DNS Abuse Mitigation

GAC PSWG Speakers:
Laureen Kapin (US Federal Trade Commission, Co-Chair GAC PSWG)
Chris Lewis-Evans (UK National Crime Agency, Co-Chair GAC PSWG)
Gabriel Andrews (US Federal Bureau of Investigation)

GAC Speaker:
Shinya Tahata (Japan, Ministry of Internal Affairs and Communications)

Invited Speakers:
Laurin Weissinger (The Fletcher School, Tufts University, M3AAWG Member)
Bill Wilson (M3AAWG Senior Advisor)

ICANN71

14 June 2021

ICANN | GAC
Governmental Advisory Committee

Agenda

1. Introduction: ICANN71 Discussions of DNS Abuse
2. SAC 115 Update (SSAC DNS Abuse Working Party Report)
3. Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets
4. Reasonable Timeline For Response To Requests for Registration Data
5. Publication of Reseller information in the RDS/WHOIS Output
6. Presentation of M3AAWG Report
7. Possible Concrete Steps for ICANN Compliance (Japan)
8. Next Steps for the GAC on DNS Abuse Mitigation

Introduction

GAC Discussions of DNS Abuse during ICANN71

- Agenda Item 3 - DNS Abuse Mitigation Discussions — Mon. 14 June 1230 UTC
- Agenda Item 10 - GAC Meeting with the ICANN Board — Tue. 15 June 1430 UTC
- Agenda Item 14 - GAC Meeting with the GNSO — Wed. 24 March 1430 UTC

Other Relevant Sessions during ICANN71

- Contracted Parties DNS Abuse WG Community Update — Wed. 16 June 0830 UTC
- Plenary Session: Understanding Reputation Block Lists Providers — Thu. 17 June 0830 UTC
- SSAC Public Meeting — Thu. 17 June 1230 UTC

SAC115 - SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS

Proposed Framework:

- Primary Point of Responsibility for Abuse Resolution
- Escalation Paths
- Evidentiary Terminology and Standards
- Reasonable Time Frames for Action
- Availability and Quality of Contact Information

Recommendations:

The SSAC recommends that the ICANN community continue to work together with the extended DNS infrastructure community in an effort to:

(1) examine and refine the proposal for a Common Abuse Response Facilitator to be created to streamline abuse reporting and minimize abuse victimization

(2) define the role and scope of work for the Common Abuse Response Facilitator, using SAC115 as an input.

Framework on DGAs for Malware & Botnets

- **“Botnets”**
  - are networks of compromised devices controlled by criminal actors.
  - Some of the largest and most dangerous botnets - such as Conficker and Avalanche - have been controlled via the use of Domain Generation Algorithms (DGAs)
- **Domain Generation Algorithms (DGAs)**
  - are tools which ‘input’ a specific date and time, and ‘output’ a domain name for that specific time.
- **Law Enforcement (LE) action vs Botnets**
  - Low Frequency / High Impact events
  - each domain only needs to be seized for a short duration at the specific date/time specified by the DGA.
- **Improving upon DGA referrals was identified by PSWG/RySG as “low hanging fruit” / attainable goal**
  - Recommends voluntary & non-binding Best Practices
  - Streamlining for an **EVERGREEN** solution
  - One action / referral by LE to Ry’s, and by Ry’s to ICANN, enabling **EVERGREEN** action going forward for that DGA.
    - Avoiding wherever possible the need to keep "coming back to the well"
- **Thanks to ICANN** for willingness their feedback and guidance on engaging the “Expedited Registry Security Request” mechanism

Timeline for response to requests for WHOIS data

Timeline to respond to urgent requests for domain name registration data continues to be debated (Phase 1 EPDP Rec. 18)

- **GAC representatives urging 24 hrs**
- "Urgent Requests for Lawful Disclosure" are *limited* to circumstances that pose *an imminent threat to life, serious bodily injury, critical infrastructure, or child exploitation in cases where disclosure of the data is necessary in combatting or addressing this threat*. Critical infrastructure means the physical and cyber systems that are vital in that their incapacity or destruction would have a debilitating impact on economic security or public safety.
  - Response time for non-urgent requests: 30 days
  - Separate timeline for *urgent* requests (Phase 1: time frame to be finalized and criteria set for Urgent requests during implementation → IRT deliberating)
    - GAC and certain other groups advocating for no more than 24 hrs
    - Registries and Registrars argue for up to *three business days* (two to acknowledge request plus one to respond) → over holiday weekends that could add up to 6 calendar days which is far too long

Publication of Reseller information in WHOIS

Issue: Public Domain Name Registration Data include Registrar but the entity that actually holds the Registration Data may be a reseller (a customer of the registrar). There may even be several levels of resellers involved. That creates challenges for law enforcement and others when they are seeking data by formal request or subpoena because they are not directing the request to the right entity.

→ **Competition, Consumer Trust and Consumer Choice (CCT) Review Team Rec. 17:**

- **ICANN should collect data about and publicize the chain of parties responsible for gTLD domain name registrations.**
- ICANN Board **accepted** this recommendation and indicated that this is already taking place
- **Problem:** The publication of this data *is not currently required*

Full acceptance and implementation of CCT Rec. 17 would require the collection and disclosure of the chain of parties [like Resellers] responsible for Domain Name registrations

M3AAWG and APWG on Changes to WHOIS

The Messaging Malware and Mobile Anti-Abuse Woking Group (M3AAWG) and The Anti-Phishing Working Group (APWG) released a Report (June 2021):

- **Survey of cyber investigators and anti-abuse service providers** to understand how ICANN's application of the European Union's General Data Protection Regulation (GDPR) has impacted WHOIS service and anti-abuse work.

- **Discusses effect of the Temporary Specification** on anti-abuse actors' access and usage of domain name registration information, which is central for various types of investigations.

ICANN, GDPR, and the WHOIS: A Users Survey - Three Years Later

A Survey by M3AAWG and APWG

June 8, 2021

Laurin Weissinger, DPhil
Lecturer
The Fletcher School

Dave Piscitello
Interisle Consulting Group

Bill Wilson
M3AAWG Senior Advisor

Who is M3AAWG?

Founded in 2004, Messaging, Malware and Mobile Anti-Abuse Working Group (**M^{3}AAWG**) is the largest global industry bringing together all the stakeholders within the online community in a confidential, technology-neutral, and non-political open forum to develop cooperative approaches for fighting online abuse and exploitation.

What Does M³AAWG Do?

We develop and publish best practices papers, position statements, training and educational videos, and other materials to help the online community fight abuse with a focus on operational practices.

