ICANN 76
COMMUNITY FORUM

CANCÚN

11-16 March 2023

ccTLD DNS ABUSE SURVEY

TRENDS & INSIGHTS

ccNSO DNS Abuse Standing Committee (DASC) ICANN76

About the ccNSO DNS Abuse Standing Committee (DASC)

1. Share information, insights and practices
2. Raise understanding and awareness
3. Promote open and constructive dialogue
4. Assist ccTLD managers in their efforts to mitigate the impact ofDNS Abuse

DASC does not formulate any policy or standards: out of scope of the ccNSO policy remit

About the DASC survey

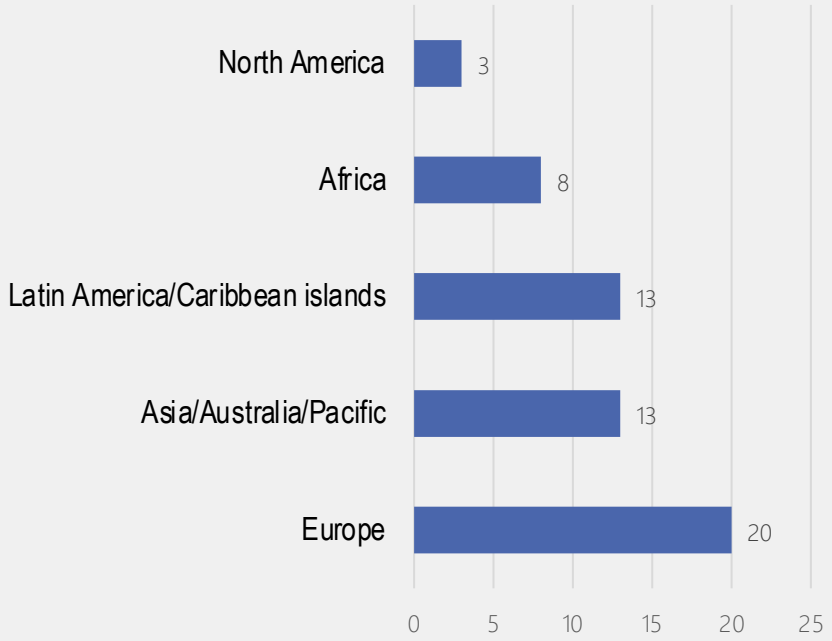
- Open: September ‘22 - end November ‘22
- All ccTLDs were invited to respond, regardless of ccNSO membership
- 57 unique responses. Estimate: representing approx. 100 ccTLDs
  - 316 delegated ccTLDs in total (ASCII & 61 IDN alike)
  - Some ccTLD managers provide services for multiple ccTLDs, but responded for 1 TLD only
  - Some ccTLD managers informed DASC they could not respond, for various reasons
  - Some ccTLDs responded multiple times: latest submission as final one
  - Some responses were incomplete
- About half of the respondents did not want their ccTLD mentioned


