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

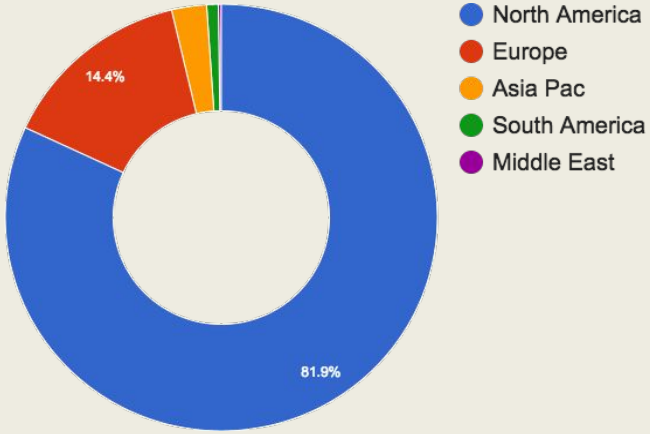
A Survey by M3AAWG and APWG

June 16, 2021

Who is M3AAWG?

Founded in 2004, Messaging, Malware and Mobile Anti-Abuse Working Group (**M^{3}AAWG**) is the largest global industry group 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.

Who is M³AAWG?
Constituencies and Demographics



"The Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) is where the industry comes together to work against botnets, malware, spam, viruses, DoS attacks and other online exploitation"

- 260 member orgs "**worldwide**"
- **300-400 conference participants**
- technology-neutral, *non-political* working body focusing on operational issues of Internet abuse
  - Supporting technologies
  - Industry collaboration
  - Informing Public Policy

M³AAWG | Messaging Malware Mobile Anti-Abuse Working Group

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.

What Does M³AAWG Do?

Distill Industry Knowledge into BCPs

The "M" *cubed*:

- **Messaging:** abuse on any messaging platform, from e-mail to SMS texting
- **Malware:** abuse is often just a symptom and vector for viruses and malicious code
- **Mobile:** addressing messaging and malware issues emerging on mobile as an increasingly ubiquitous platform

Develop and Publish:

- Best practice papers
- Position statements
- Training and educational videos

What Does M³AAWG Do?

Distill Industry Knowledge into BCPs

Recent BCPs

- M3AAWG Best Practices for Sending Mandated Emails to Large Audiences
- Exploring the Impact of Nonhuman Interactions on Email Send Metrics
- M3AAWG Email Authentication Recommended Best Practices

What Does M³AAWG Do?

Distill Industry Knowledge into BCPs

Operation Safety-Net

https://www.m3aawg.org/news/operation-safety-net-helps-business-and-government-leaders-understand-global-online-security

Public Policy and Industry Guidelines

https://www.m3aawg.org/for-the-industry/published-comments

The Anti-Bot Code of Conduct for Internet Service Providers

https://www.m3aawg.org/abcs-for-ISP-code

What Does M³AAWG Do?

Who Do We Work With?

Unsolicited Commercial Enforcement Net

- Operation Safety Net

FIRST

- Anti-abuse business case and outreach

Internet Society

- Provided training material

i2Coalition

- Hosting BCP

EastWest Institute

- Outreach and Transnational Policy Engagement

Anti-Phishing Working Group (APWG)

