for root splits: Gaps in policy, management, or leadership splits the root

Ecosystem-wide "Reductive" forces (security, risk-mitigation, control through rules, etc.) splits the root

"Regional" or "segment" focus Widespread natural disaster brings down the root or a major TLD

Provider or organization-focused risk Attacks exploiting technical vulnerabilities of the DNS bring down the root or a major TLD

Need: coordination, fast response

Need: models, tools, support, direction

Inadvertent technical mishap brings down the root or a major TLD
Findings: 5 Broad Risk Scenarios

Question: Have we missed an important topic?

NOTE: If you want to share embarrassing ideas, contact Paul Vixie (paul@vix.com)

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
Next phase

“Go deep” into the five risk topics

- **Strategic**
  - Cross-community collaboration

- **Ecosystem-wide**
  - "Regional" or "segment" focus

- **Immediate**
  - Coordination, fast response
  - Provider or organization-focused risk

- **Tactical**
  - DNS providers are at the forefront

**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

**Next phase**

"Go deep" into the five risk topics

- Models, tools, support, direction

**Need:**

- Coordination, fast response
Next phase

“Go deep” into the five risk topics

Refine by doing
Next phase

“Go deep” into the five risk topics

Refine by doing

Finish assessment

1. Refine tools by doing one in detail
   Build and validate the tools

2. Finish assessment
   Demo the tools and reduce cycle time

需要：模型，工具，支持，方向

需：协调，快速响应

风险场景

- 在政策，管理，或领导层分歧时，生态系统中的根源问题
- "减损" 应对（安全，风险管理，控制等）分裂了根
- 广泛的自然灾害导致根或主顶级域的崩溃
- 意外的技术失误导致根或主顶级域的崩溃
- 攻击利用DNS的漏洞导致根或主顶级域的崩溃

长远

近期

长期

短期

需要：提供商或组织专注于风险

ICANN Prague 2012
Questions?
Are we on the right track?
Have we missed something important?

![Diagram of DNRMF scope – Risk Management Framework](image)

**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

**Risk Planning**

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

**Mitigate**

- Compliance and Activity-Monitoring

**Assess**

- Standards, Tools, Techniques
- Education, Training, Awareness

**Monitoring**

- All other – including front-line mitigation...

---

![ICANN PRAGUE No. 44 - 24 - 29 JUNE 2012](image)