
**ICANN** NO. 51 | 12-16 OCTOBER 2014

LOS ANGELES

*#ICANN51*

14 October 2014

# DNS Risk Framework Update

**John Crain & Jacks Khawaja**

Chief SSR Officer; Enterprise Risk Director

# Agenda

- History
- Moving Forward

# History

# Defined Resiliency Model

OBJECTIVES

IDIOSYNCRATIC RISK

HAZARD | OPPORTUNITY COST

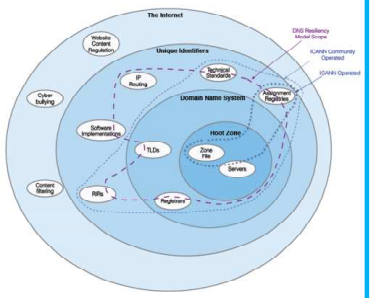
SYSTEMATIC RISK

HAZARD | OPPORTUNITY COST | LEVEL 1 | LEVEL 2

SYSTEMIC AMPLIFIERS / ATTENUATORS (CONDITIONING, CONSTRAINING, ENABLING)

**SYSTEM OBJECTIVES:**

**AVAILABILITY, CONSISTENCY, INTEGRITY**



**RESPONSIBLE PARTIES**

**ASSETS**

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**A. SYSTEMS & NETWORKS**

- 1.Denial Of Service
- 2. IP Transition
- 3. DNS Resolving
- 4. Software Corruption
- 5. Cryptographic Key Compromise

**B. INFORMATION ASSETS**

- 6. Cache Poisoning
- 7. Response Modification
- 8. Route Leakage
- 9. Route Interception

**C. IT EQUIPMENT, SERVICE PROVIDERS**

- 10. Hardware Failure
- 11. Business Disruption / Systems Failure
- 12. Registration Services Performance
- 13. Root / TLD Operator Performance
- 14. IANA / ICANN Service Disruption
- 15. Technology Vendor Failure

**D. PEOPLE**

- 16. Root Operator Coercion
- 17. Fraud

**E. PHYSICAL**

- 18. Root / TLD attack
- 19. Physical Damage to (DNS) Physical or Digital Assets

**F. PROGRAM**

- 20. IDN gTLD Delegation
- 21. Technical / Policy conflict

**G INNOVATION**

- 22. Technical
- 23. Business Model

**SYSTEMIC AMPLIFIERS / ATTENUATORS (CONDITIONING, CONSTRAINING, ENABLING)**

1. SCIENTIFIC UNKNOWNS
2. LOSS OF SAFETY MARGINS
3. POSITIVE FEEDBACK
4. VARYING SUSCEPTIBILITIES TO RISK
5. CONFLICTS ABOUT INTERESTS, VALUES, SCIENCE
6. SOCIAL DYNAMICS
7. TECHNOLOGICAL ADVANCES
8. TEMPORAL COMPLICATIONS
9. COMMUNICATION
10. INFORMATION ASYMMETRIES
11. PERVERSE INCENTIVES
12. MALICIOUS MOTIVES AND ACTS

Source: International Risk Governance Council (IRGC)

# CONSULTATION PAPER

## ICANN – DNS RISK ASSESSMENT

### Purpose

The purpose of this document is to:

- Brief the ICANN Community on the approach used in an initial assessment of DNS risks; and
- Through a process of consultation at ICANN 50, receive feedback to help further refine the approach prior to subsequent rounds of engagement with the wider Community in a more broad-based assessment of DNS risks.

### Background

In November 2013 at ICANN 48 in Buenos Aires, the ICANN Board adopted the ICANN DNS Risk Management Framework ("Framework") and in February 2014 a group of selected ICANN staff undertook an initial (limited scope) DNS risk assessment using the Framework.

The initial DNS risk assessment was intended to serve as a pilot, with a focus on features that would help ensure it remains durable (practical, dynamic and adaptable) and 'fit-for-purpose' given the evolutionary nature of the Internet and ICANN's multi-stakeholder model.