- Anti-Phishing Best Practices for ISPs and Mailbox Providers

LAC-AAWG

- Updating and developing BCPs to reflect LAC dynamics

JP-AAWG Development

- Working with regional orgs and industry partners

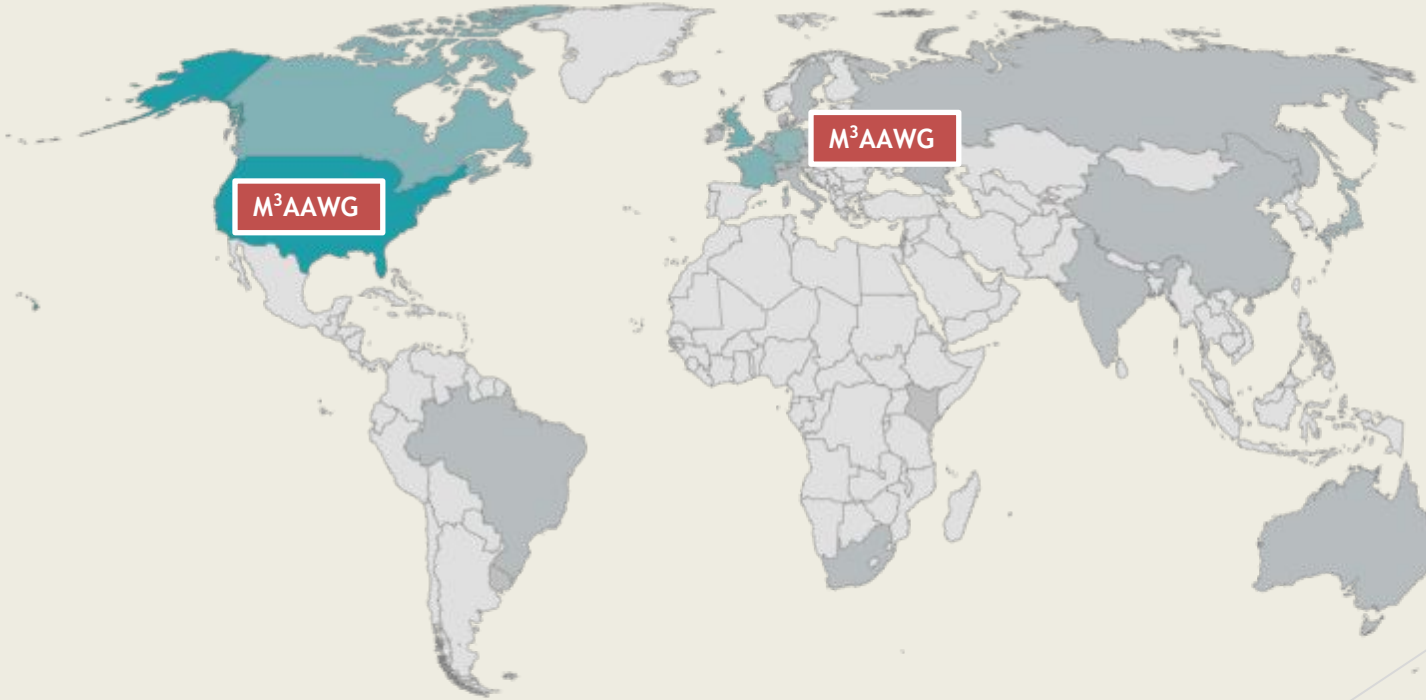
AF-AAWG Development

- In progress with AfricaCERT

Outreach:
Anti-Abuse Working Group Development

Regional AAWG Development

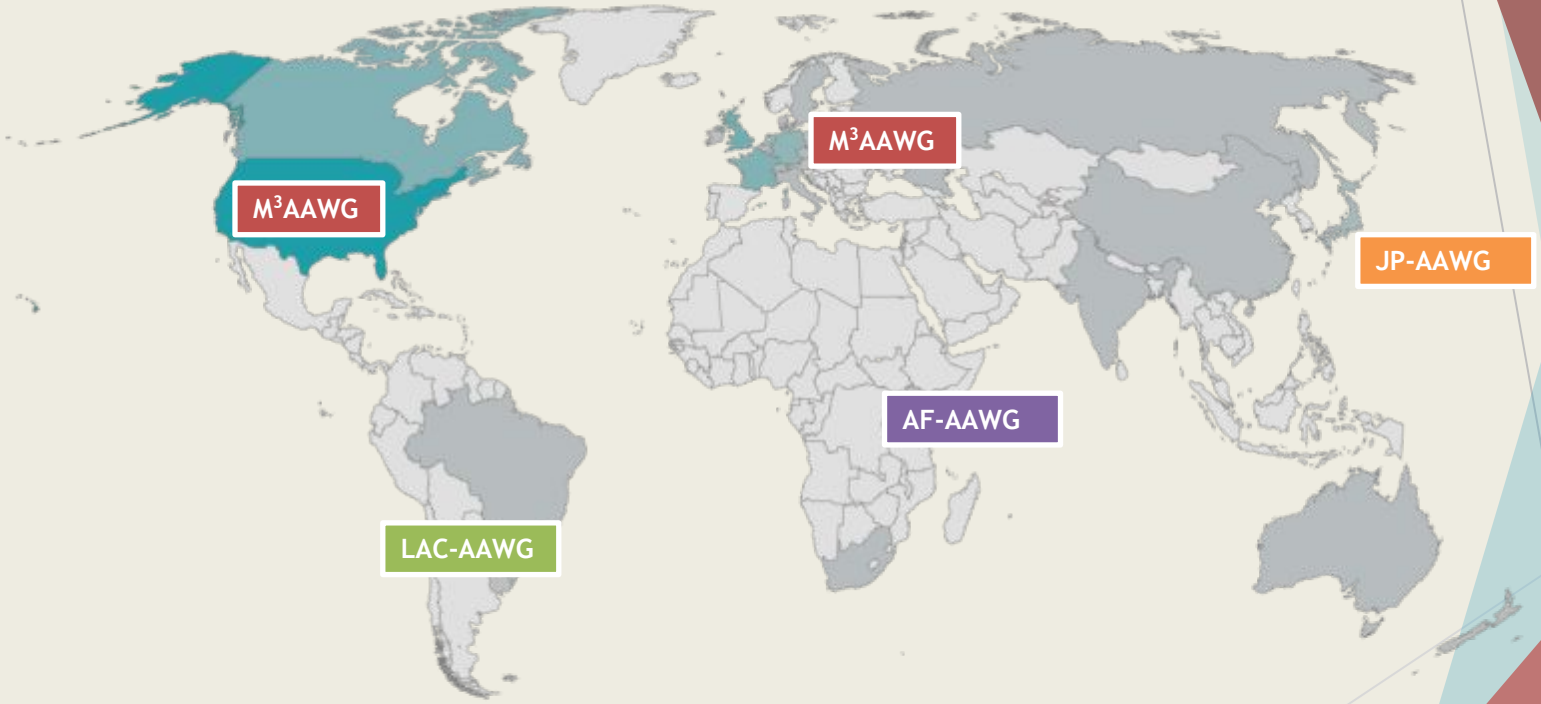
Contributing to *Peer* Working Groups



M³AAWG | Messaging Malware Mobile Anti-Abuse Working Group

Regional AAWG Development

Contributing to *Peer* Working Groups



M³AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Regional AAWG Development

Peer Working Group in LAC

lacnog

LACTLD
Latin American and Caribbean ccTLDs Organization

lacnic

AAWG Principles and Objectives

- Promulgate anti-abuse norms and principles
- Further develop regional anti-abuse expertise
  - Anti-abuse research
  - BCPs within and across regions
- Convene anti-abuse actors
  - operators
  - public policy
  - LE
- Represent regional anti-abuse expertise
- Exchange expertise
  - among operators within the regions
  - globally, among peer regions

M3AAWG | Messaging Malware Mobile Anti-Abuse Working Group

Regional AAWG Development *Peer* Working Group in Japan

Establishing New Organization

Content Sharing

- Bringing translated content to Japanese audiences
- Japanese members translating existing BCPs

Establishing initial membership set

- 75+ attendees at first two meetings
- In addition to development team, involvement from Equalitia, Rakuten, SoftBank, and others in region

Government Support for Olympics Milestone

- Yasuhiko Taniwaki, the Director-General for Information Security has provided endorsement and expressed his desire for cooperative working relationship

Regional AAWG Development

Peer Working Group in AF

Progress

- AF-AAWG charter drafted
- AfricaCERT is the home
- Jean-Robert Hountomy is driving engagement
- Collaborating with a variety of organizations including
  - AfriNIC
  - AFIX
  - ISOC
  - ICANN

Names and Numbers Committee

Formerly known as DNS Abuse - Addressing risks and threats against the identifier systems of the Internet

Chairs: Carlos Alvarez (ICANN), Carel Bitter (Spamhaus), and Leslie Nobile (NRO/ARIN)

Expert Advisor: Rod Rasmussen

Planning: Session for Oct 2021 meeting
Discovery of Designated Resolvers
(https://datatracker.ietf.org/doc/html/draft-ietf-add-ddr-00)

Engagement Series (May 2021)- Names and Numbers: Infrastructure for Good and Bad (Available Online M3AAWG Members)

June 9th session: RIRs and Anti-Abuse: The Perspective from the Numbering World

Questions?
Comments?
Volunteers?

Severin_Walker@comcast.com

The WHOIS Study

Laurin Weissinger, DPhil
Lecturer
The Fletcher School

Dave Piscitello
Interisle Consulting Group

Bill Wilson
M3AAWG Senior Advisor

Background

- WHOIS services provide access to data on registered assignees of Internet resources – this presentation is about domain names.
- In 2018, in response to the European Union's General Data Protection Regulation (GDPR), ICANN introduced the *Temporary Specification* ("Temp Spec"), which resulted in a broad suppression of registration contact data.
- M3AAWG and APWG conducted an initial survey of cyber investigators and anti-abuse service providers in 2018 to determine the impact of the new measures introduced by the Temporary Specification.