DEMOGRAPHICS

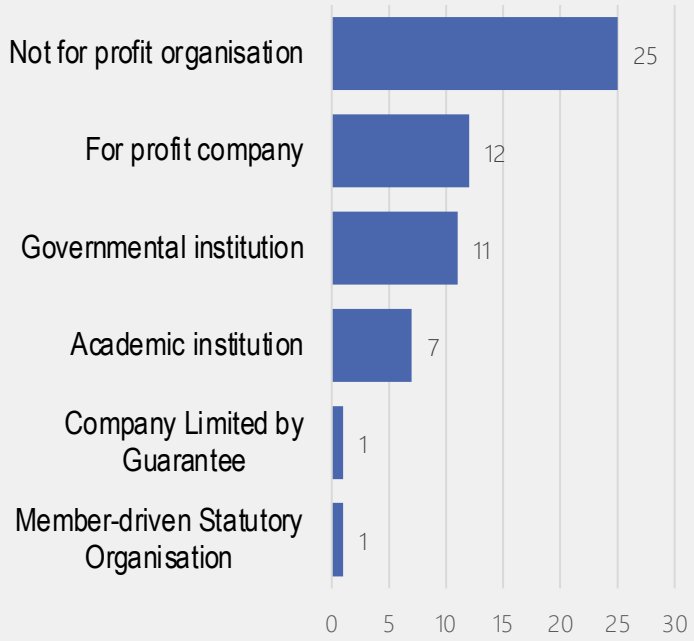
DEMOGRAPHICS

One size does not fit all: the ccTLD landscape is diverse

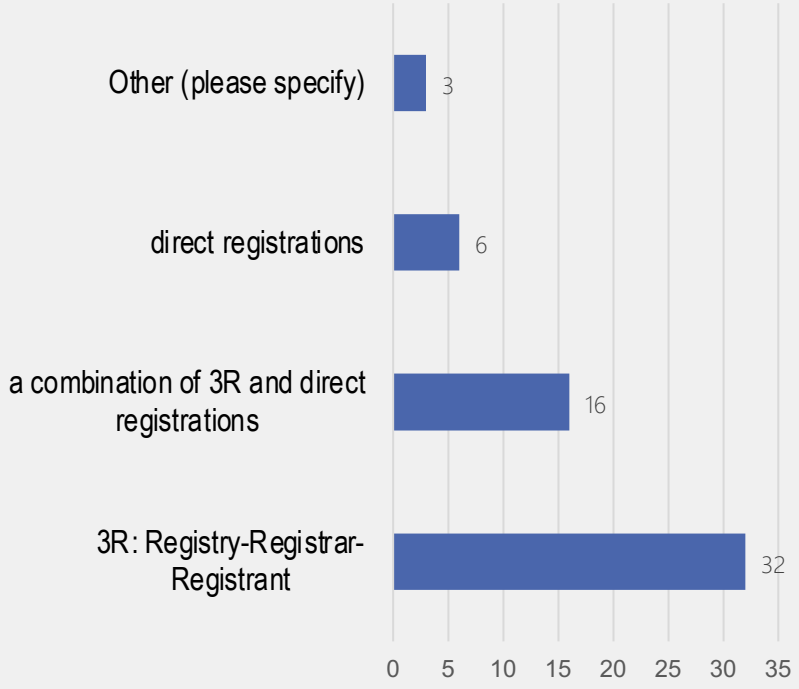
Select the ICANN geographical region for your ccTLD



What is the governance model of your ccTLD?



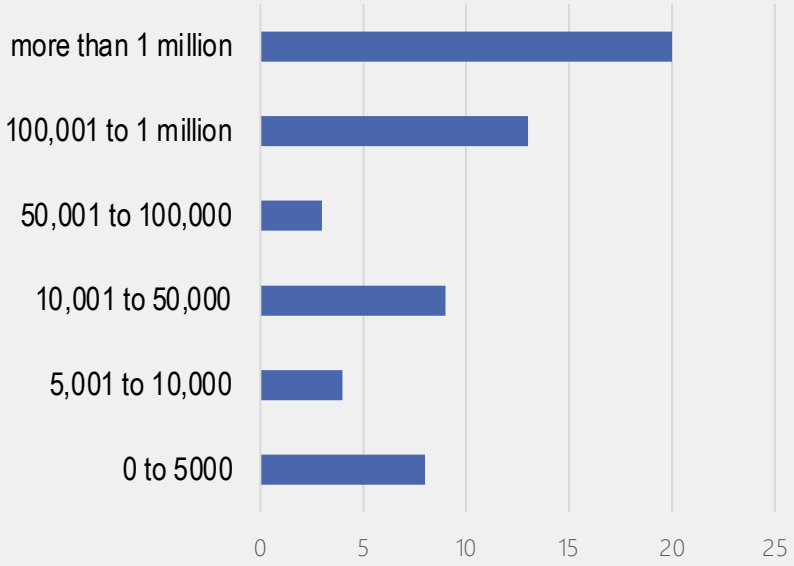
Which registration model do you follow?



DEMOGRAPHICS

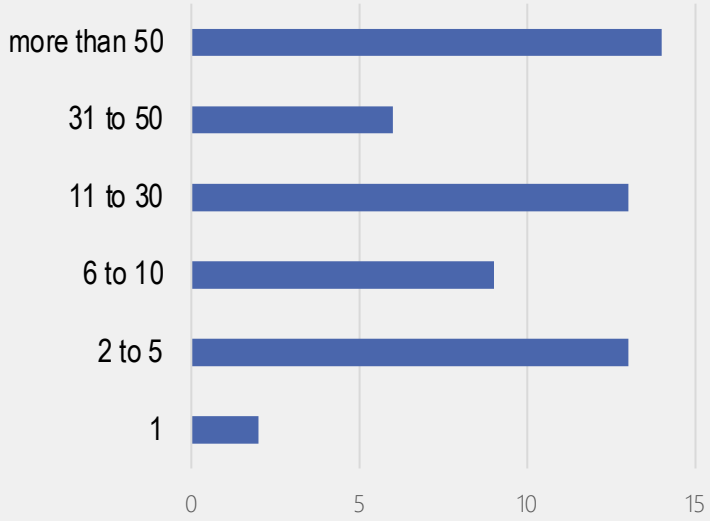
One size does not fit all: the ccTLD landscape is diverse

What is the number of registered domain names by your ccTLD?



