ccNSO DNS Abuse Standing Committee

DASC survey webinar, 28 September 2023

ICANN | ccNSO

Country Code Names Supporting Organization

About the ccNSO DNS Abuse Standing Committee (DASC)

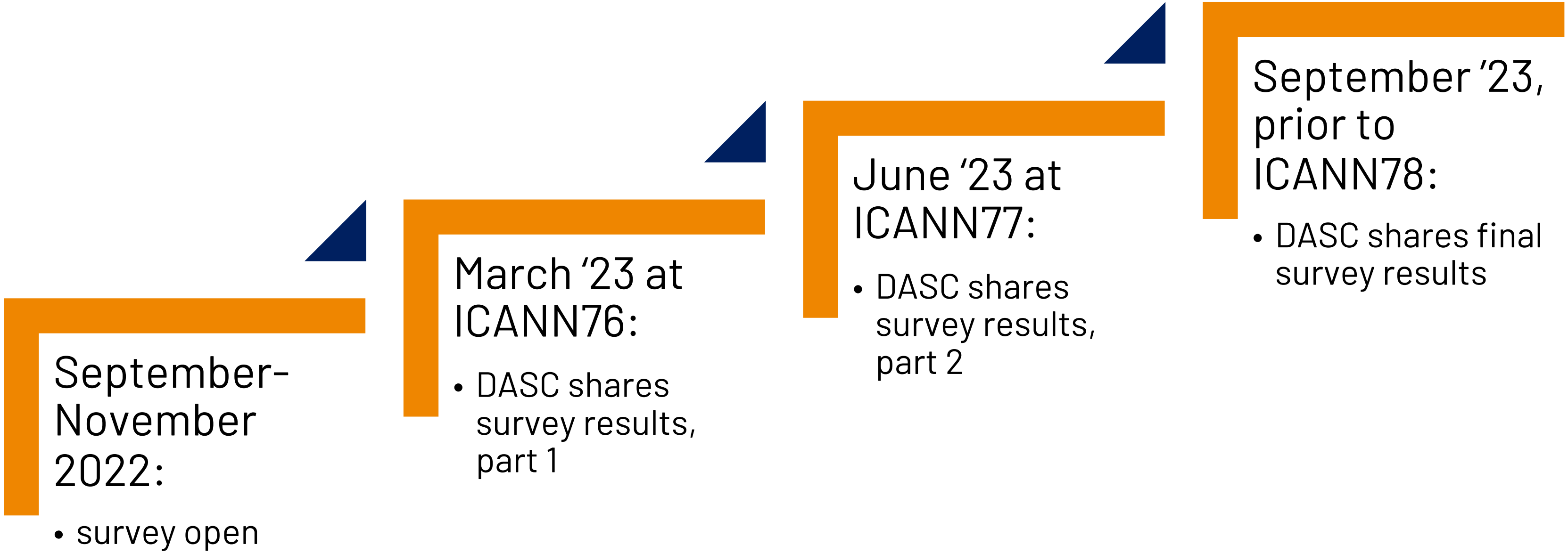
1. Share information, insights and practices
2. Raise understanding and awareness
3. Promote open and constructive dialogue
4. Assist ccTLD managers in their efforts to mitigate the impact of DNS Abuse

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

Timeline



September-November 2022:

- survey open

March '23 at ICANN76:

- DASC shares survey results, part 1

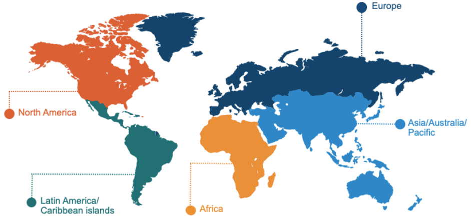
June '23 at ICANN77:

- DASC shares survey results, part 2

September '23, prior to ICANN78:

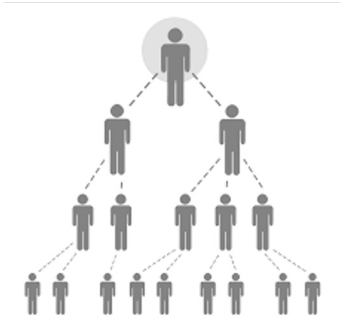
- DASC shares final survey results

What makes ccTLDs different?



Region

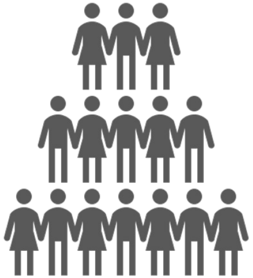
Governance model



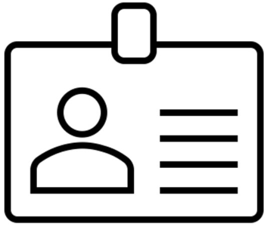
Registry model

% domains exposed to DNS Abuse

Number of domains



Number of employees



ccTLD has Abuse Officer

ccTLD is affected by DPL

What was shared previously?