The 2021 Survey and Report - Purpose

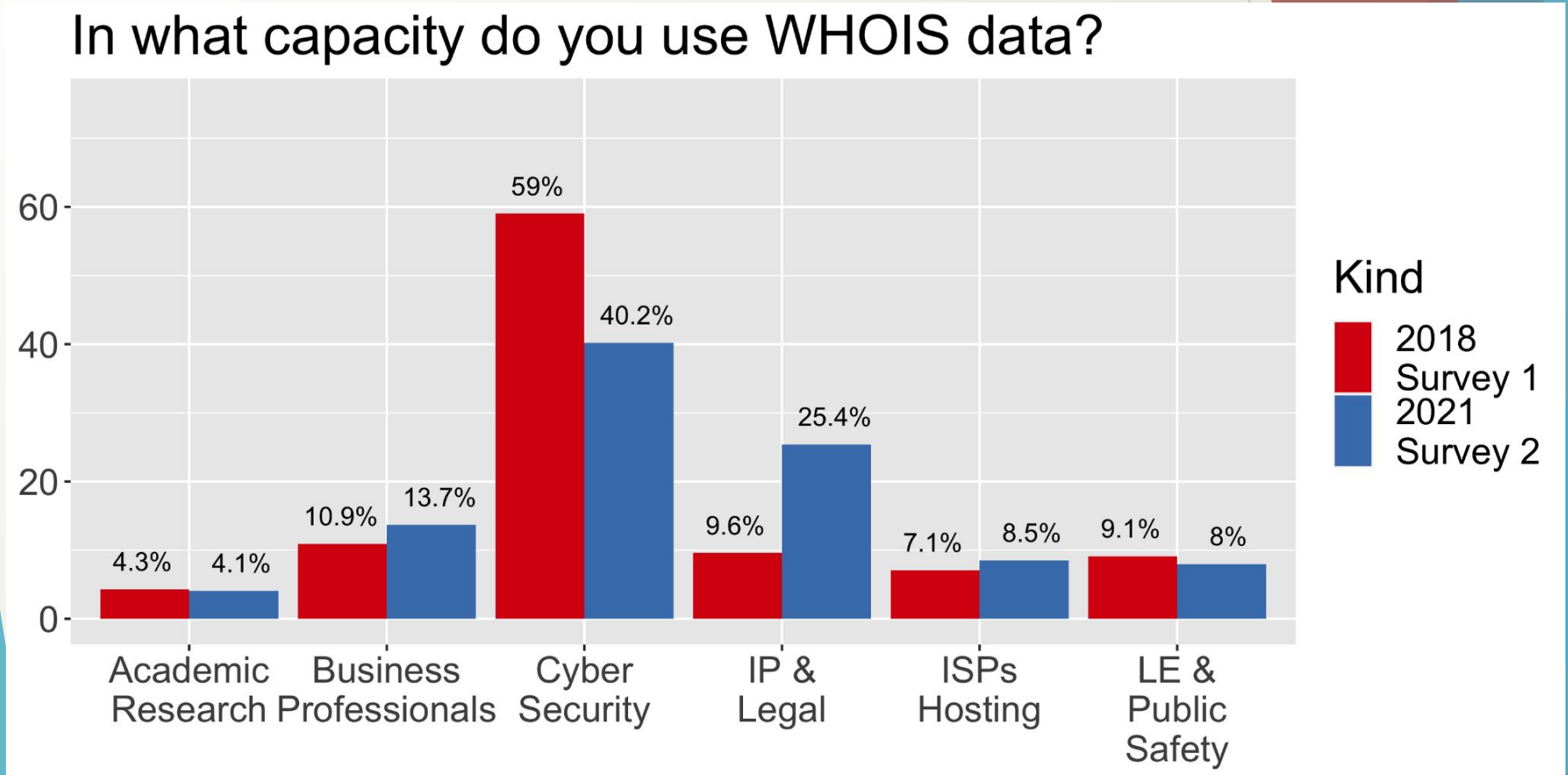
- M3AAWG and APWG recently conducted a second survey
  - Does the Temporary Specification and the redaction regime continue to affect the security and safety community… and how?
  - This presentation focuses on the challenges respondents continue to face.
- **Method**
  - Questions were prepared by M3AAWG members and their BoD
  - All graphs exclude N/A, "does not apply", or similar categories
  - 277 Respondents, recruited via email lists

WHOIS Use is Diverse

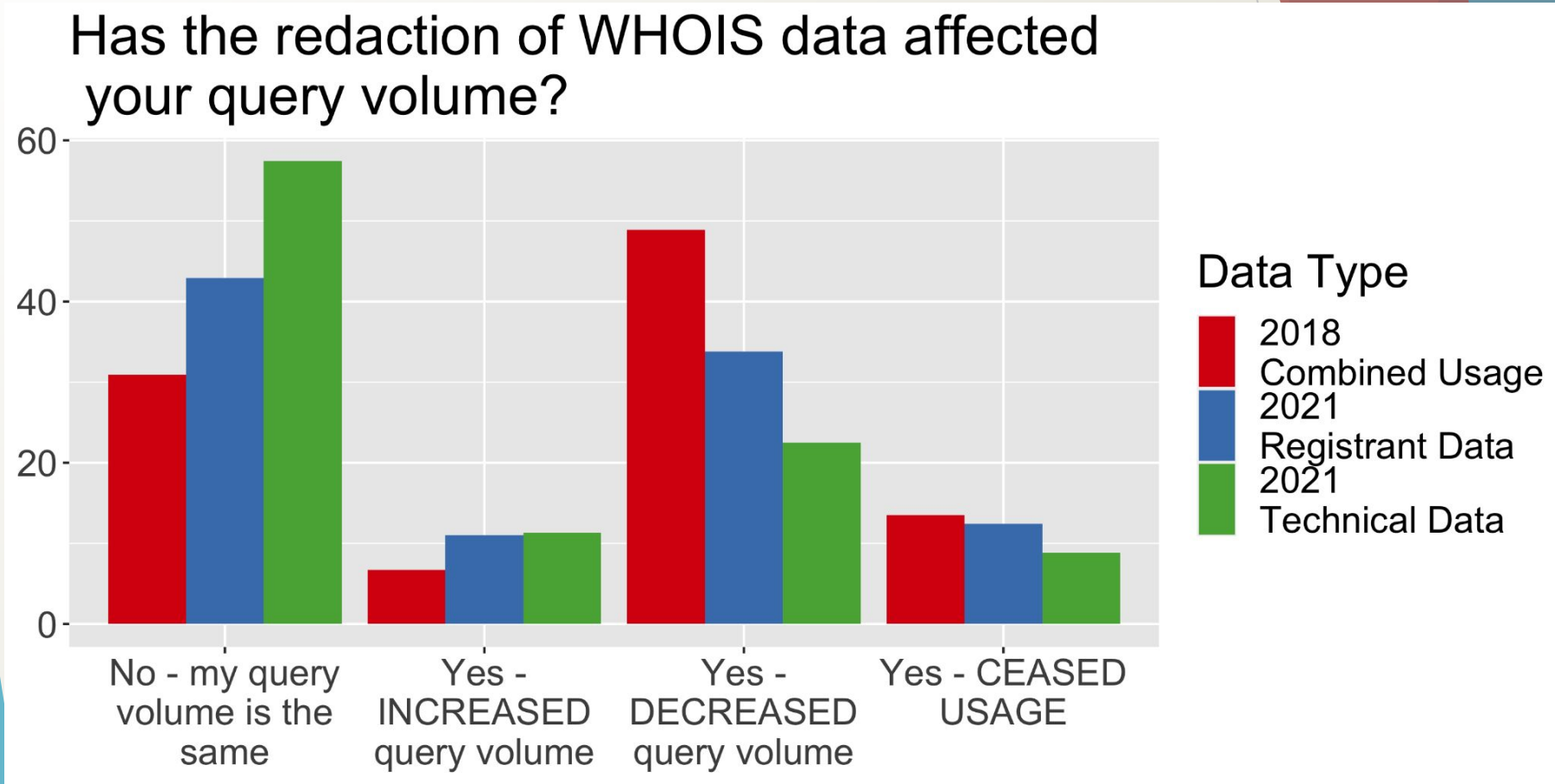
- Different users have different needs and use cases
  - How many records are accessed?
  - What happens with these records?
  - What properties are needed for data to be actionable/useful?
  - How quickly are these data required?