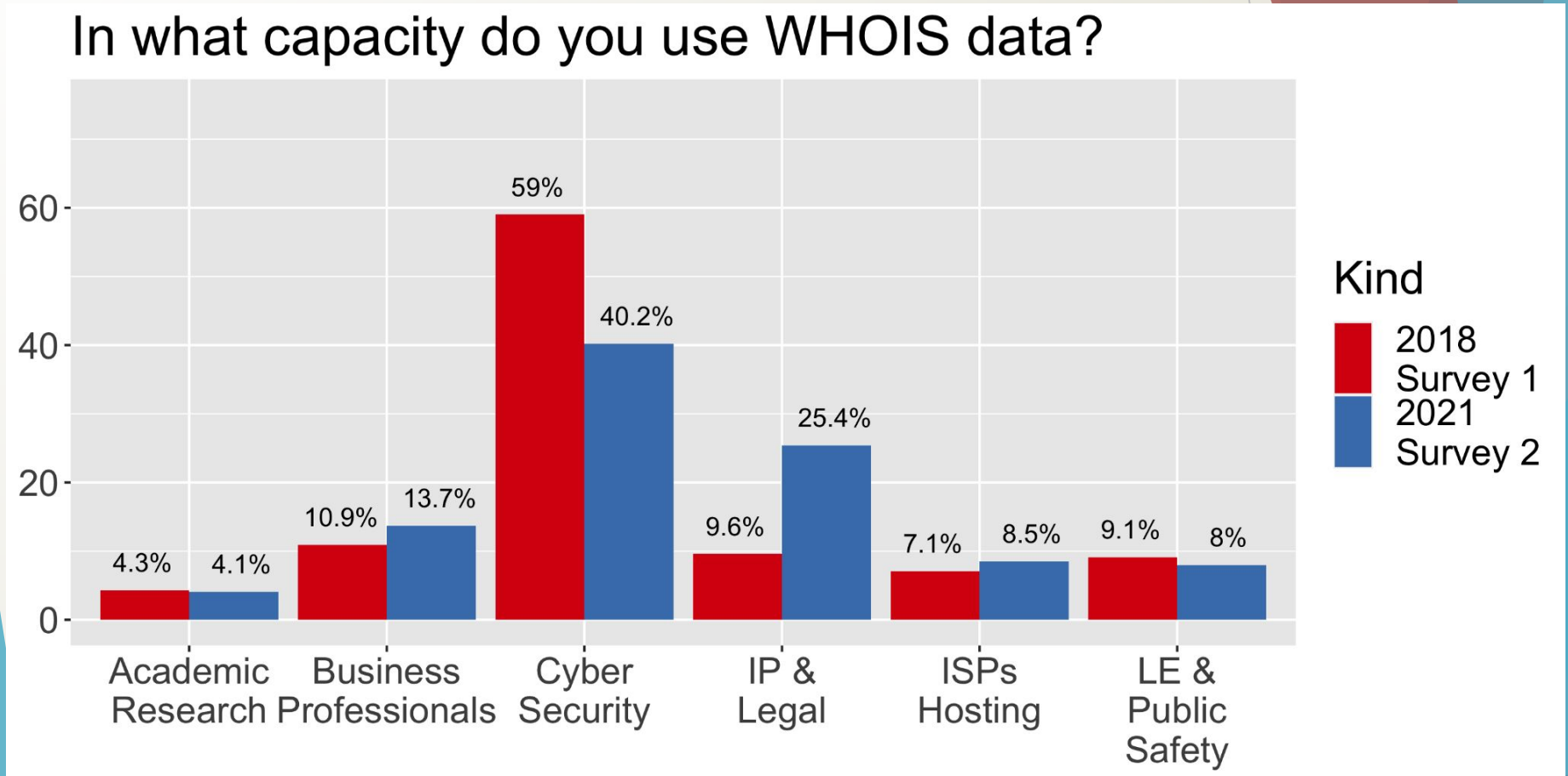
Our public policy advocacy (which is not lobbying) provides technical and operational guidance to governments and Internet and public policy agencies developing new Internet policies and legislation.

WHOIS Use is Diverse

- Different users have different needs and use cases
  - How many records are accessed?
  - What happens with these records?
  - What properties are needed for data to be actionable/useful?
  - How quickly are these data required?

- Examples
  - Bulk user doing data analysis (lots of data, frequently)
  - Investigator requesting records (infrequent, manual)