ICANN76

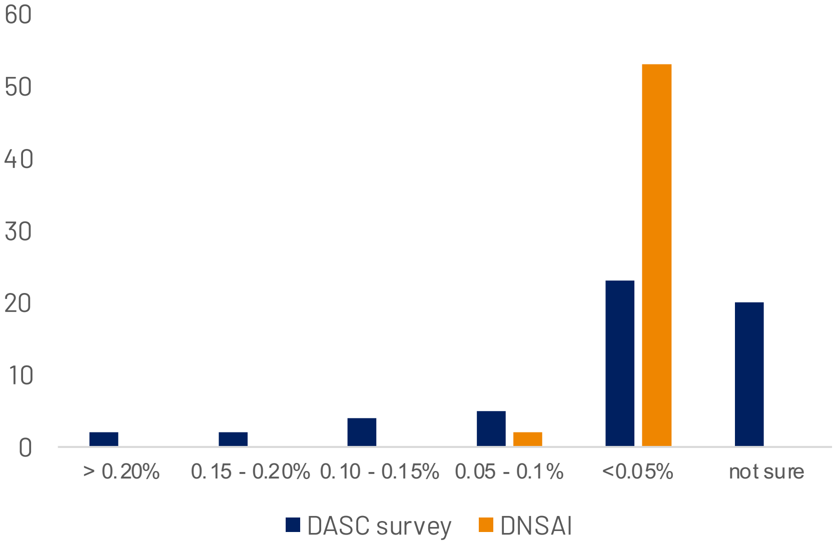
- Where and when do respondents take action?
- What are the DNS Abuse mitigation trends?
  - Mitigation methods, outreach & education to registrars
  - Trusted notifier arrangements, type of action when abuse is detected, reporting mechanisms for the public
- Tools & feeds
- Combined results: mitigation methods vs region, registry model, size

ICANN77

- Pre-registration
  - Which information is being collected?
  - Do respondents perform pre-registration verifications?
  - Do respondents perform checks at time of registration, and if so, for which data?
- Post-registration
  - Methods: manual vs automated
  - When do post-registration verifications happen?
- Mid-cycle
  - Type of action when abuse is detected, based on: Feed, LEA request, due diligence verifications
  - Measures to keep registration data accurate over time
- Renewal
  - Do respondents perform verifications?

What stood out?

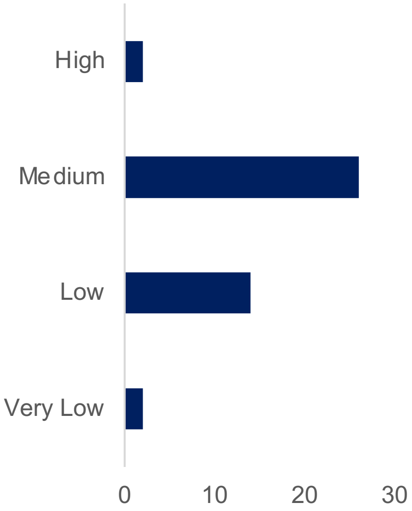
Comparison: survey responses vs DNSAI data



- Many respondents unsure about level of Abuse in their TLD. Hence, comparison with DNS Abuse Institute (DNSAI) data.
- DNSAI Compass data refers to phishing and malware only.
- Vast majority: less than 0.05% of abusive domains, less than 20 names reported as DNS Abuse.
- DNS Abuse rate of 0.05% means: only noticeable number (e.g. >100) for ccTLDs with large domain portfolio. This may explain why respondents were unsure about levels of abuse in their ccTLDs

What stood out?