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

Demographics and Use of WHOIS



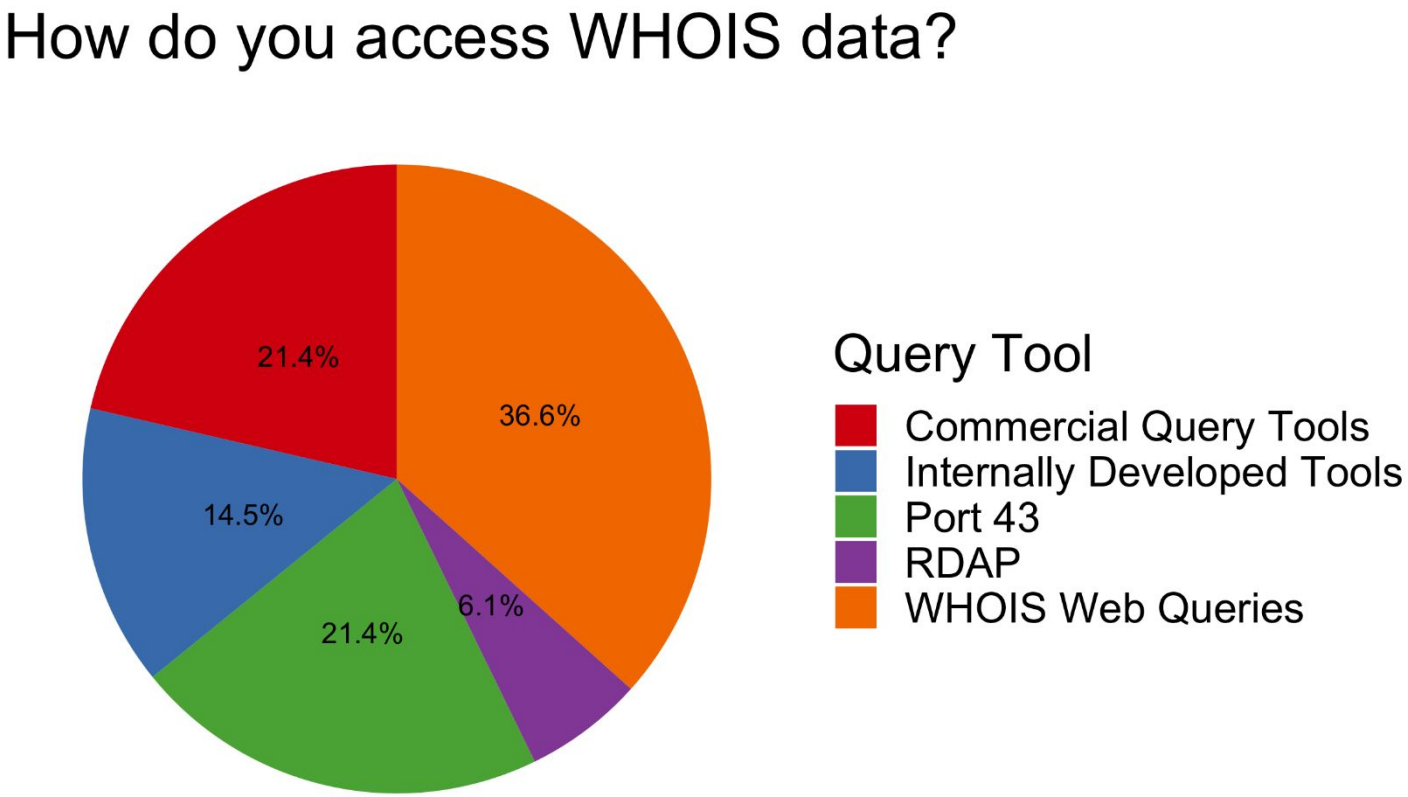
The Effect of the "Temp Spec" on WHOIS Use



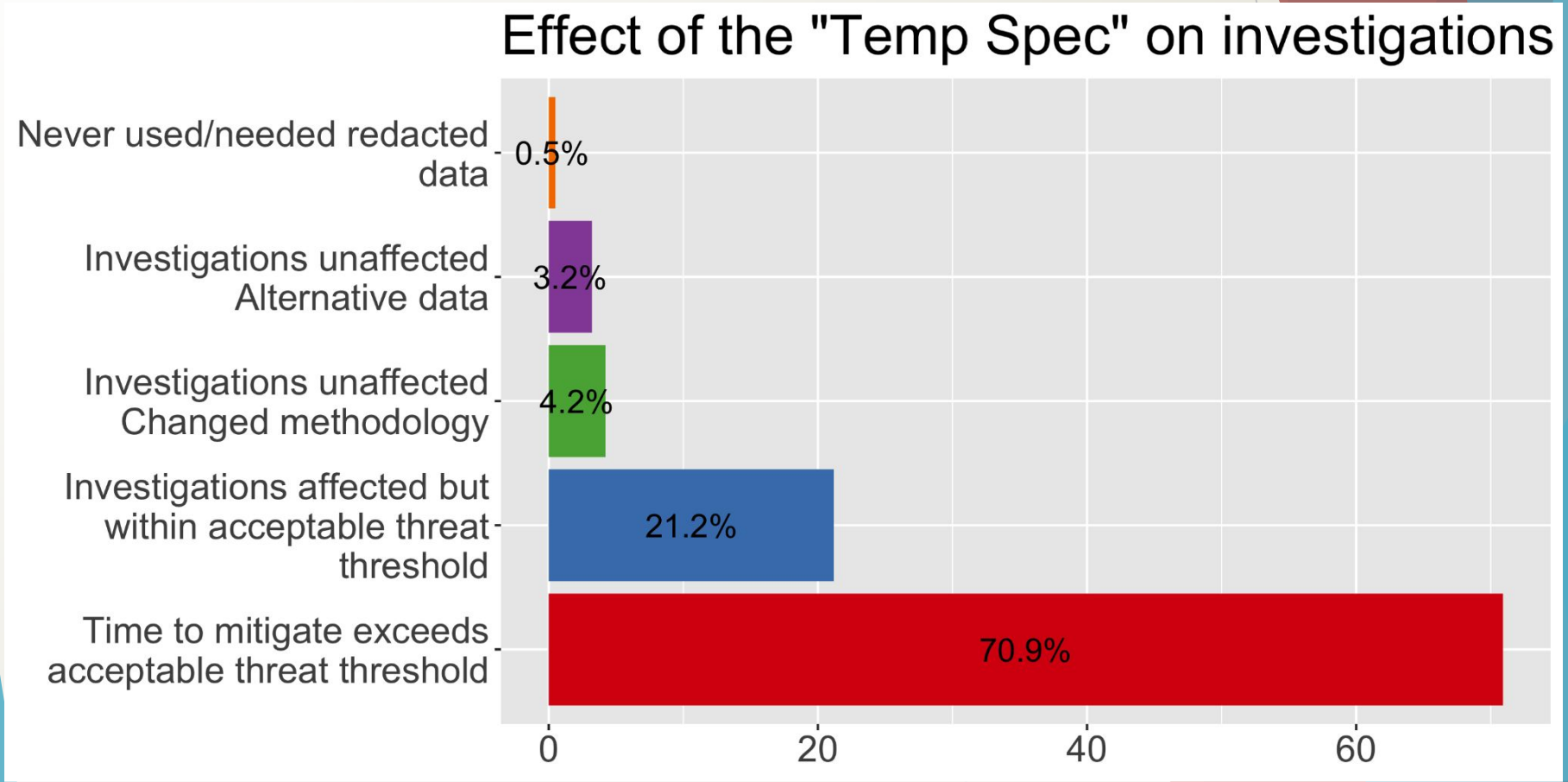
WHOIS Use

- 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.