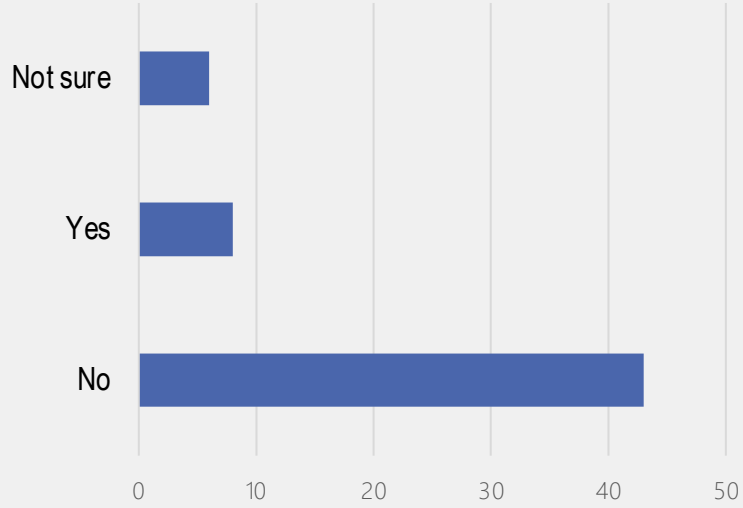
A significant number of respondents have > 1 million domains. On average, respondents have over 10k domains

How many employees (Full Time Equivalents) work within the registry/registry department?



Big diversity in terms of ccTLD staffing.

My ccTLD has an DNS Abuse Officer as part of the registry.

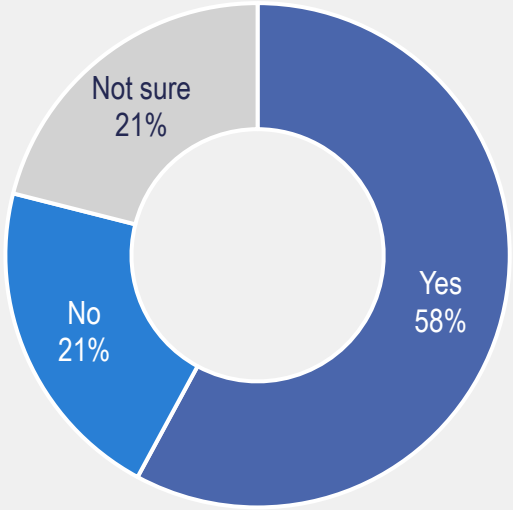


Over 75% of the respondents indicated they do not have a dedicated DNS Abuse Officer

DEMOGRAPHICS

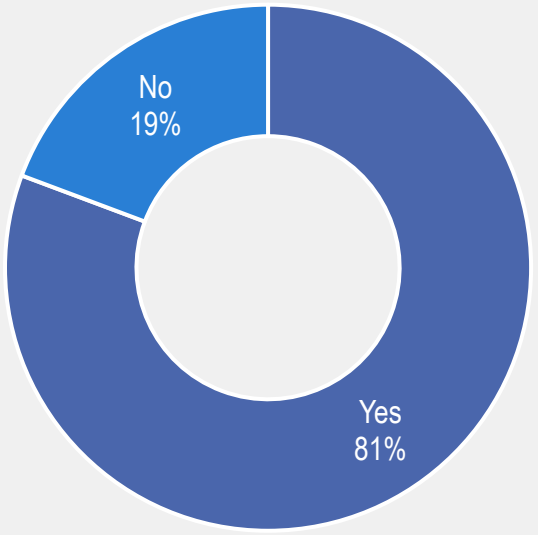
One size does not fit all: the ccTLD landscape is diverse

Data Protection legislation affects my ccTLD.



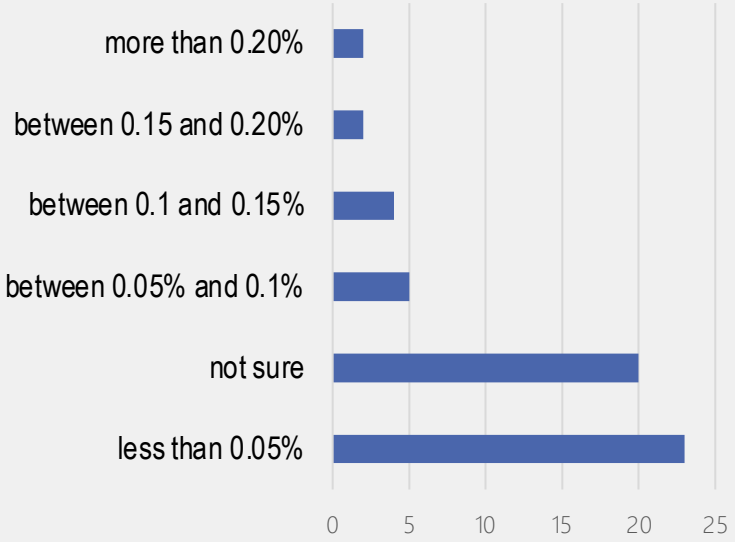
Close to 60% of the respondents stated they are affected by Data Protection legislation.