Pricing variation across ccTLDs

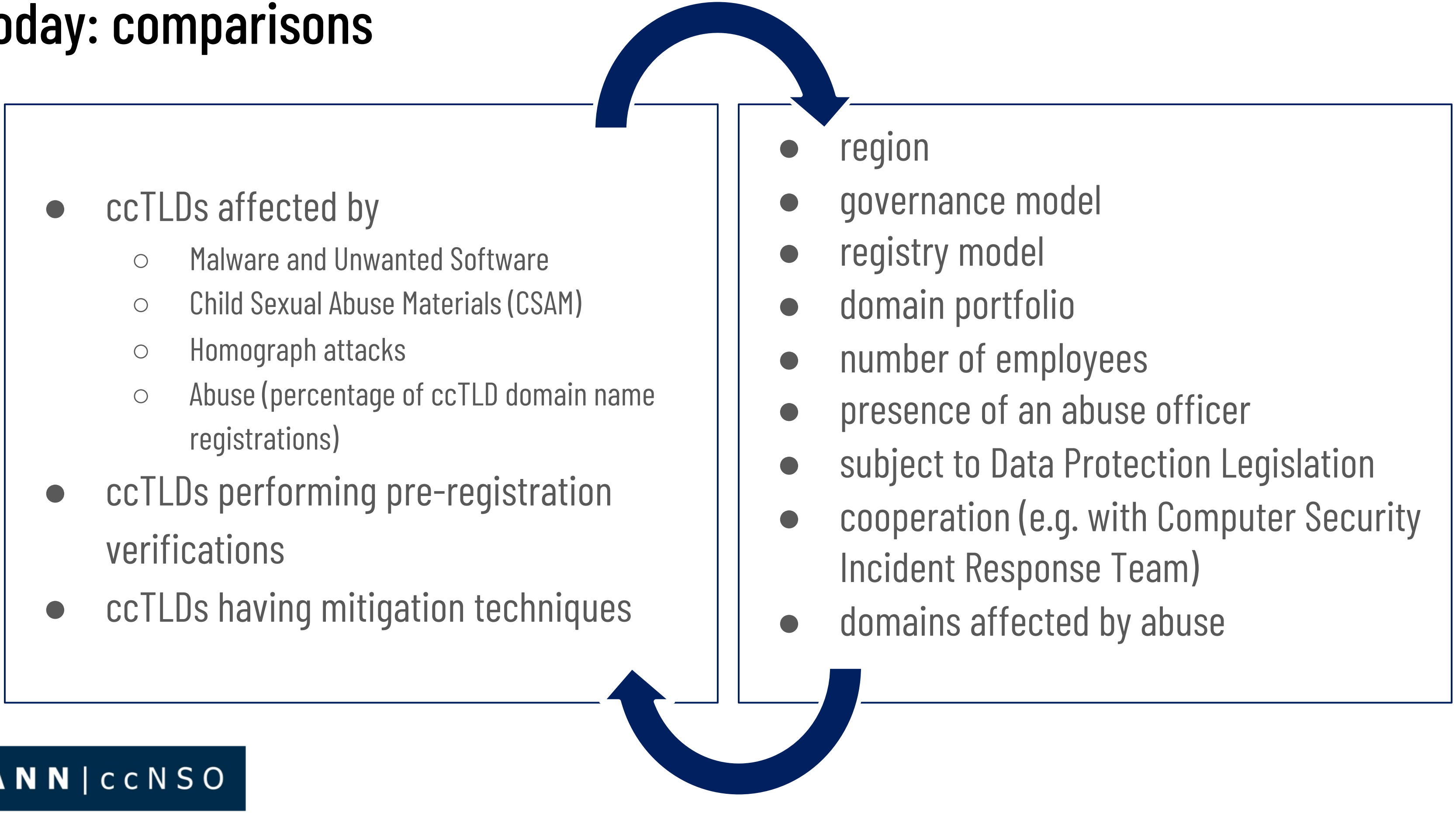


Legend
At retail level

High: > 100 USD
Medium: 21-99 USD
Low: 6-20 USD
Very Low: < 5 USD

- Largest ccTLDs in terms of volume of names generally in the low price range
- No discernible correlation of price with the level of DNS Abuse
- Data based on registrar and ccTLD registry pricing, where publicly available (44 ccTLDs)

Today: comparisons



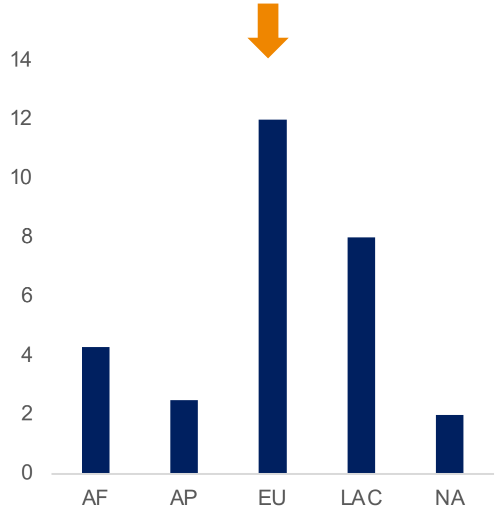
- ccTLDs affected by
  - Malware and Unwanted Software
  - Child Sexual Abuse Materials (CSAM)
  - Homograph attacks
  - Abuse (percentage of ccTLD domain name registrations)
- ccTLDs performing pre-registration verifications
- ccTLDs having mitigation techniques

- region
- governance model
- registry model
- domain portfolio
- number of employees
- presence of an abuse officer
- subject to Data Protection Legislation
- cooperation (e.g. with Computer Security Incident Response Team)
- domains affected by abuse

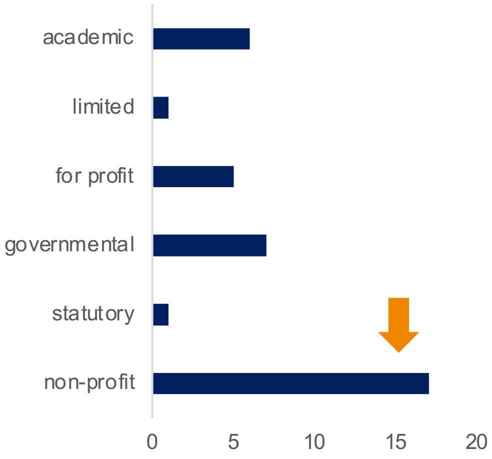
ccTLDs affected by Malware and Unwanted Software