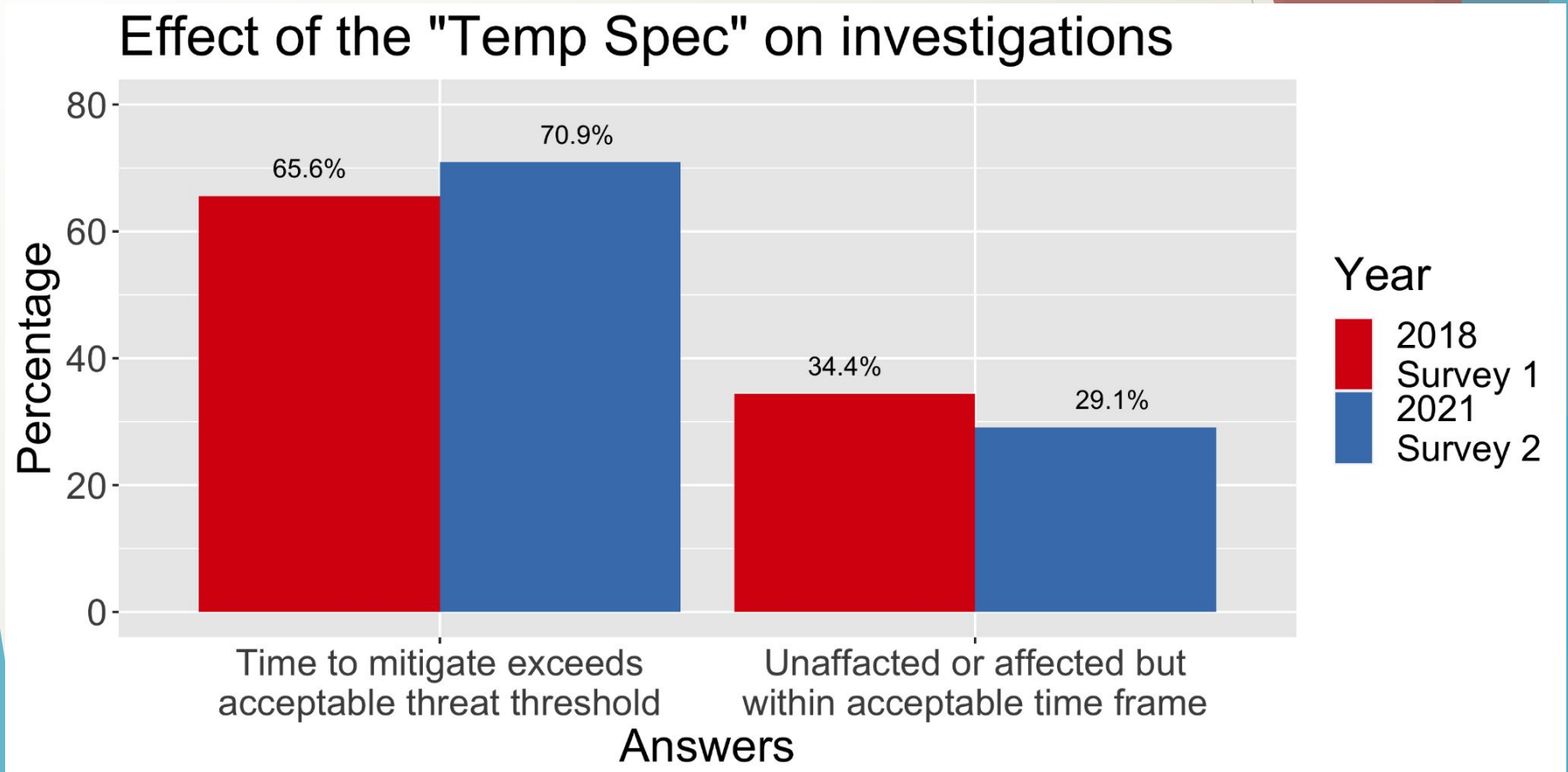
Demographics and Use of WHOIS



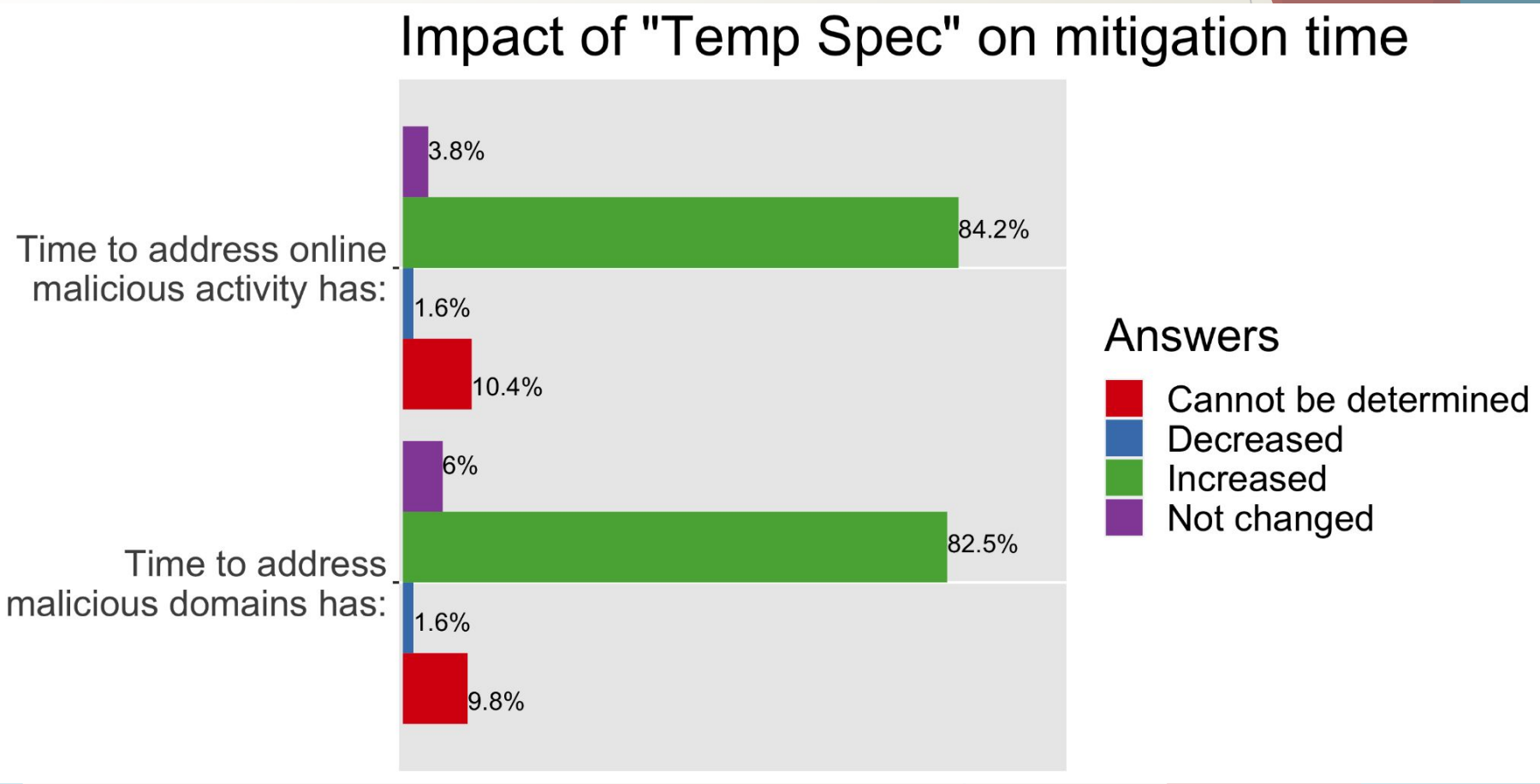
The Effect of the Temporary Specification on WHOIS