ccTLD Participates in Some Form of Collaboration

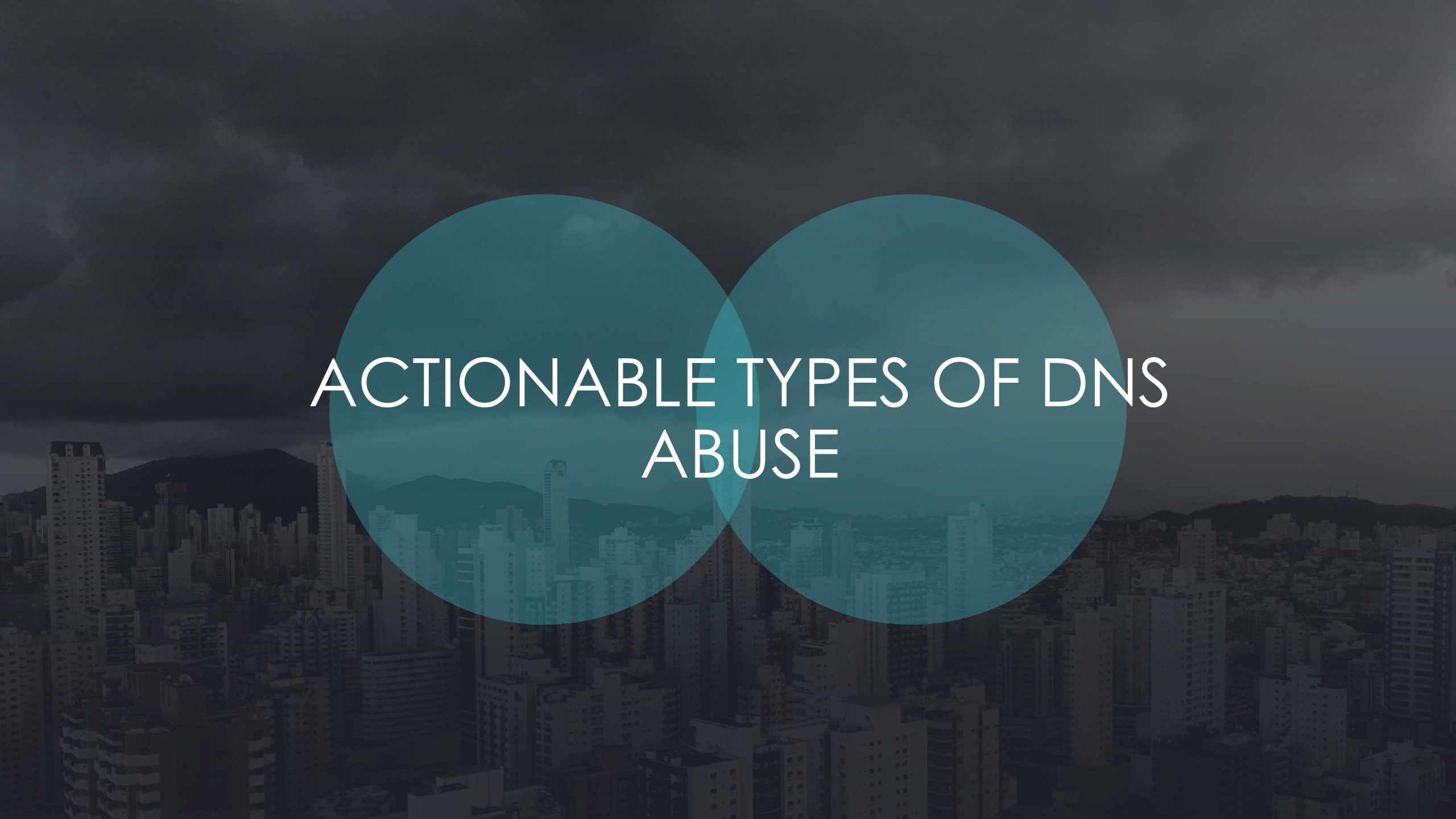


Over 80% of the respondents collaborate with either national Computer Security Incident Response Teams, Law Enforcement Agencies or Trusted Notifiers.

Approximately what % of domains do you believe are subject to DNS Abuse in your ccTLD?



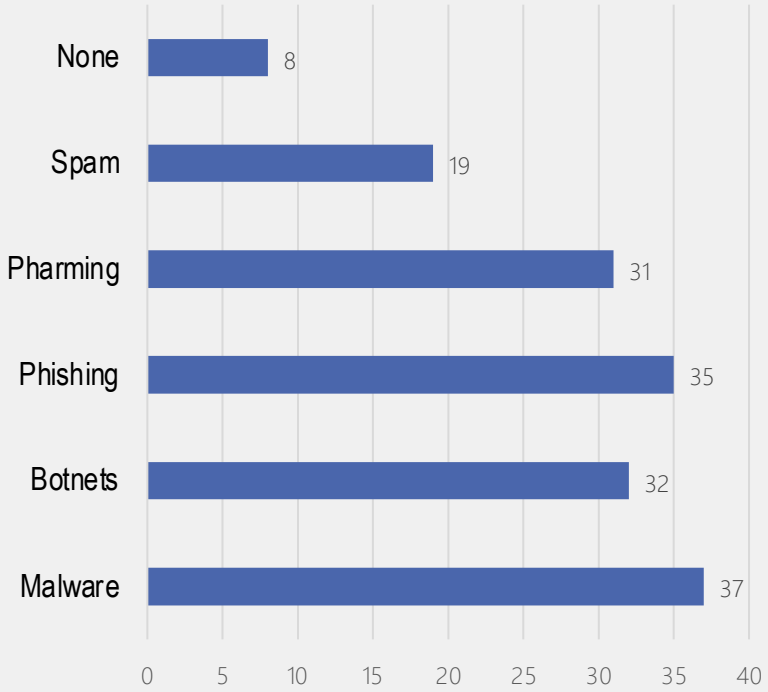
Most respondents indicated that less than 0.05% of their domain names under management are subject to DNS Abuse. 35% was not sure