ccTLDs affected by Malware and Unwanted Software

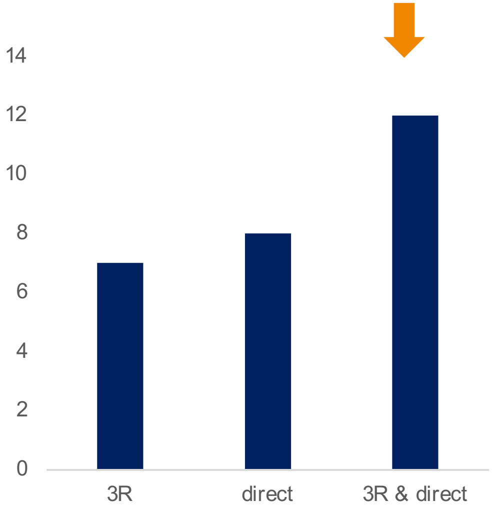
Region



Governance model

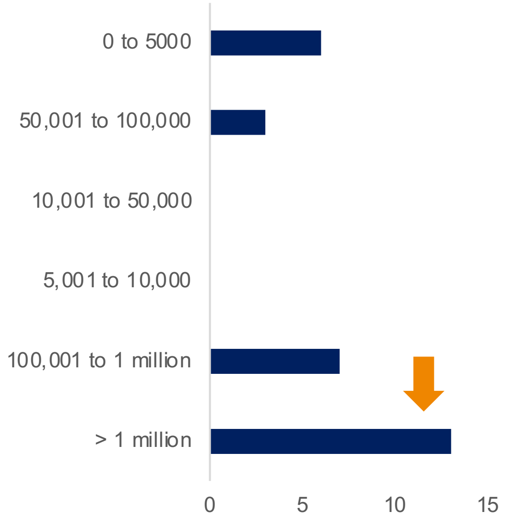


Registry model

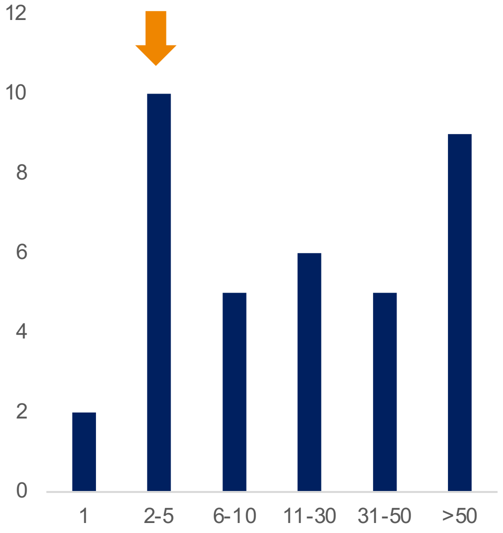


ccTLDs affected by Malware and Unwanted Software

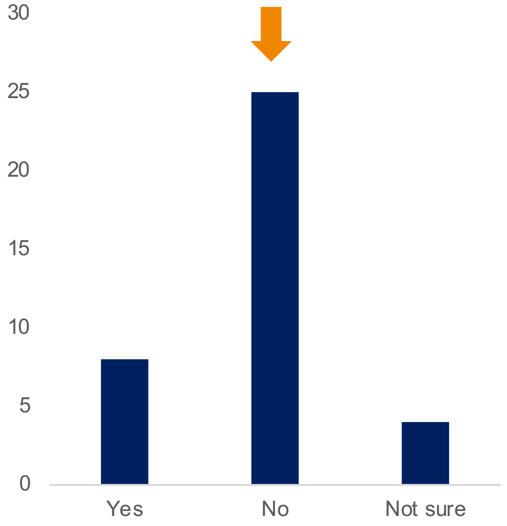
Domain portfolio



Employees

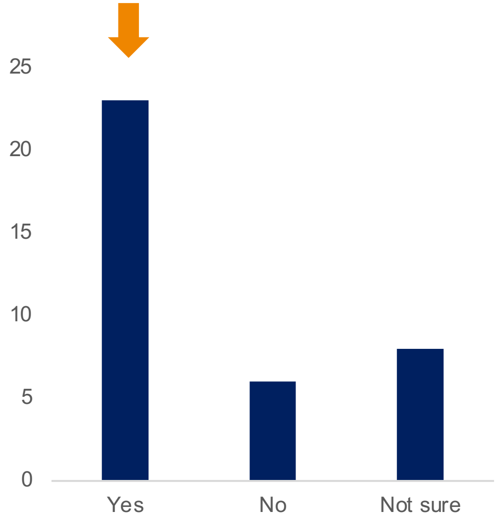


Abuse officer

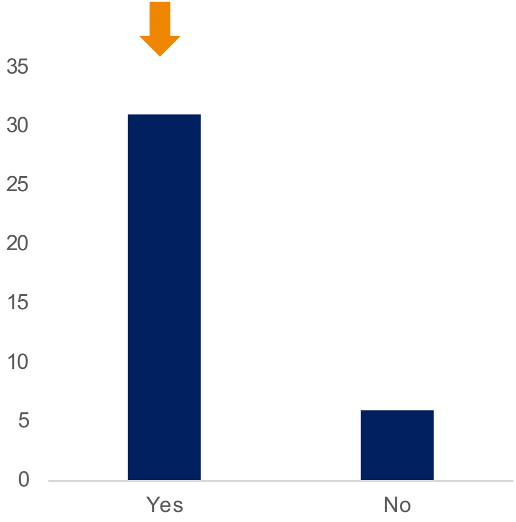


ccTLDs affected by Malware and Unwanted Software

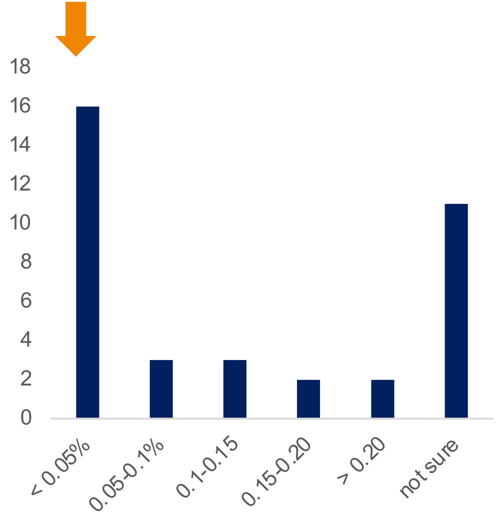