The Effect of the Temporary Specification on WHOIS



The Effect of the Temporary Specification on WHOIS

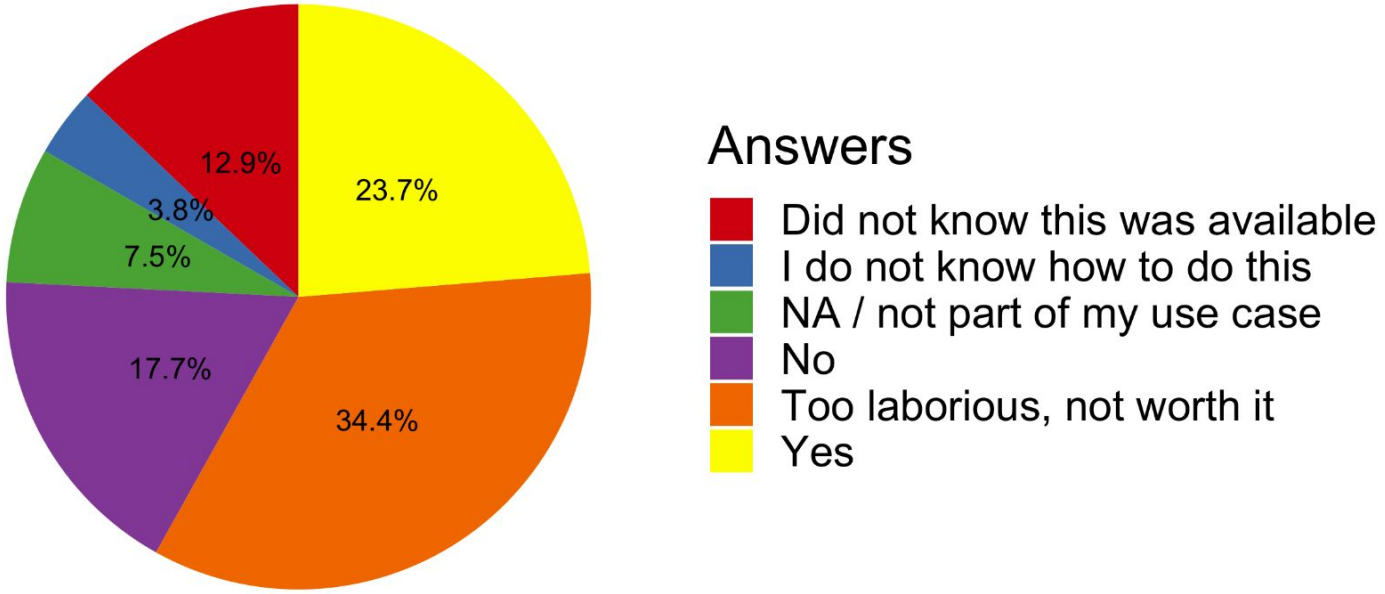


Summary of Issues

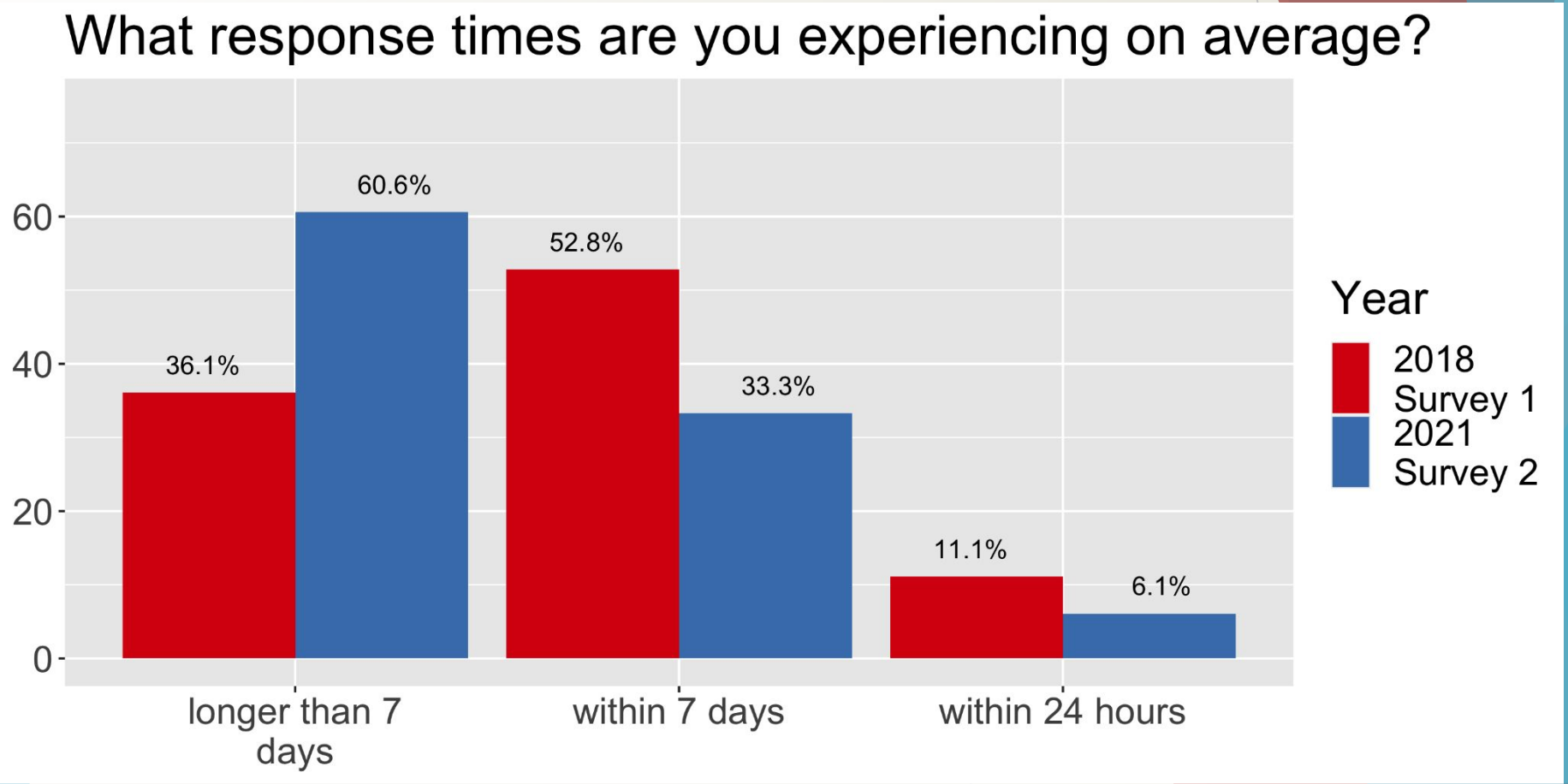
Generally, many use cases of WHOIS data are affected:

- 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.