ACTIONABLE TYPES OF DNS ABUSE

TYPES OF DNS ABUSE

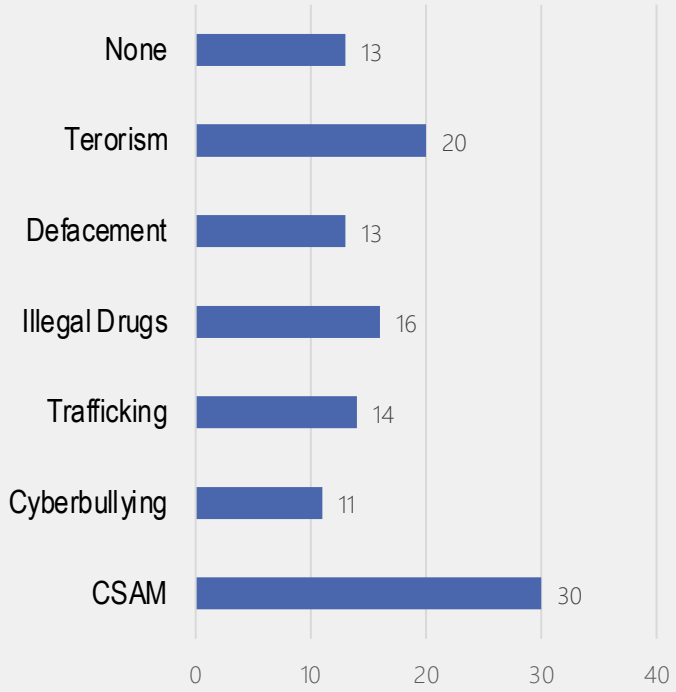
Where do the respondents take action?

DNS Abuse



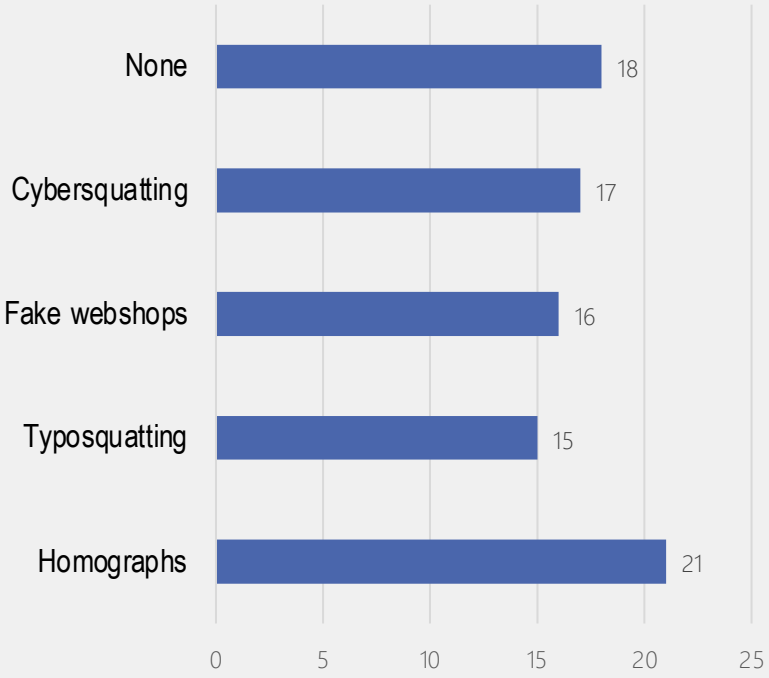
Most respondents consider Malware, Phishing, Botnets and Pharming to be actionable, and Spam to a lesser extent.

Content Abuse



Most respondents will take action on Child Sexual Abuse Materials.