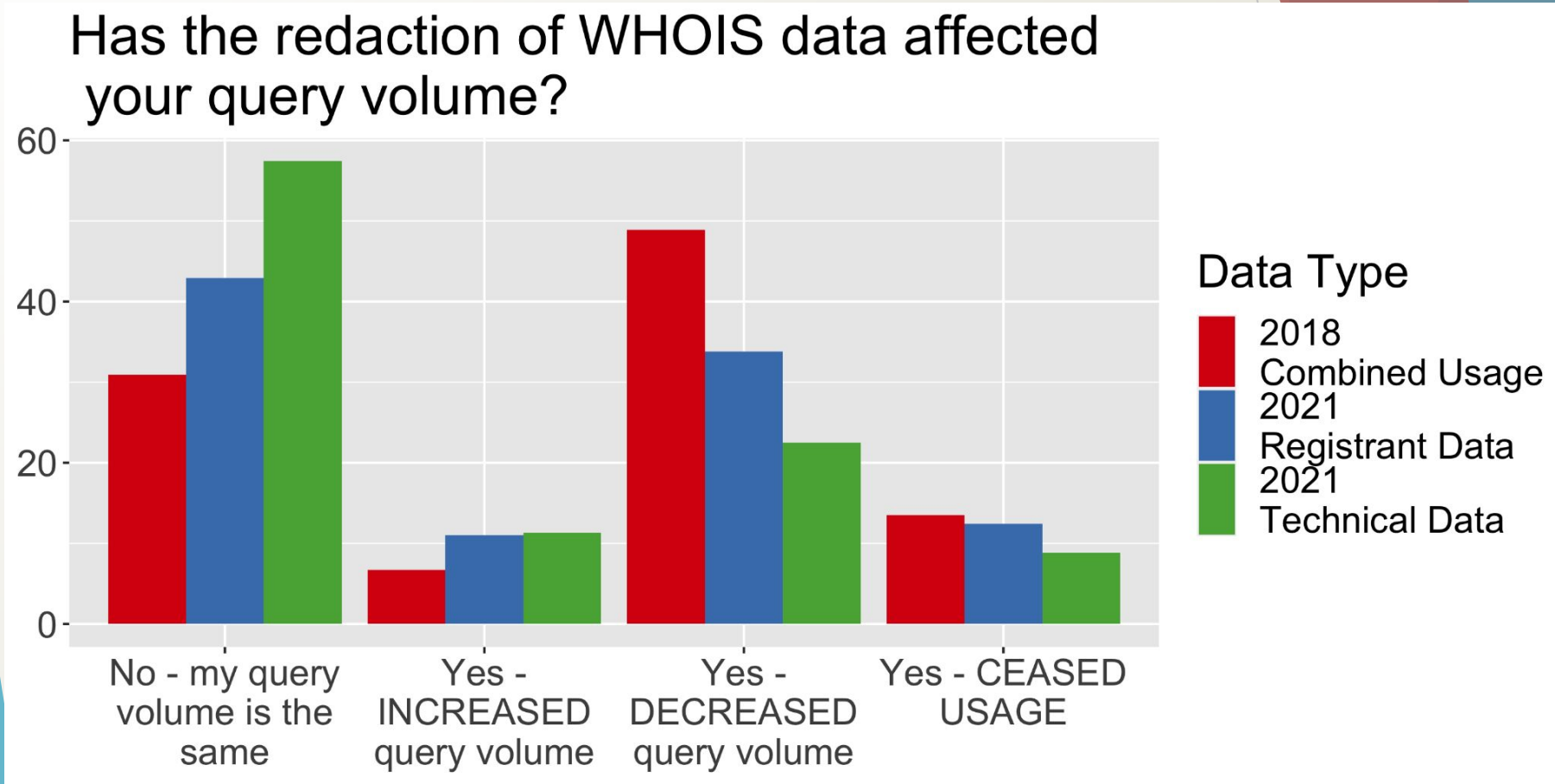
Demographics and Use of WHOIS



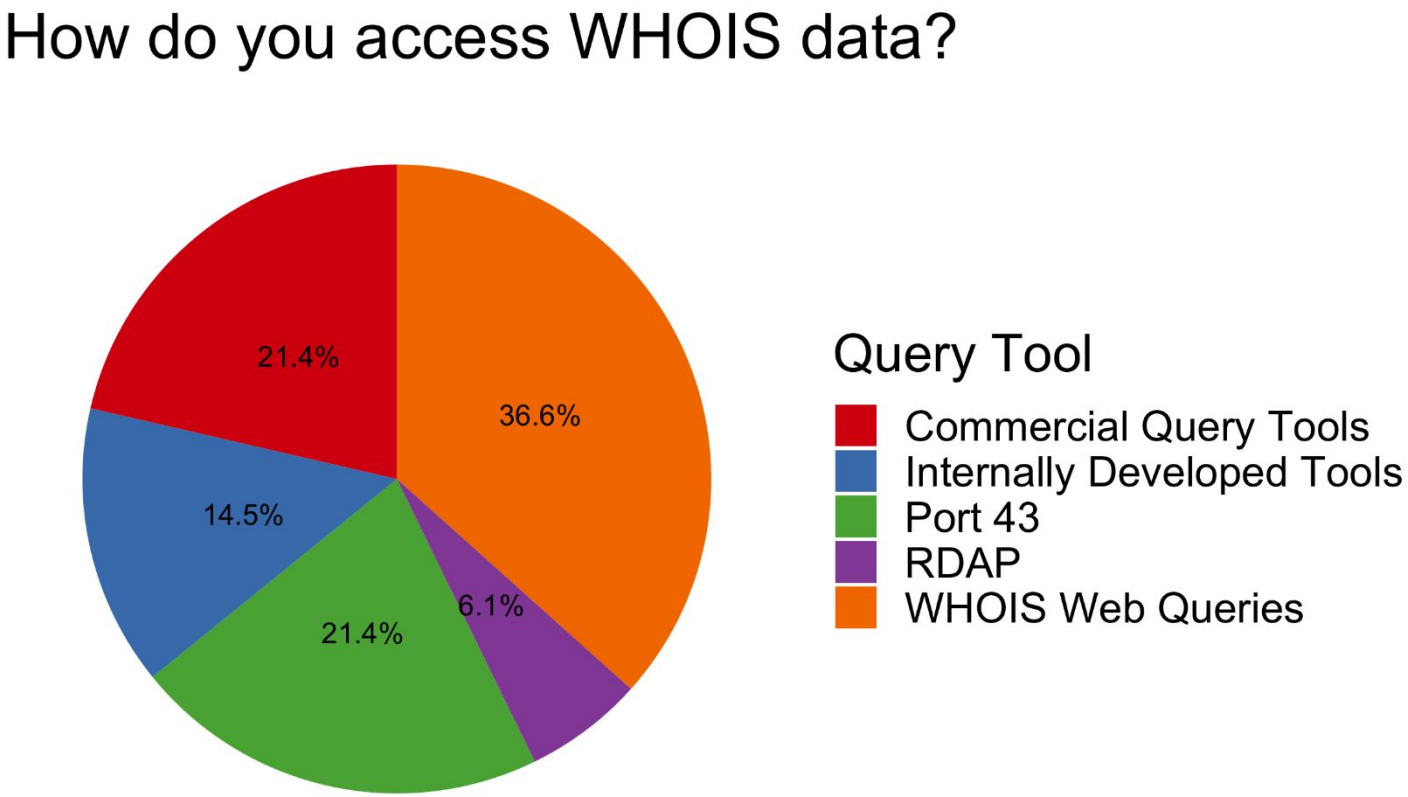
WHOIS Use

- Even within our particular sample, only one out of ten respondents makes more than 10000 queries per day.
- More than two thirds of our respondents are below 100 daily queries.
- Beyond mere numbers, what requests are for, and how records are used is variable.

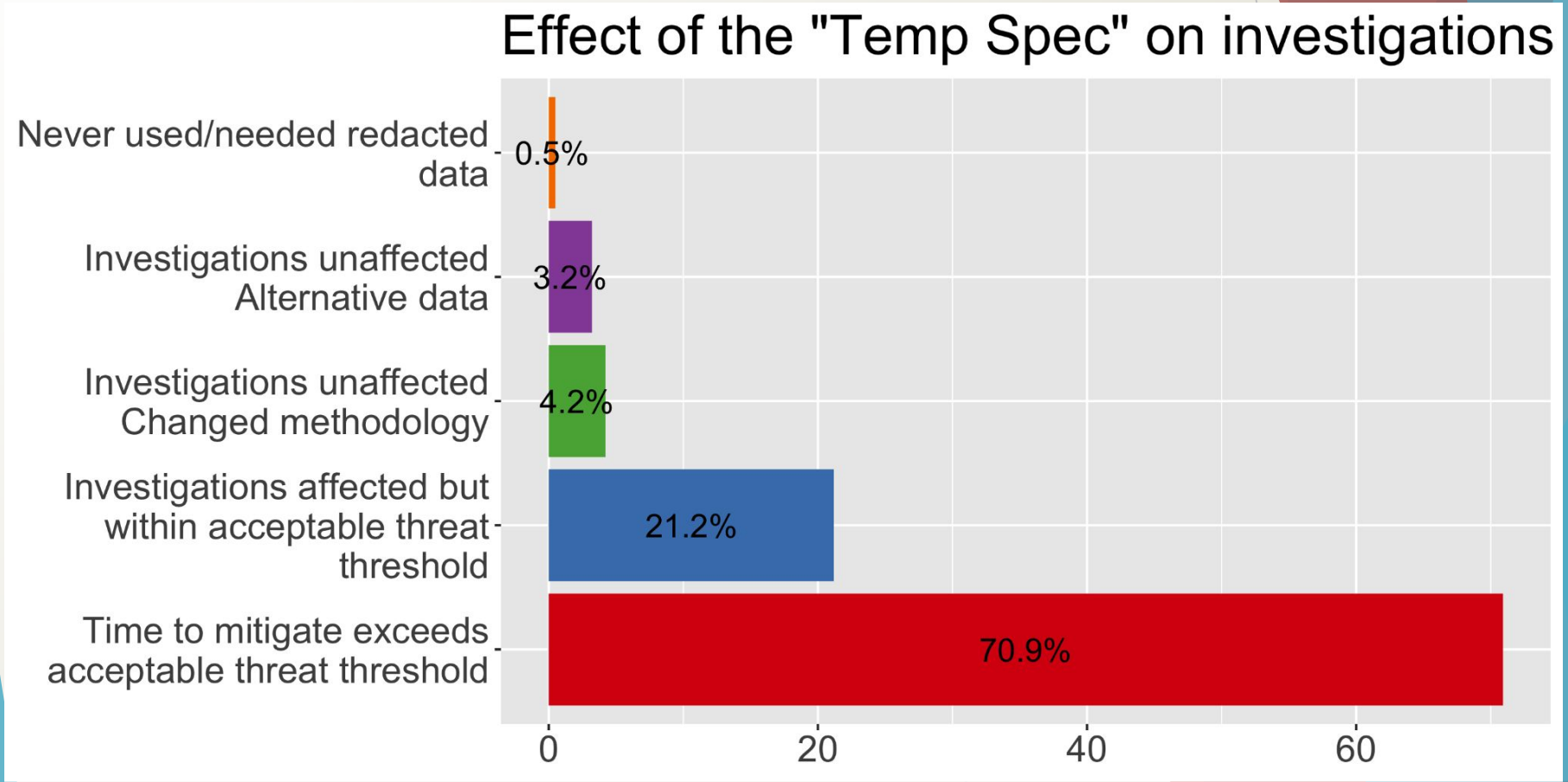
The Effect of the "Temp Spec" on WHOIS Use