The results were presented to the ICANN Board Risk Committee at ICANN 49 in Singapore and comprised of:

# 23 Risks Defined

## CONSULTATION PAPER

### ICANN – DNS RISK ASSESSMENT - RISK DEFINITIONS

ICANN

**Explanatory**

- The following table should be read in conjunction with the accompanying Consultation Paper (DNS Risk Assessment).
- It provides brief definitions and accompanying explanations of the systematic risks referred to in the DNS Resilience Model.

| # | Risk: | Impacted assets: | Description: | Additional explanation / examples |
|---|---|---|---|---|
| 1 | Denial of Service | Systems and Networks | An incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Typically, the loss of service is the inability of a particular network service to be available or the temporary loss of all network connectivity and services.<br>A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems (compromised or otherwise) are used to attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. Can take 2 forms:<br>• *Resource Depletion* where resources are consumed nearly entirely by the requests from attackers and insufficient resources (such as Internet bandwidth, server CPU, or memory) are available to provide services.<br>• *Resource Disruption* where an event makes | An attacker floods the network with traffic, blocking reliable transmission of DNS requests and replies; attacker is able to disrupt normal operations of routers or switches.<br>Exploitation of a software vulnerability causes a server to fail.<br>Power failure (intentional or accidental); attacker is able to crash DNS servers. |

# Moving Forward

# Numbers

- Examining Risk
  - Typically, step 1 = identify assets
  - Impractical to identify all individual elements of DNS
- Our Approach

**Categorize assets by sphere of influence**

# Where can ICANN:

Implement

Directly Influence

Indirectly Influence

?

# Assets directly controlled by ICANN

- Assets that ICANN directly manages or contracts to third parties (Example: XXX, XXX)
- ICANN's own corporate infrastructure
- External-facing services such as websites and request management systems
- DNS infrastructure of L.root-servers.net
- Others?

# Assets directly influenced by ICANN

- Assets that ICANN can influence through contractual agreements (Example: Service Level Agreements, etc.)
- Registries or registrars are guided by contracts that include Service Level Agreements
- It is their remit as the asset owners to decide how they meet those SLAs and how to implement mitigation of their risks

# Assets outside ICANN's realm

- The Internet is a "network of networks" and each operator of a network or service is ultimately responsible for their own risk management
- ICANN and the community can indirectly influence these through outreach and awareness efforts
- ISOC's Deploy360 is an excellent example of this

# SSR-001 DDOS (Example)

# SSR001 Description (abridged)

- User or organization deprived of service(s) or resource(s) they would normally have
- Distributed denial-of-service (DDoS) attack:
  - Multitude of systems (compromised or otherwise) are used to attack a single target
  - Flood of incoming messages to the target system essentially forces it to shut down. This can take two forms:
    - Resource Depletion
    - Resource Disruption

# What is the Risk?

- This risk discusses the probability that parts of the DNS could be disabled for a sustained period
- To ascertain the likelihood or the effect of such an attack, it's important to first define the assets that are affected. This is also critical to understanding who owns the risk and who is able to best mitigate such risks

# Look at DNS Assets from Both Sides

- Publish the data on the authoritative servers (root servers, TLD servers, and registrants servers)
- Query the data on the recursive servers (ISP's, corporations, and DNS service providers)

# Assets directly controlled by ICANN

**Authoritative**

- ICANN:
  - Operates L.root-servers.netICANN runs some infrastructure for TLDs (ARPA, int.)
  - Runs its own network DNS infrastructure

**Recursive**

- ICANN runs its own recursive servers for staff
- Risks to these are covered in ICANN's ERM

# Assets directly influenced by ICANN

## Authoritative

- ICANN has an advisory committee (RSSAC) that provides Service Level Recommendations for root servers
- (Upcoming RSSAC002)
- ICANN has contracts in place with many, but not all TLDs. Those contracts contain SLAs

## Recursive

- ??

# Assets outside ICANN's realm

**Authoritative**

- Registrants' DNS services

**Recursive**

- ISPs, corporations, homes and DNS service providers
- Should the community work together to influence these?
- We have SSAC and RSSAC that provide advice

# Can We Tackle the Root Causes?

There are many efforts underway to reduce the severity of DDoS attacks

- Source Address Validation (BCP38)
- Open Resolver project
- Botnet dismantling
- Others

**Should ICANN staff and community members play a more active role?**

# Going Forward

- For each of the 23 risks, we will:
  - Document assets
  - Identify existing mitigation strategies that are in place
  - Suggest areas where new or improved mitigation plans may be considered
- How do we involve community expertise?
  - Dedicated workshops?
  - Working Groups?
  - Other suggestions?

# GDD + Related Sessions

## Wednesday, 15 October

- GDD Service Delivery, Customer Service & Service Level Agreements
- Universal Acceptance

## Thursday, 16 October

- DNSSEC Key Rollover Workshop
- Thick WHOIS Implementation (Working Session)
- Deploying the IETF's WHOIS Replacement

# Engage with ICANN on Web & Social Media


twitter.com/icann


gplus.to/icann


facebook.com/icannorg


weibo.com/icannorg


linkedin.com/company/icann


flickr.com/photos/icann


youtube.com/user/ICANNnews


icann.org

ICANN