Subject to Data Protection Legislation



Cooperation (e.g. Computer Security Incident Response Team)



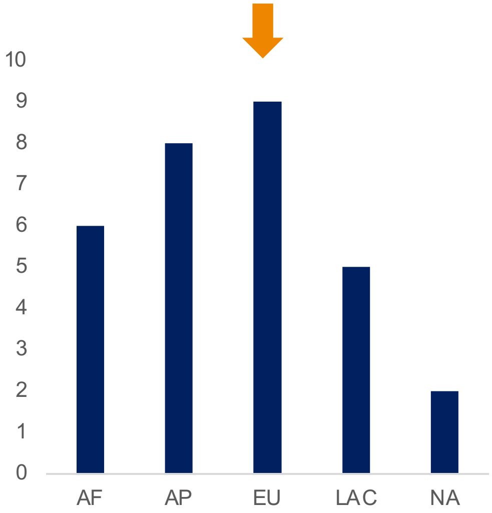
Domains affected by abuse



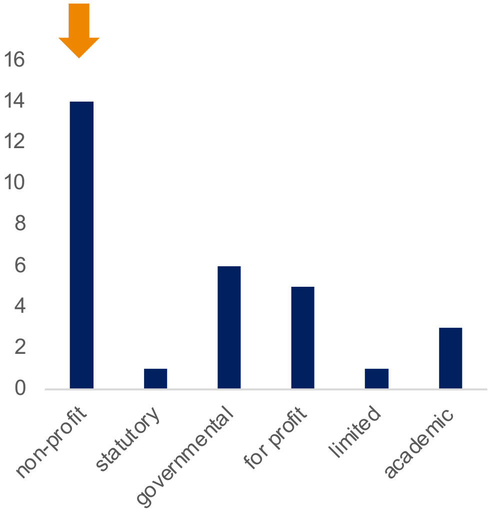
ccTLDs affected by Child Sexual Abuse Material (CSAM)

ccTLDs affected by Child Sexual Abuse Material (CSAM)

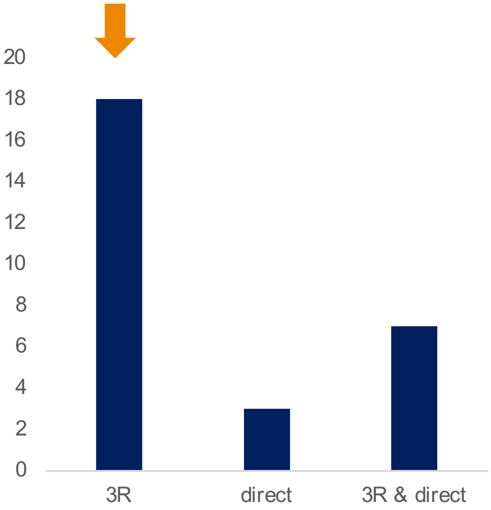
Region



Governance model

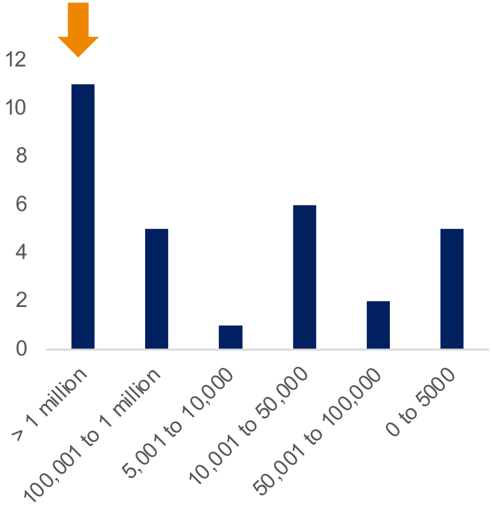


Registry model

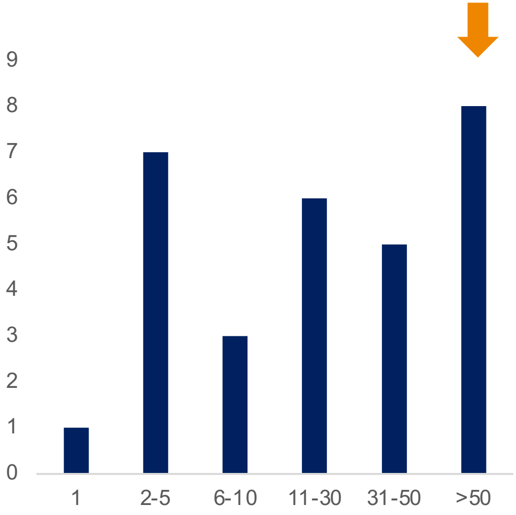


ccTLDs affected by Child Sexual Abuse Material (CSAM)