Trademark Infringements



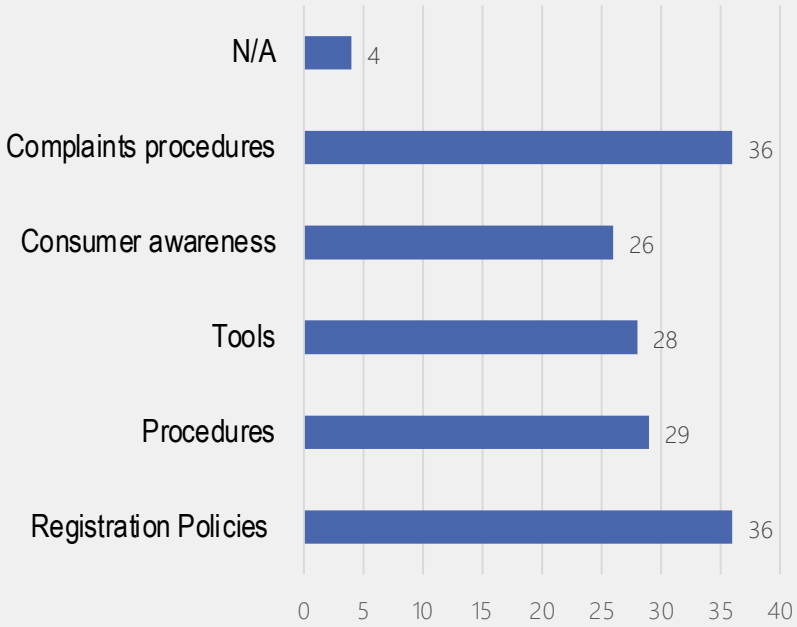
Most respondents will take action on homograph infringements. Some respondents indicated they never take action on the listed types of abuse.

DNS ABUSE MITIGATION: TRENDS

DNS ABUSE MITIGATION: TRENDS

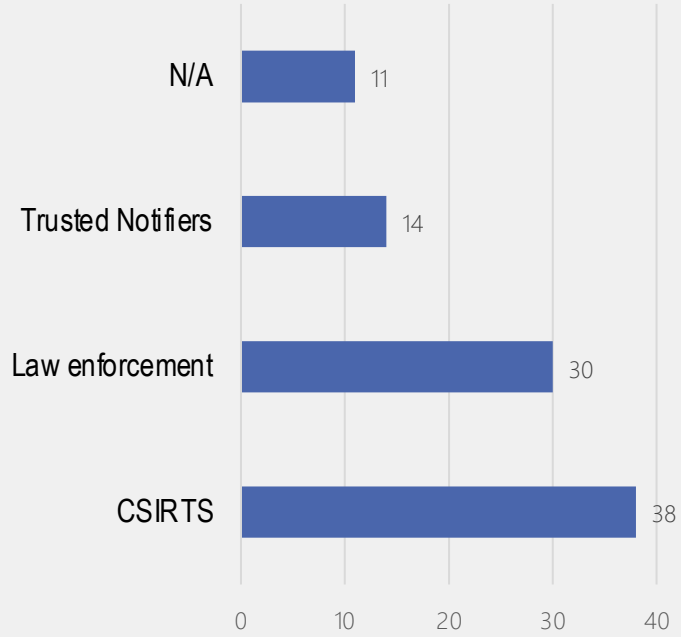
What do the numbers say?

To mitigate DNS Abuse, my ccTLD uses the following methods:



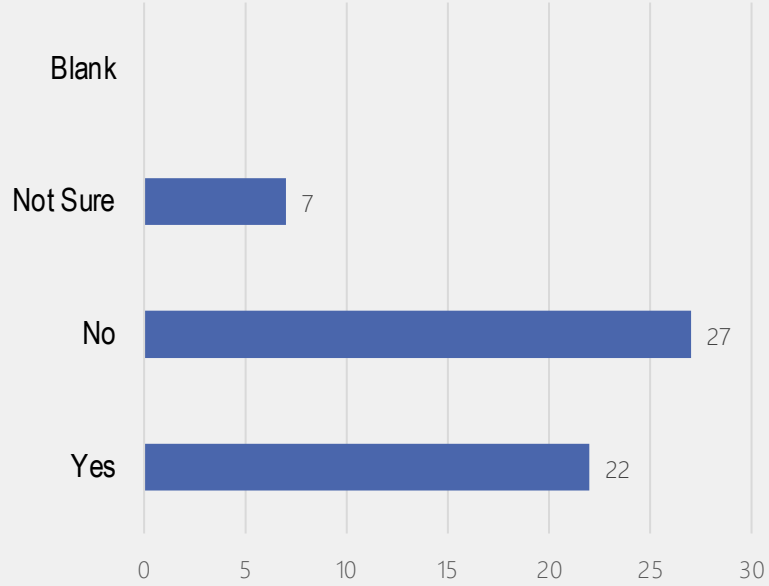
Respondents indicated a high reliance on a Registration policies and Complaints procedures.

My ccTLD has a collaborative relationship with:



Most respondents stated they have a collaborative relationship with national Computer Security Incident Response Teams and Law enforcement.