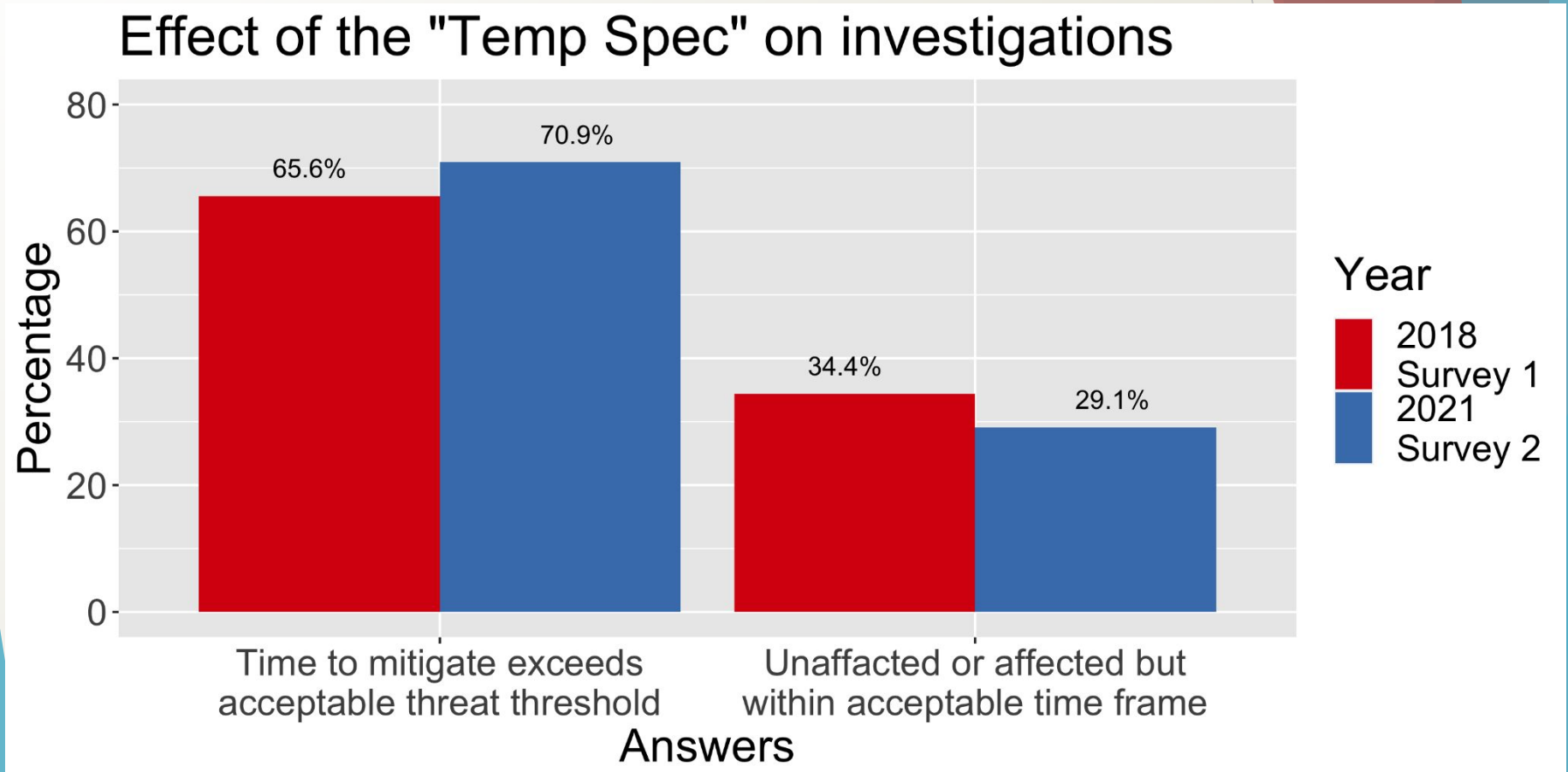
Demographics and Use of WHOIS



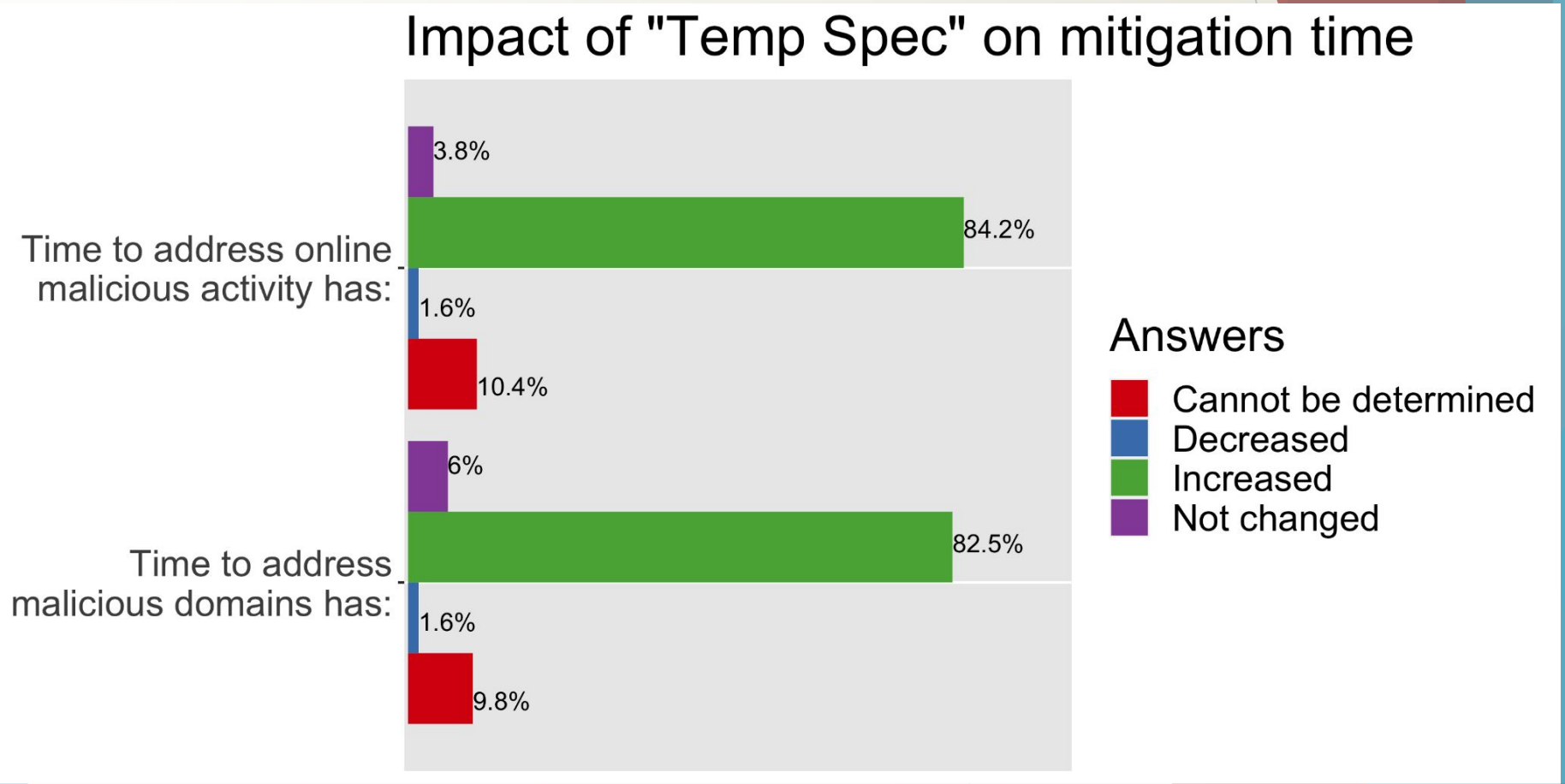
The Effect of the Temporary Specification on WHOIS