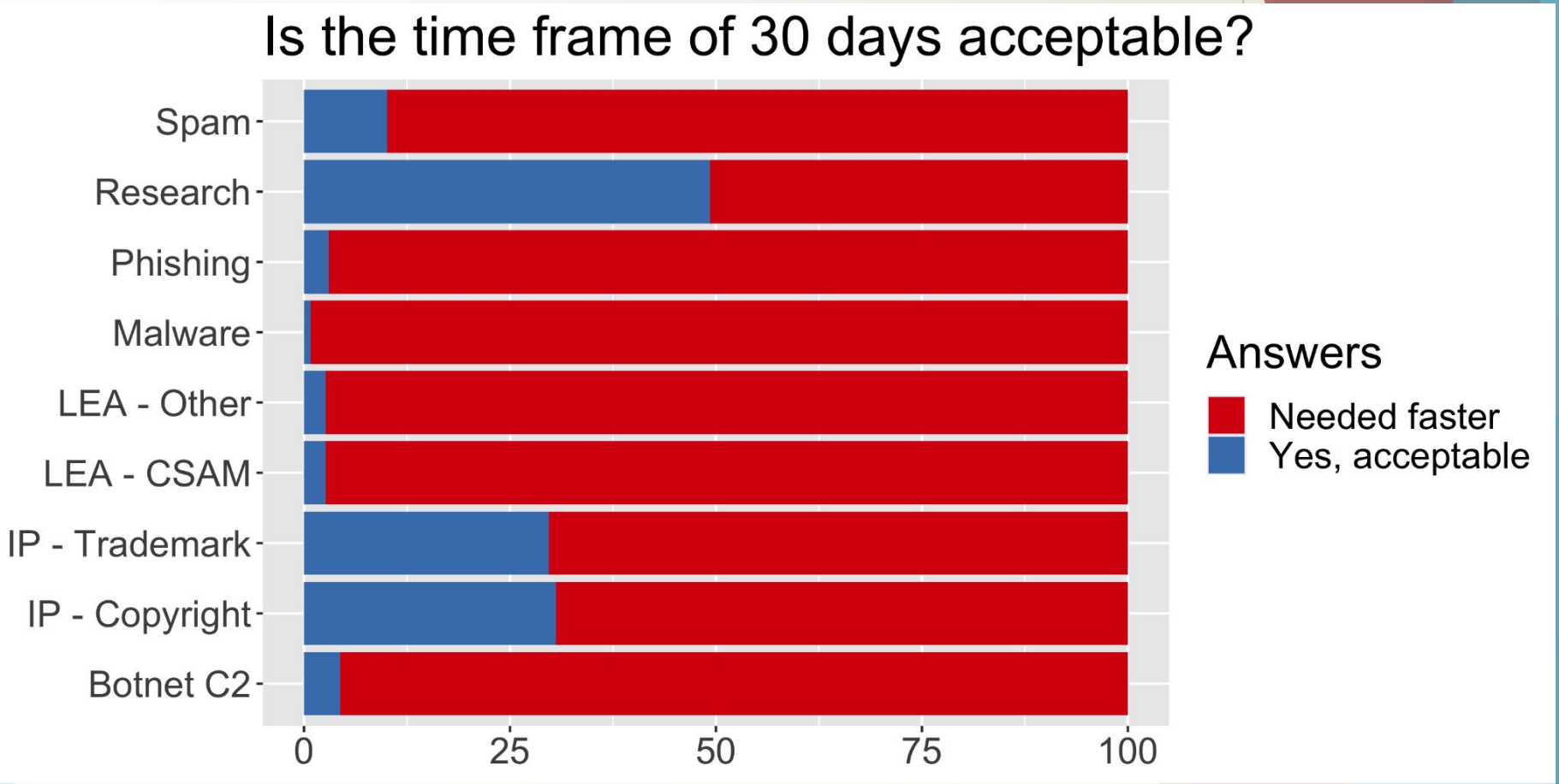
Disclosure of Redacted Data



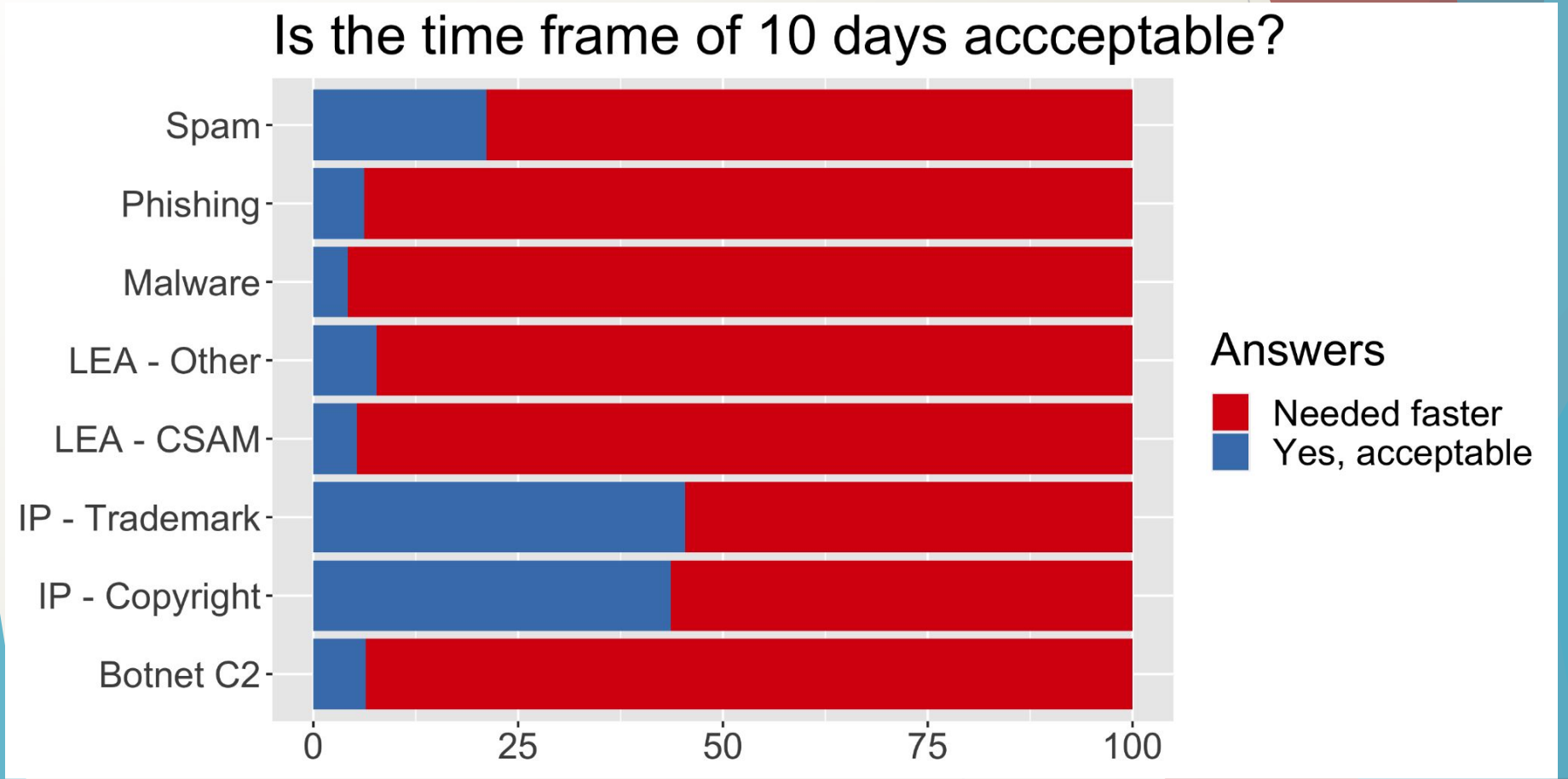
Disclosure of Redacted Data



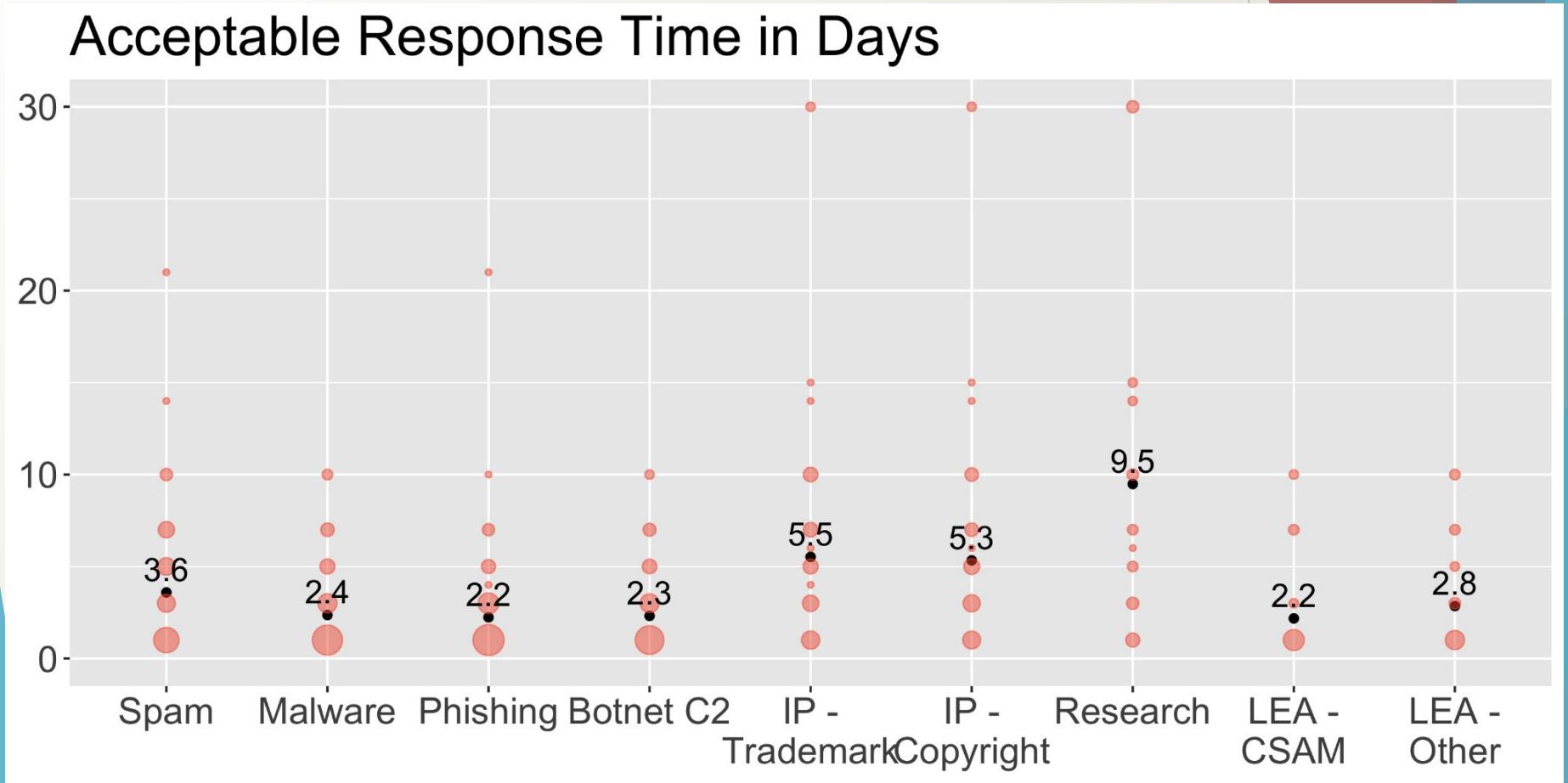
Disclosure of Redacted Data



Disclosure of Redacted Data



Disclosure of Redacted Data



Responses

Respondents report inconsistent behavior after requesting disclosure.

However, according to our respondents, the overwhelming majority of requests are:

- not acknowledged
- denied without explanation
- or answered with fake or otherwise non-actionable data

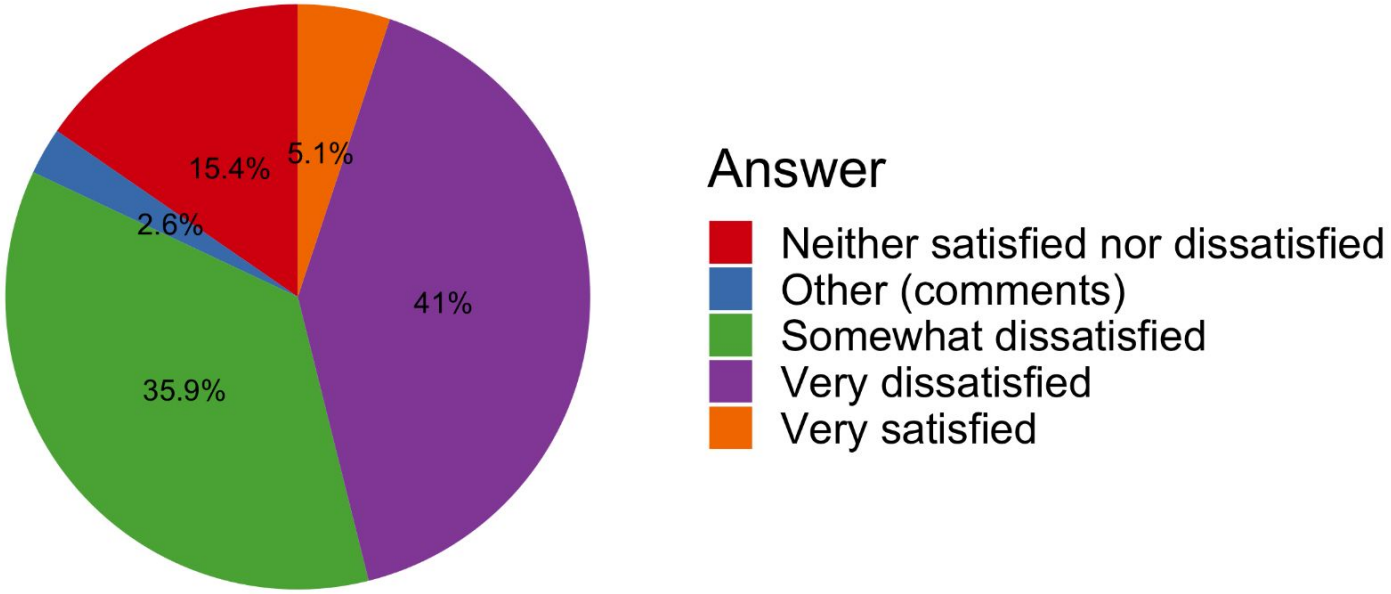
Disclosure Systems under ICANN consideration

- 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 and Conclusions from the Data

- 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.
- Respondents call for a functional system of registrant data access for accredited parties, workable in terms of time delays and administrative burden. It 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.

Next Steps

This presentation was about data and reporting on what our respondents told us.

M3AAWG will focus on the policy issues and potential solutions in the coming months, leveraging our members' breadth and depth of experience and expertise.

Contact Us

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