My ccTLD does outreach/education to registrars/registrants, related to DNS Abuse

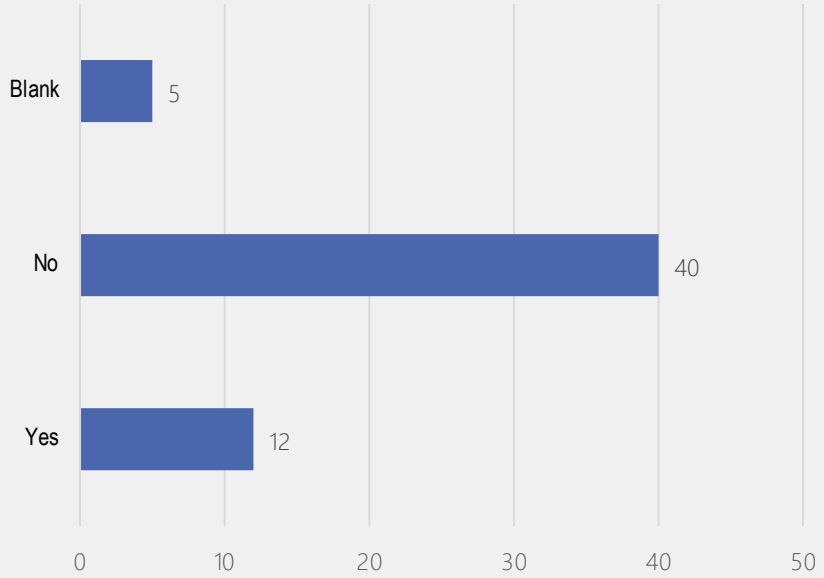


Most respondents do not have any outreach or educational activities regarding DNS Abuse

TRENDS ON DNS ABUSE MITIGATION

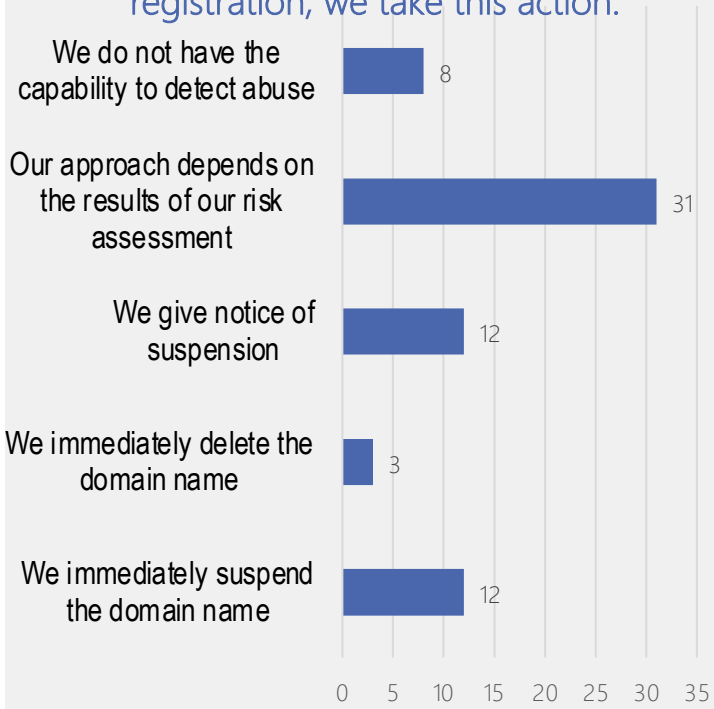
What do the numbers say?

My ccTLD has entered into a Trusted Notifier arrangement to address DNS Abuse



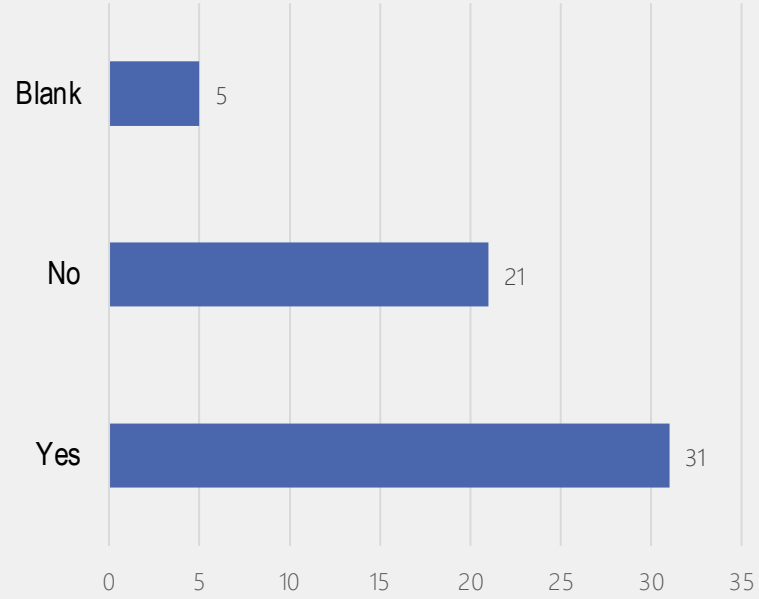
The majority of the respondents have not entered into a Trusted Notifier arrangement.