The Effect of the Temporary Specification on WHOIS



The Effect of the Temporary Specification on WHOIS

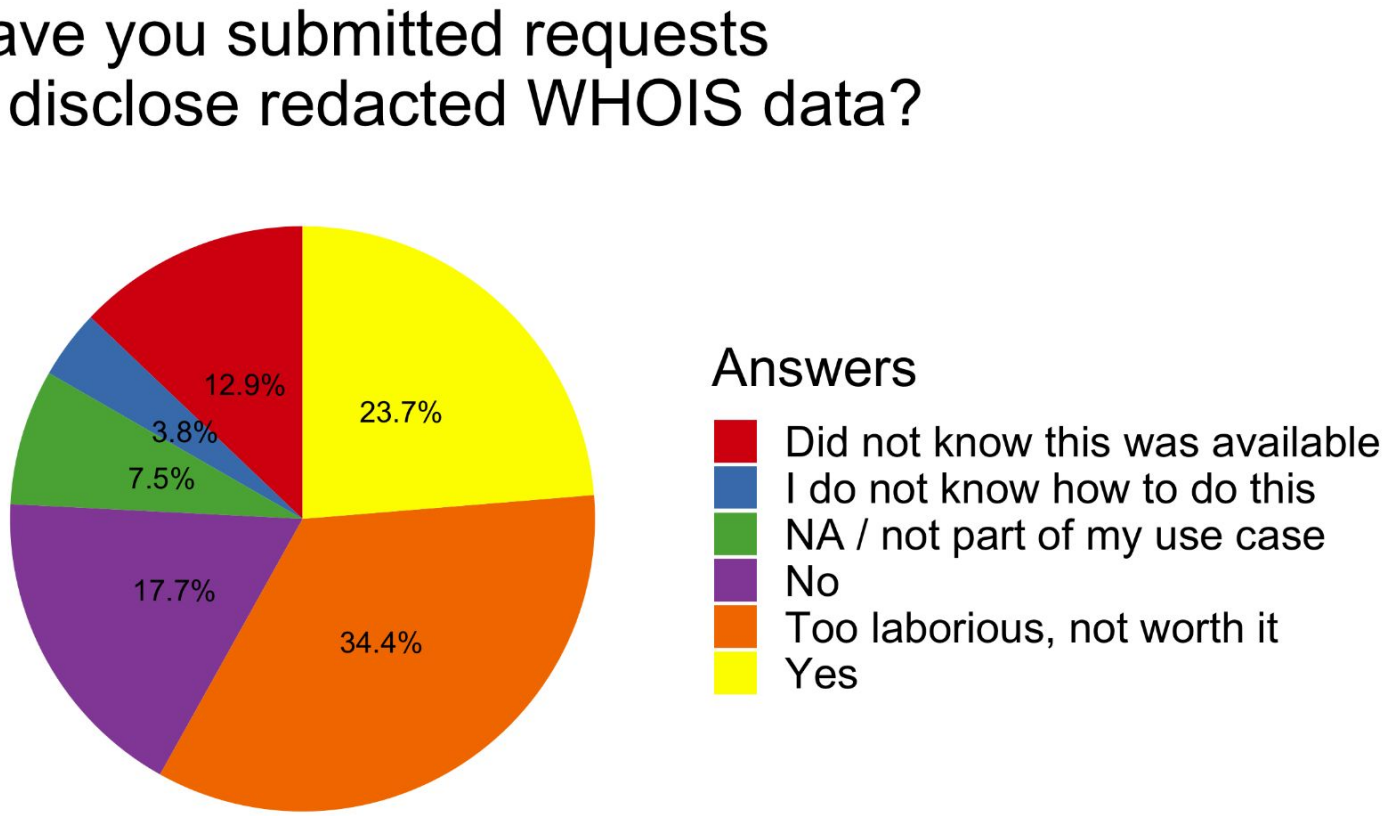


Summary of Issues

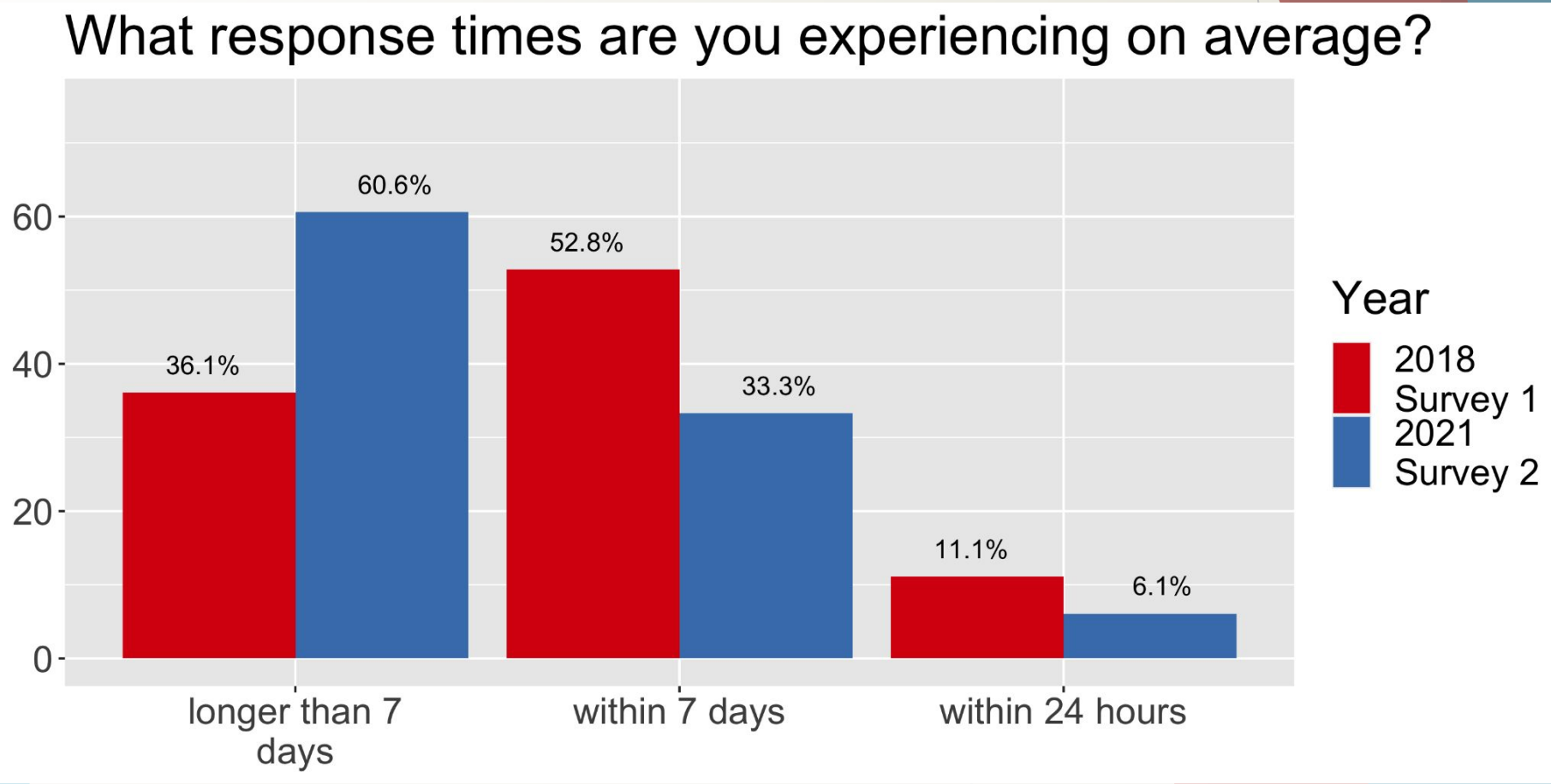
Generally, many use cases of WHOIS data are affected:

