



No. 49  
23-27 MARCH 2014

# Singapore



# Agenda

1. Welcome and roll call
  2. Metrics that require baseline, but have a high barrier to execution
    - a. 1.13: Consumer Trust - Quantity of Compliance Concerns regarding Applicable National Laws, including reported data security breaches.
    - b. 1.17: Consumer Trust - Quantity and relative incidence of detected phishing sites using new gTLDs.
    - c. 1.18: Consumer Trust - Quantity and relative incidence of detected botnets and malware distributed using new gTLDs.
    - d. 1.19: Consumer Trust - Quantity and relative incidence of sites found to be dealing in or distributing identities and account information used in identity fraud.
    - e. 1.22: Consumer Trust - Qualitative comparison of mission and purpose set forth in Question 18 of the new gTLD Application with current actual use of the gTLD.
    - f. 5.2-5.4: Consumer Trust - Growth in use of hosted pages (i.e. Facebook)/QR codes/URL shortening services
  3. Adding additional metrics
    - a. Collisions
    - b. Registrar discrimination by registrars owned by registries
  4. 4. Next Steps
  5. Any other business
- #ICANN49





# LAG-CCT metrics discussion

#ICANN49



## 1.13: Quantity of Compliance Concerns regarding Applicable National Laws, including reported data security breaches.

- National laws
  - Compliance may include complaint code for complaints based on national laws
  - Further define “applicable national law” to determine LEA input, i.e. tax laws, identity theft, pornography, etc.
  - WIPO indexes a subset of cases that reference national laws – but ultimately these cases are tracked as UDRP decisions in other metrics
- Data security breach reports collected per 2013 RAA 3.20
- Registry agreement 2.18: ICANN may receive complaints on insufficient protection of personal data

1.17: Quantity and relative incidence of detected phishing sites using new gTLDs.

- Registry Agreement, Spec. 11: Report on incidents of phishing, pharming, malware & botnets provided on ICANN's request
- APWG phishing data dates to 2007
  - Plan to incorporate new gTLDs in analysis, which will show top TLDs for phishing

## 1.18: Quantity and relative incidence of detected botnets and malware distributed using new gTLDs.

---

- Potential sources:
  - Spamhaus: DROP lists botnets and malware
  - ShadowServer: Tracks botnets and malware and has historic data
  - Malware Domain List: Historic data to 2009
  - APWG: May collect some of this data

1.19: Quantity and relative incidence of sites found to be dealing in or distributing identities and account information used in identity fraud.

---

- Research has found that stolen identities are not distributed via sites but rather underground chat rooms or other networks.
- May be able to measure instance of sites *collecting* identities, but this might mirror the information in metrics 1.16-1.18

1.22: Qualitative comparison of mission and purpose set forth in Question 18 of the new gTLD Application with current actual use of the gTLD.

---

- Qualitative study would require outside resources, possibly hiring a consulting or other firm to conduct analysis.



## 5.2-5.4: Growth in use of hosted pages (i.e. Facebook)/QR codes/URL shortening services

---

- Comscore has some U.S./Europe-centric data on mobile phone usage (QR codes)
- More representative global data available for desktop computer users on hosted pages and URL shorteners
- Costs vary but can do snapshot reports or provide access to subscription service
- Other market research firms for comparison: Nielsen Online, Alexa

# Social Media



<https://twitter.com/ICANN>



<http://gplus.to/icann>



<https://www.facebook.com/icannorg>



<http://weibo.com/icannorg>



<http://www.linkedin.com/company/icann>

#ICANN49

