DNS Risk Management Framework WG Charter

ICANN 43

15 March 2012

Agenda

- Working group formation and charter
- Preliminary issues list
  - Definition of “the DNS” and map of the environment, potential risks
  - Business impact analysis, risks analysis, measures need to be in place to control the (largest) risks on critical services
  - Systemic risks associated with the diversity and possible fragility of entities in the DNS
  - Risks associated with DNSSEC
  - IPv6 readiness (and IPv4 transition)
  - State of new gTLD operational readiness

The Working Group

- Background on the DNS Risk Management Framework Working Group (Ray Plzak)
- Working Group members:
  - Bill Graham [chair]
  - Ray Plzak
  - Ram Mohan [SSAC liaison]
  - Suzanne Woolf (RSSAC liaison]
  - Patrik Fältström [SSAC Chair]
  - Bill Woodcock [CEO, Packet Clearing House]
  - Roelof Meijer [CEO, SIDN]

Work Plan

- Short-term project: done by Prague
- Intention to scope work, bootstrap a risk management framework
- Hand off to staff as an ongoing project
- Steps proposed:
  - Scoping study and budget (est. 9 April)
  - Public comment (9 April to 18 May)
  - Output workshop (~25 June, Prague)
  - Board approval (~29 June)
  - Transition to Board Risk Committee

For discussion: Issues list

1. Develop a definition of "the DNS" and map the entities that are part of the environment for the purposes of this Working Group.
2. Looking broadly at DNS security and stability issues (within and beyond ICANN), what are the greatest risks in the current environment?
   a) which of those are within ICANN's span of control?
   b) for those outside ICANN's span of control, are there entities that should be alerted to those risks?
   c) for those outside ICANN's span of control, are there any existing coordination mechanisms or organizations that have or can take responsibility?

Issues list (2)

3. Business impact analysis (what are the services most essential to ICANN's business with regard to the security and stability of the DNS)
4. Risks analysis (what are the risks that threaten those services)
5. What measures need to be in place to control the (largest) risks on critical services

Issues list (3)

6. Is the DNS software environment sufficiently robust to adequately deal with risks to the DNS?
   – are there systemic risks to the DNS due to having a single predominant DNS software implementation?
   – does the resource intensive nature of developing DNS software result in vulnerabilities? Are there other mechanisms that might address those challenges?
   – are adequate procedures (e.g. documentation, security testing, change & release management, (external) code review) incorporated in the development of DNS software?

Issues list (4)

7. Systemic risks associated with the diversity and possible fragility of entities in the DNS, including non-ICANN accredited entities.
   - registration vulnerability
   - name service robustness
   - compromise of personnel
   - incompatibility of policies
   - knowledge levels
   - anti-abuse procedures (or lack thereof)
   - international variation

Issues list 5

8. DNSSEC Deployment
    - risks from key management errors
    - knowledge levels (at registries, registrars, and levels below)

9. IPv6 readiness (and IPv4 transition)

10. New gTLD operational capability
    - is the current system of name servers able to handle anticipated growth of the Internet's naming system?

Discussion