- Only one quarter of respondents were able to find alternative data sources.
- Attribution is very much impaired, with 9 out 10 respondents reporting problems.
- Over 50% consider redaction of legal and non-EU persons to be excessive.
- Only 2.2% think the Temp Spec is working.

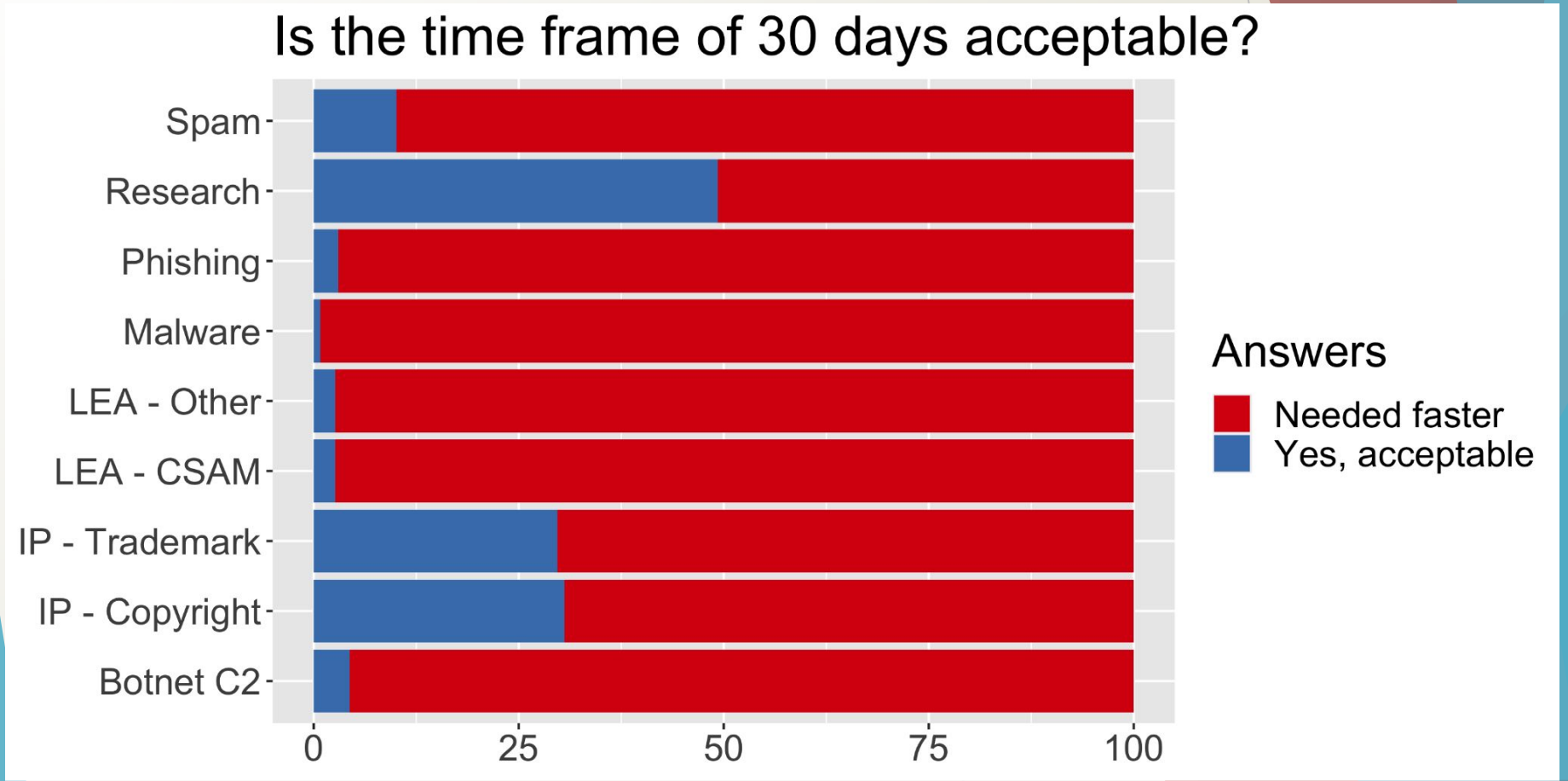