If my ccTLD detects abuse, post-registration, we take this action:



When an abuse issue is detected once the domain name is already registered, the type of action for most respondents depends on the results of their internal risk assessment.

My ccTLD has mechanisms in place for members of the public to report DNS abuse



Most respondents indicated the availability of reporting mechanisms regarding DNS abuse for members of the public.


TOOLS & FEEDS
Commercial, Open Source, or Both?

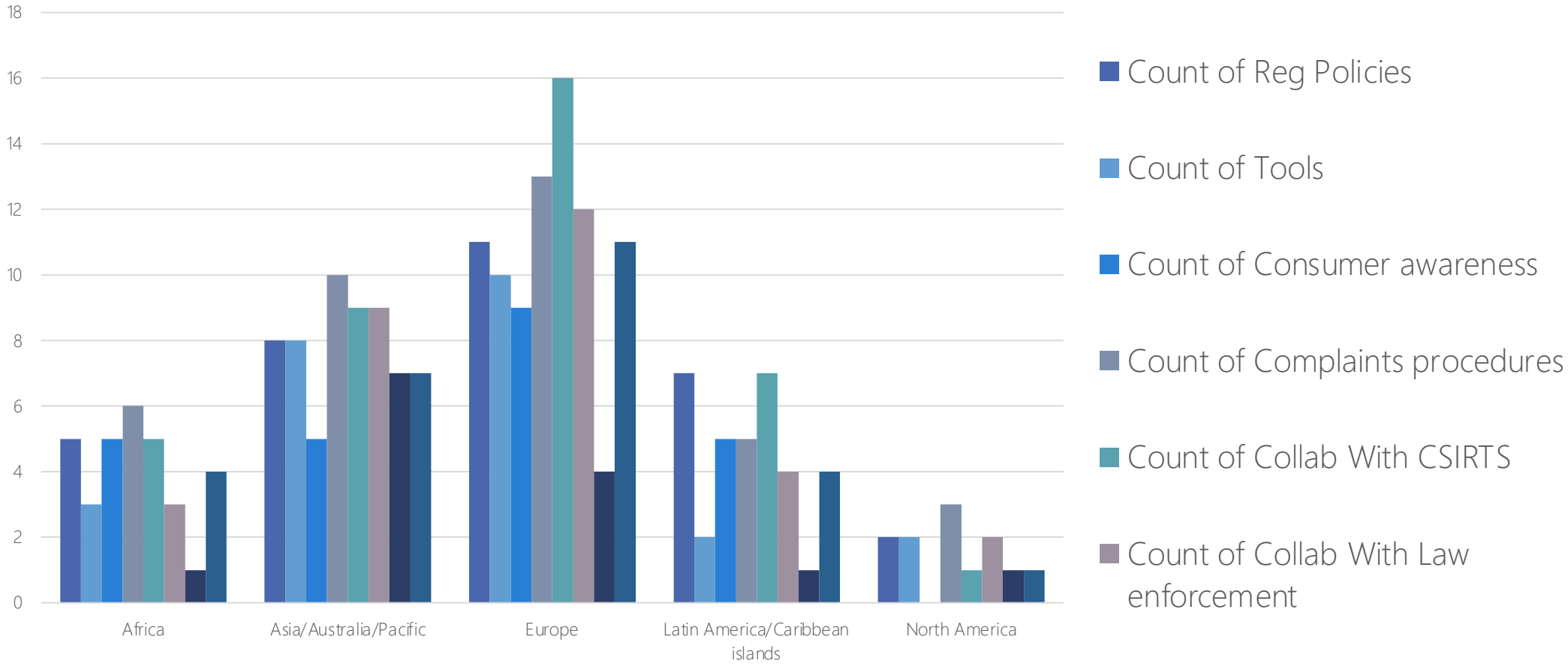
Common tools used by ccTLDs

Open Source	Commercial
DGArchive Shadowserver OpenPhish (Community) PhishTank	SURBL Spamhaus Anti-Phishing Working Group (APWG) Netcraft Sophos Recorded Future Malware Bytes Malware Patrol IQ Global (aggregation of feeds)

OTHER FINDINGS

Combining demographics and trends

Mitigation by demographics: region



More to come!

Stay tuned

Angela Matlapeng

Bruce Tonkin

Tatiana Tropina

Nick Wenban-Smith

DASC survey subgroup

- Angela Matlapeng (.bw)
- Bruce Tonkin (.au) | Chair DASC survey subgroup
- Tatiana Tropina (NomCom appointed ccNSO Council member)
- Nick Wenban Smith (.uk) | Chair DASC
- Brett Carr (former member)

https://ccnso.icann.org/en/workinggroups/dasc.htm


THANK YOU