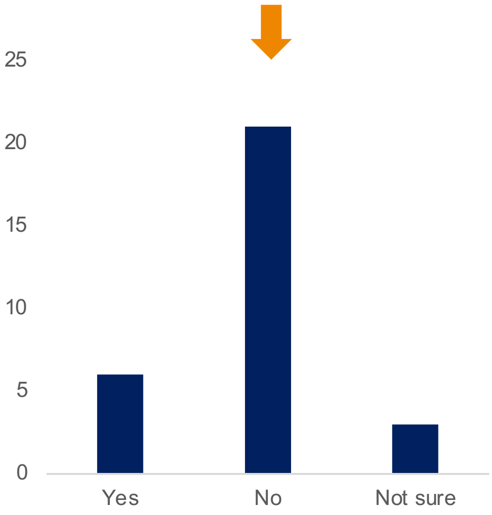
Domain portfolio



Employees

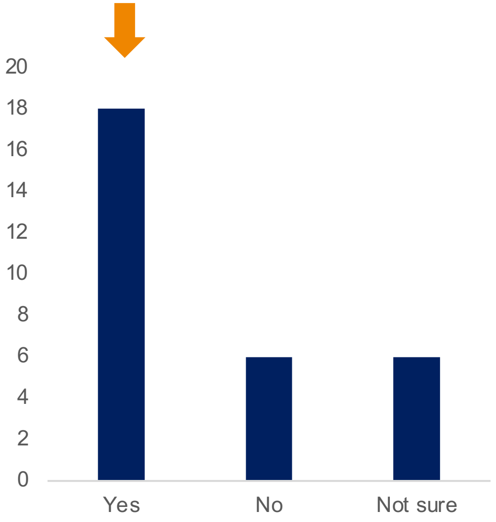


Abuse officer

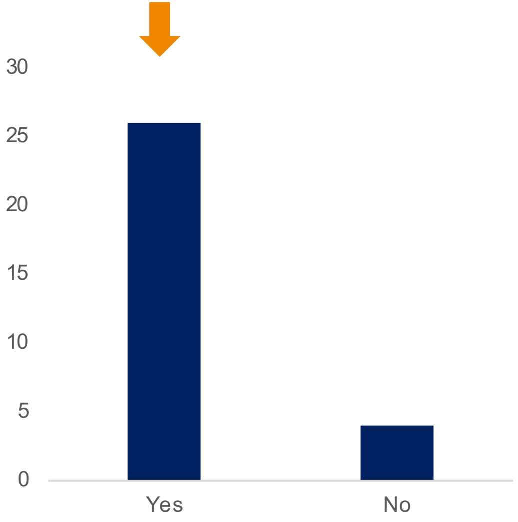


ccTLDs affected by Child Sexual Abuse Material (CSAM)

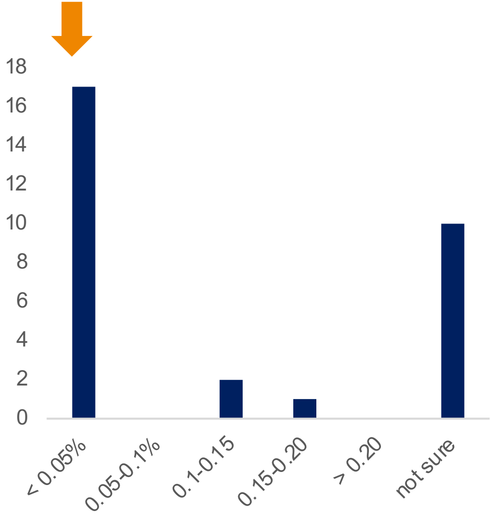
Subject to Data Protection Legislation



Cooperation (e.g. Computer Security Incident Response Team)



Domains affected by abuse



ICANN | ccNSO

ccTLDs affected by Homograph Attacks

What is a homograph attack?

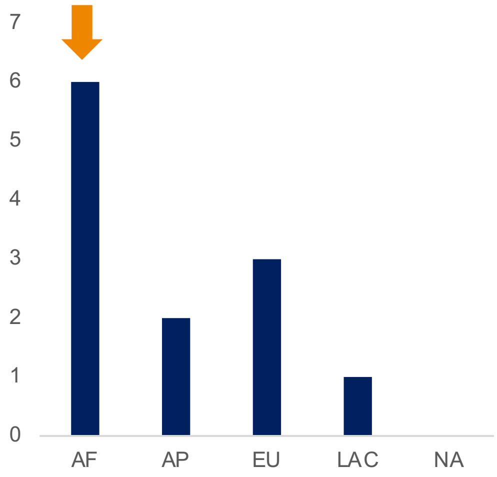
Homograph (also known as homoglyph) phishing attacks are based on the idea of using similar characters to pretend to be another site. While most of them are easily recognizable by end-users with proper training, the homograph attacks based on international domain names (IDN) can be unrecognizable from the domains they are spoofing.