Disclosure of Redacted Data



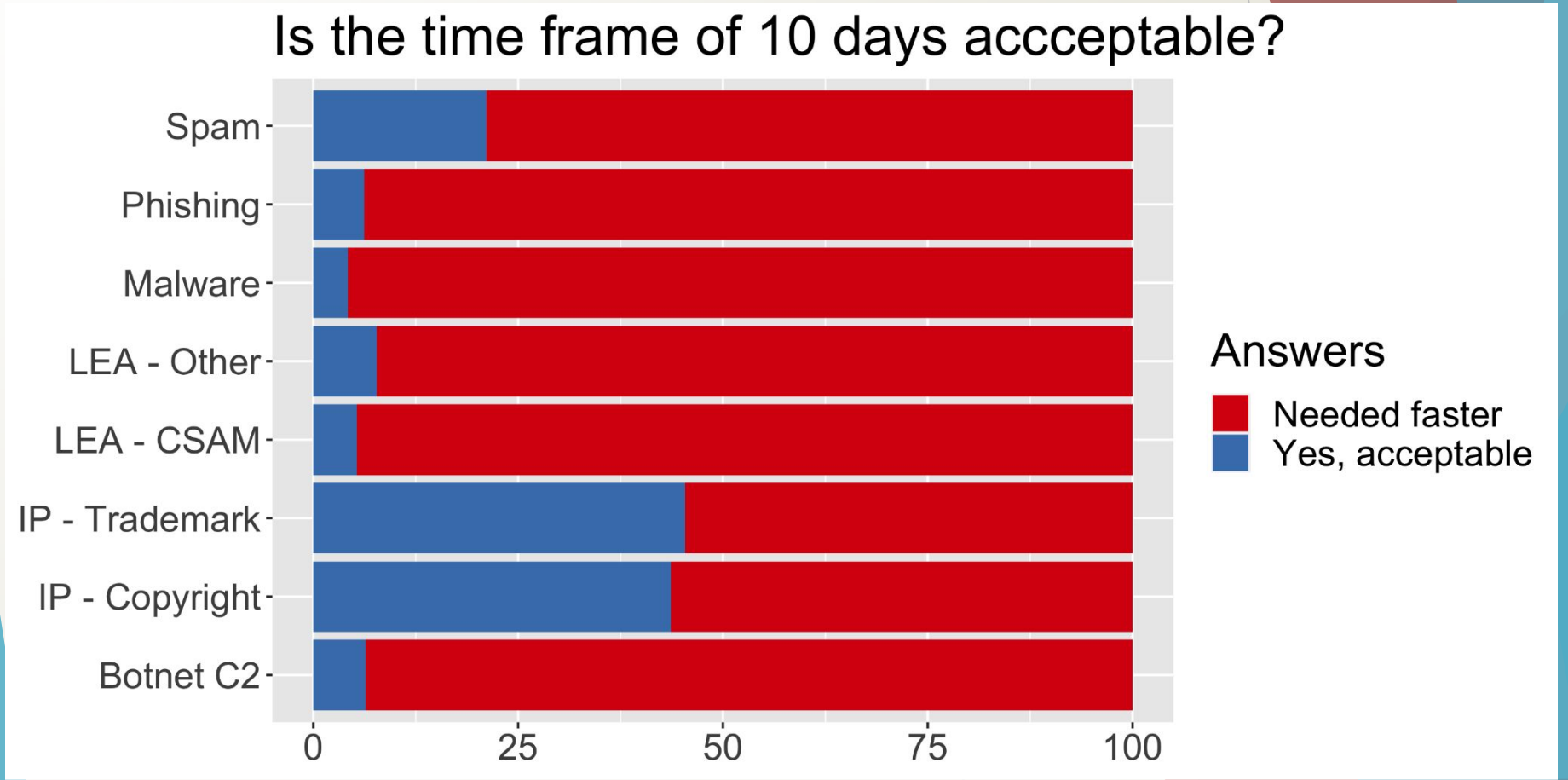
Disclosure of Redacted Data



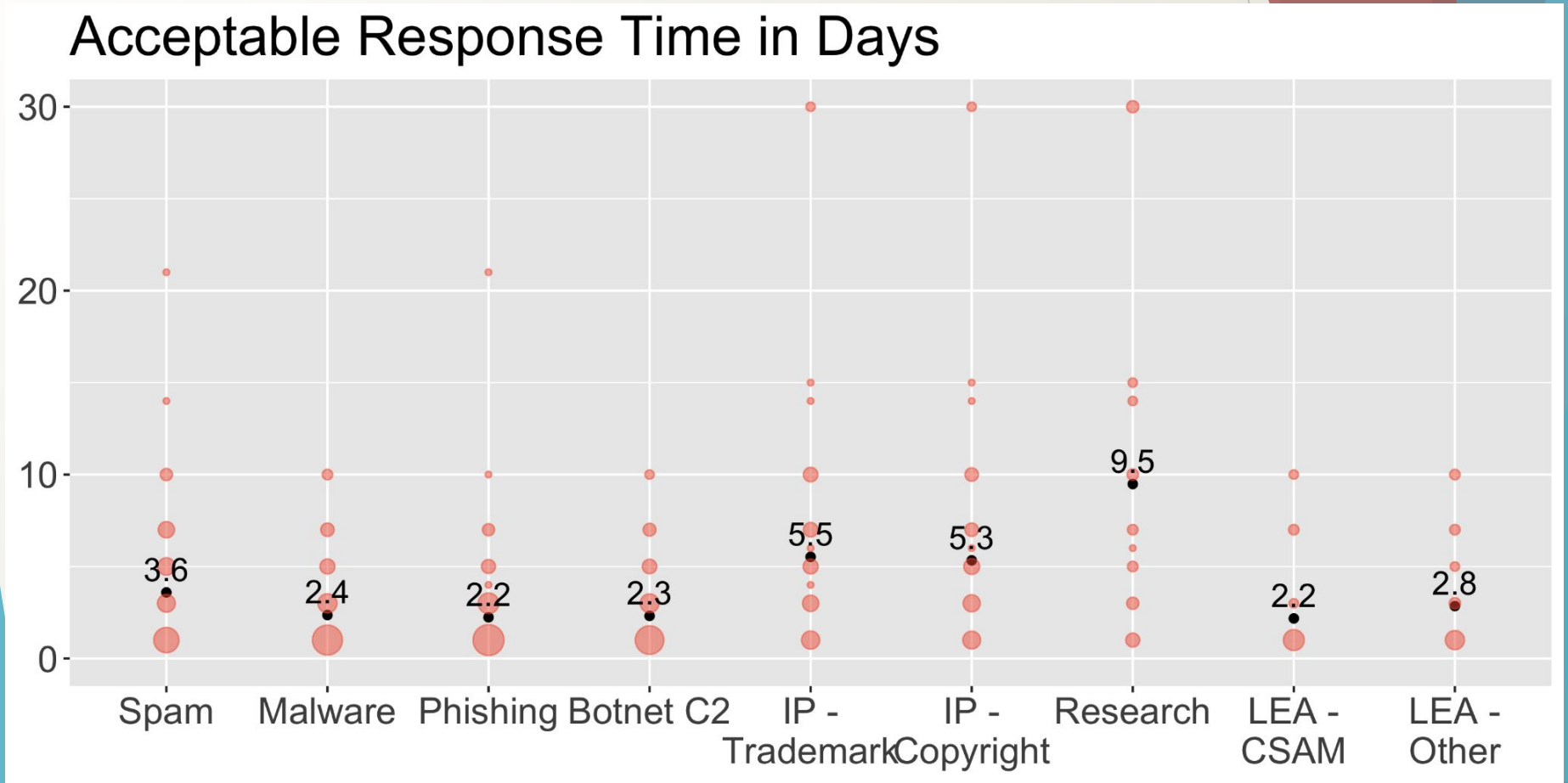
Disclosure of Redacted Data



Disclosure of Redacted Data



Disclosure of Redacted Data



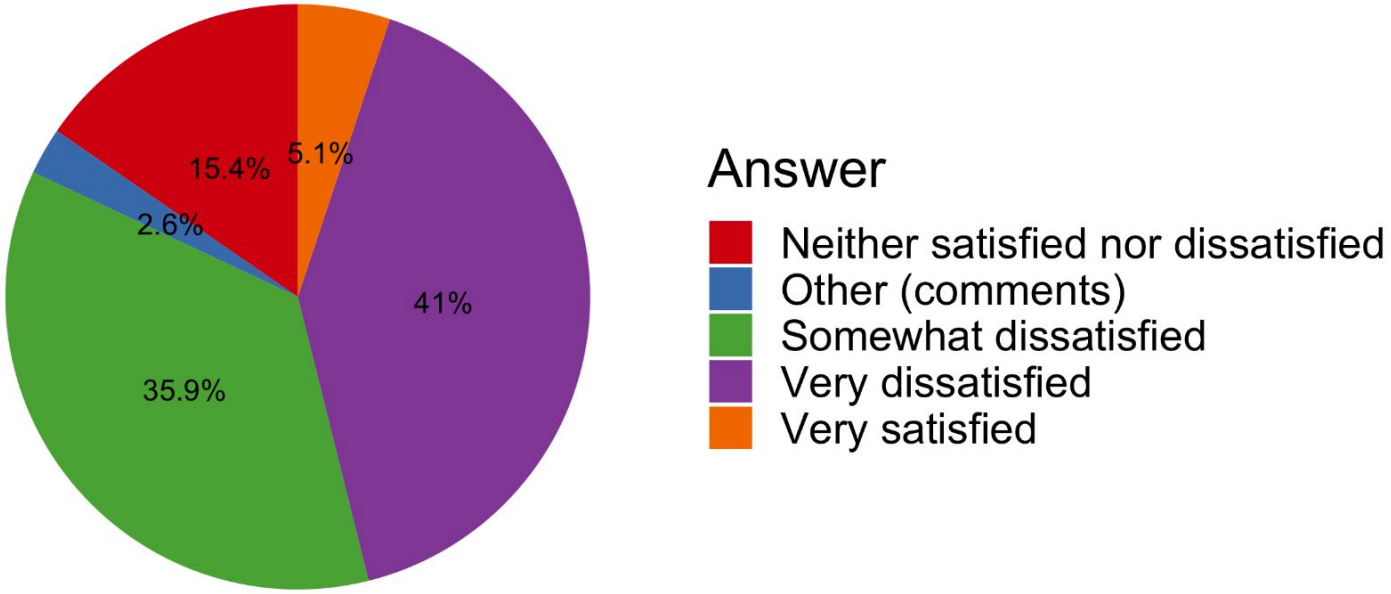
Disclosure Systems under ICANN consideration

