Registry Internet Safety Group (RISG)

Re: Potential for Malicious Conduct and new TLD Process

- RISG's mission is to facilitate data exchange and promulgate best practices to address Internet identity theft, especially phishing and malware distribution.
- Members include:
  - registry operators Afilias (.INFO), NeuStar (.BIZ, .US), Nominet (.UK), The Public Interest Registry (.ORG), and SIDN (.NL);
  - security firms Cyveillance, Internet Identity, McAfee, and Symantec;
  - registrars GoDaddy.com, MarkMonitor, MelbourneIT, Network Solutions, and Oversee.net;
  - observers from law enforcement agencies.
- Following points are consensus statements from the above members. *Individual RISG members have varying opinions and positions on new TLD issues.*

RISG Approach to Abuse Issues

Create best practices that registries (and registrars) can adapt according to their needs and circumstances. Why?

- Registries face widely varying types,levels of domain name abuse.
- Registries legitimately have different business plans, and therefore different sales channels and registrant bases.
- Different types of abuse demand different responses.
- A registry must meet the restrictions & requirements of jurisdiction(s) in which it is based or operates, and other legal obligations.
- Registries and registrars can often choose different -- but effective -- ways to solve a particular problem.

Specific policies or implementations often can't be applied well across TLDs. Rather, each TLD can shape policies and procedures according to its needs, and share ideas about what works.

Scope

- Our opinion is that no one party -- and no one type of entity -- can fight the problem of e-crime alone. Collaboration, data sharing, and education are effective and important.
- ICANN is a very useful forum for parties to come together and pursue information exchange and education.
- The future is unknowable. But we can comment on trends and past experience.

Question 1

Increases in criminal activity associated with increase in domain names or TLDs?

- A TLD may become more of a target for criminals once it becomes accepted by and known to end-users.
- Criminals tend to migrate from TLD to TLD (and registrar to registrar) over time. This happens in the 200+ TLDs and the many registrars already in existence. We assume this pattern will continue.

Question 2

In cases where urgent measures are needed to deal with malicious conduct involving the Domain Name System, what challenges exist?

Registries and registrars face a number of challenges regarding abuse mitigation:

- Legal: Varying privacy laws and government regulation and control. Risks involved in suspending domain names (esp. false-positives).
- Alleged abuse or malicious behavior is sometimes difficult to identify and verify.
- Technical challenges, including obtaining, examining, and acting upon high-quality data.
  - data that is timely and formatted
  - Registrant data may be dispersed and/or inaccurate.
- Costs. Security work is a cost center that impacts the bottom line.

Question 3

As the current model of cooperative interaction between registries, registrars, security organizations, and law enforcement scales to become more global, what new processes will be needed to mitigate malicious conducts that utilize the Domain Name System?

- Cooperation is already global. We urge further voluntary data-sharing and cooperation between interested parties.
- '*threats to the security and stability of the DNS*' is very different 'from malicious conduct *involving or using* the Domain Name System'.
- The mitigation of "malicious conduct that utilizes the Domain Name System" seems largely beyond ICANN's scope.
- We suggest that ICANN, where appropriate, take steps to become aware of threats to the security and stability of the DNS itself as they develop, and to then inform and cooperate with relevant parties who can help prevent or mitigate such problems.

Question 4

What specific measures can be employed by ICANN as a corporation to mitigate any potential increase in malicious conduct that might arise solely from the additions of new gTLDs?

1. New gTLD applications are examined for technical, operational, financial, and service capabilities. We recommend that ICANN consider whether the applicant addresses abuse topics, such as proposing anti-abuse policies or procedures (based upon current best practices as defined by industry leaders). Applications that fail to include any mention of abuse should be referred to the Extended Evaluation process.
2. The ICANN compliance staff has a central role in ensuring that registrars respond to WHOIS complaints, and making sure that registrars are maintaining their WHOIS servers properly. The ICANN compliance staff should conduct regular reviews of all registrars' compliance with WHOIS requirements, in accordance with existing agreements and consensus policies.

Thank you!