Example:

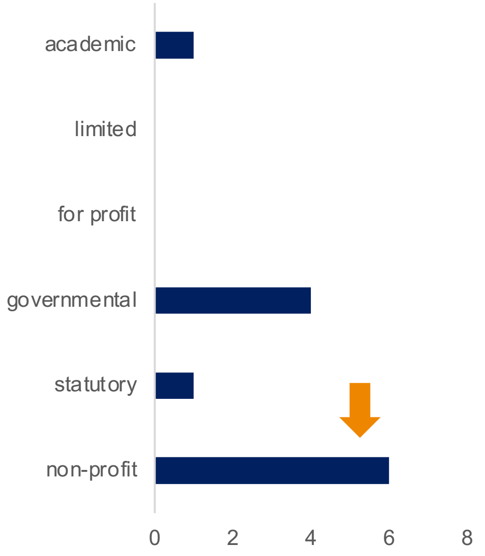
- g00gle.com
- replacing the Latin "a" with the Cyrillic "а" (U+0430) creates a visually identical but distinct character

ccTLDs affected by Homograph Attacks

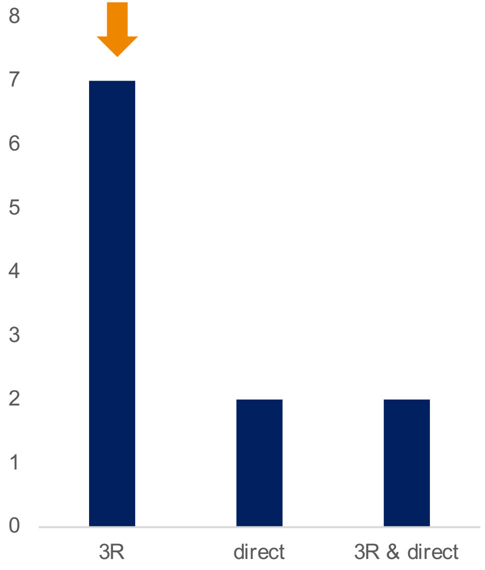
Region



Governance model

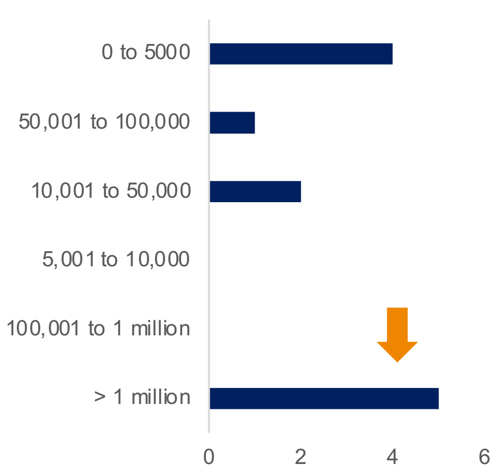


Registry model

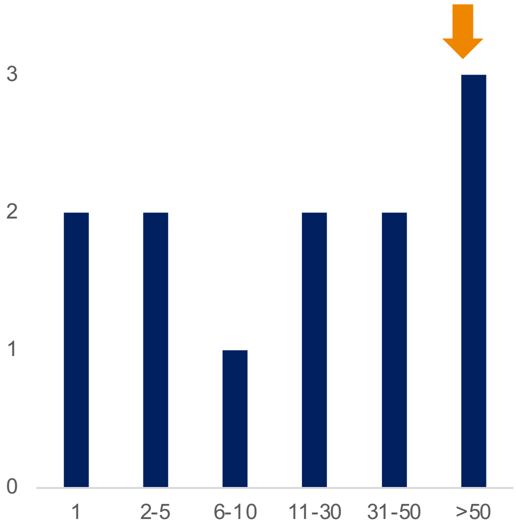


ccTLDs affected by Homograph Attacks

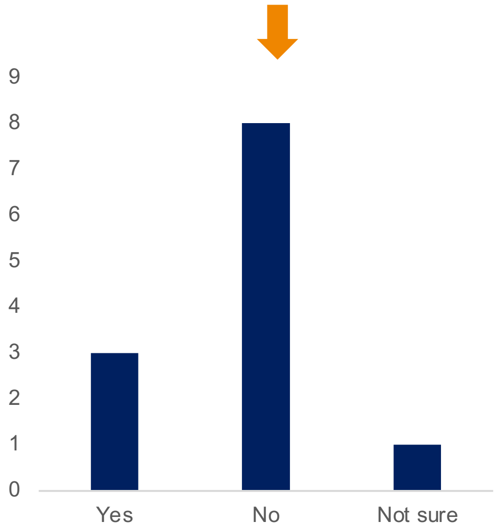
Domain portfolio



Employees

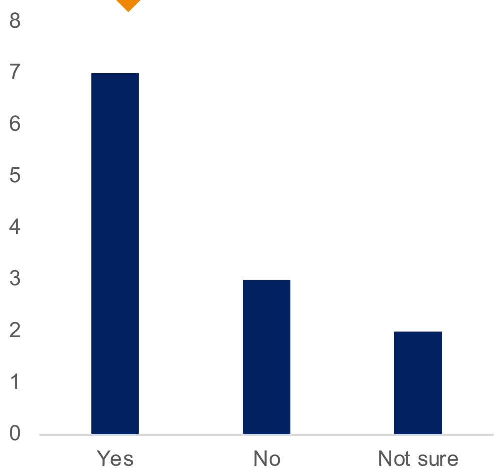