- Future disclosure systems are being discussed at ICANN
  - A paid system is one of these approaches.
  - 61% do not have the ability/resources to pay.
  - Multiple respondents underline that such a system is wholly inappropriate

- Of the 39% who indicate that they are able to pay fees:
  - 78% would pay a (reasonable) accreditation fee (30%).
  - 61% would accept tiered or per volume pricing (24%).

Complaints to ICANN

How satisfied have you been with ICANN Compliance's handling of your disclosure-related complaints?



Observations

- Access to relevant data should be available while protecting natural persons' privacy.
- The survey responses indicate that the solutions currently discussed at ICANN would not meet the needs of law enforcement and cybersecurity actors.
- ICANN should establish a functional system of registrant data access for accredited parties; such a system needs to be workable for cybersecurity professionals and law enforcement in terms of time delays and administrative burden, and should include strict privacy and security controls.
- Both sporadic WHOIS users who make relatively few requests, as well as bulk users who use data-driven approaches, e.g. for blocklisting, should be accommodated.

Summary

- Post Temp Spec WHOIS access increases the time it takes to address various types of abuse.
  - Timeliness of access is a challenge
  - The absence of uniformity across registrars hinders investigations
- The formal request system to access redacted data fails regularly.
  - Requests are routinely ignored, denied, or not responded to.
- ICANN compliance processes are described as lengthy and inefficient, frequently providing no resolution or recourse.

Contact Us

For additional questions, please email:
publicpolicy-chair@mailman.m3aawg.org

Concrete Steps for ICANN Compliance

[Presentation by Japan]

@ ICANN70

Japan's proposal

'In order to guarantee that the operations of Registries and Registrars are in compliance with ICANN contracts,

Japan would like to propose that GAC begin discussions on finding appropriate measures to strengthen enforcement, such as audits, under the session of DNS Abuse.'

ICANN70 GAC Communiqué

'The GAC also emphasized **the importance of taking measures to ensure that Registries, Registrars and Privacy/Proxy Providers comply with the provisions in the contracts with ICANN**, including audits.'

@ ICANN71

Possible concrete ideas for contractual compliance

① **Collecting accurate information from registrants at the timing of domain registration**
- ✓ Correct breached registrars through audits — ref. RAA Data Retention Specification Article 1

② **Verification of the identity of registrants**
- ✓ Pursue data accuracy — ref. SSR2 RT Final Report Recommendation 9.2
- ✓ Verify phone number — ref. RAA WHOIS Accuracy Program Specification Article 5

③ **Strict response to abuse reports from ICANN compliance**
- ✓ Ask for evidence to prove that domain names are not abusive ones

2013 Registrar Accreditation Agreement Data Retention Specification

1. During the Term of this Agreement, for each Registered Name sponsored by Registrar within a gTLD, Registrar shall collect and securely maintain in its own electronic database (as updated from time to time) the data specified below:

1.1. **Registrar shall collect the following information from registrants at the time of registration of a domain name (a "Registration")** and shall maintain that information for the duration of Registrar's sponsorship of the Registration and for a period of two additional years thereafter:

1.1.1. **First and last name or full legal name of registrant**;
1.1.2. First and last name or, in the event registrant is a legal person, the title of the registrant's administrative contact, technical contact, and billing contact;
1.1.3. **Postal address of registrant, administrative contact, technical contact, and billing contact**;
1.1.4. **Email address of registrant, administrative contact, technical contact, and billing contact**;
1.1.5. **Telephone contact for registrant, administrative contact, technical contact, and billing contact**;
1.1.6. WHOIS information, as set forth in the WHOIS Specification;
1.1.7. Types of domain name services purchased for use in connection with the Registration; and
1.1.8. **To the extent collected by Registrar, "card on file," current period third party transaction number, or other recurring payment data.**

2013 Registrar Accreditation Agreement WHOIS Accuracy Program Specification

5. **Upon the occurrence of a Registered Name Holder's willful provision of inaccurate or unreliable WHOIS information, its willful failure promptly to update information provided to Registrar, or its failure to respond for over fifteen (15) calendar days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration, Registrar shall either terminate or suspend the Registered Name Holder's Registered Name or place such registration on clientHold and clientTransferProhibited, until such time as Registrar has validated the information provided by the Registered Name Holder.**

ICANN Compliance 'Registrar Compliance Program'

'**Examples of steps registrars took to investigate and respond to abuse reports:**

- Contacting registrant
- **Asking for and obtaining evidence or licenses**
- Providing hosting provider info to complainant
- Performing WHOIS verification
- Performing transfer upon request of registrant
- Suspending domain'

Next Steps on DNS Abuse Mitigation

Context

1. The GNSO's New gTLD Subsequent Procedures PDP indicated that DNS Abuse needs to be addressed w/respect to all gTLDs (not just new gTLDs)
   - yet first round of new gTLD contracts included more robust provisions to combat DNS Abuse

2. Community disagrees on scope and definitions of DNS Abuse
   - yet GAC Statement on DNS Abuse (18 Sept. 2019) identified some common ground on definitions
     i. based on contract language prohibitions and prior community work
     ii. other Stakeholder Groups including Contracted Parties have also proposed definitions

Concrete Proposal: Definition of DNS Abuse

Seek closure of discussion on DNS Abuse definitions

GAC Statement on DNS Abuse (18 September 2019) notes range of definitions:

- **CCT Review Team**:
  - "intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names."
  - "DNS Security Abuse" refers to more technical forms of malicious activity, such as malware, phishing, and botnets, as well as spam when used as a delivery method for these forms of abuse
- **ICANN contracts**:
  - Required prohibition on registrants: distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing consequences for such activities including suspension of the domain name.
  - **Registry Operators of new gTLDs** must "periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, **such as** pharming, phishing, malware, and botnets." (list is illustrative rather than exhaustive)
  - **Registrars of new gTLDs** must promptly "investigate and respond appropriately to any reports of abuse."

→ **These sources, developed within the ICANN multistakeholder community comprise a common foundational understanding of what comprises DNS Abuse**.

Next Steps

GAC should participate in possible community work on:

- definitions of DNS Abuse
- improved contract provisions
- public education on avoiding DNS Abuse

Thank You and Questions

Visit us at **icann.org**

 @icann

 facebook.com/icannorg

 youtube.com/icannnews

 flickr.com/icann

 linkedin/company/icann

 slideshare/icannpresentations

 soundcloud/icann