Abuse officer

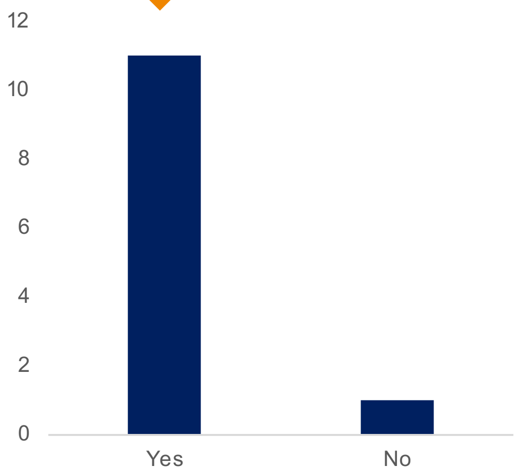


ccTLDs affected by Homograph Attacks

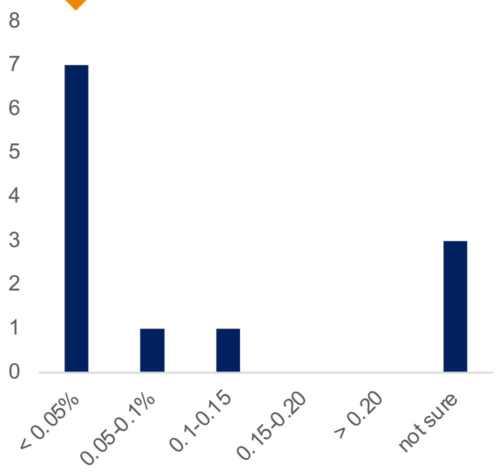
Subject to Data Protection Legislation



Cooperation (e.g. Computer Security Incident Response Team)



Domains affected by abuse

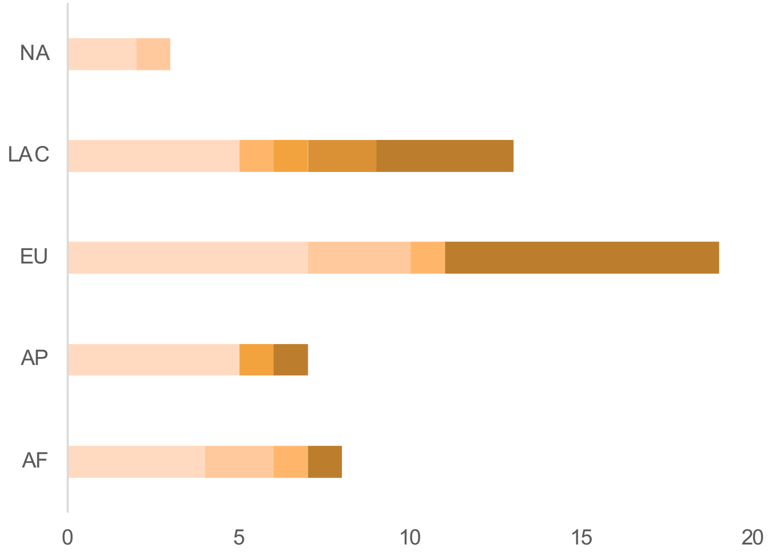


Comparing the percentage of ccTLD registrations exposed to abuse

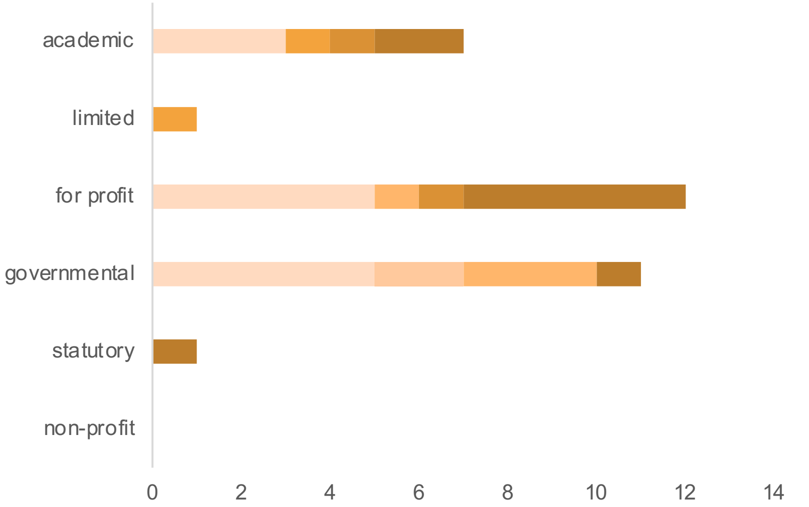
% of domains exposed to DNS abuse

< 0.05%
0.05-0.1%
0.1-0.15
0.15-0.20
> 0.20
not sure

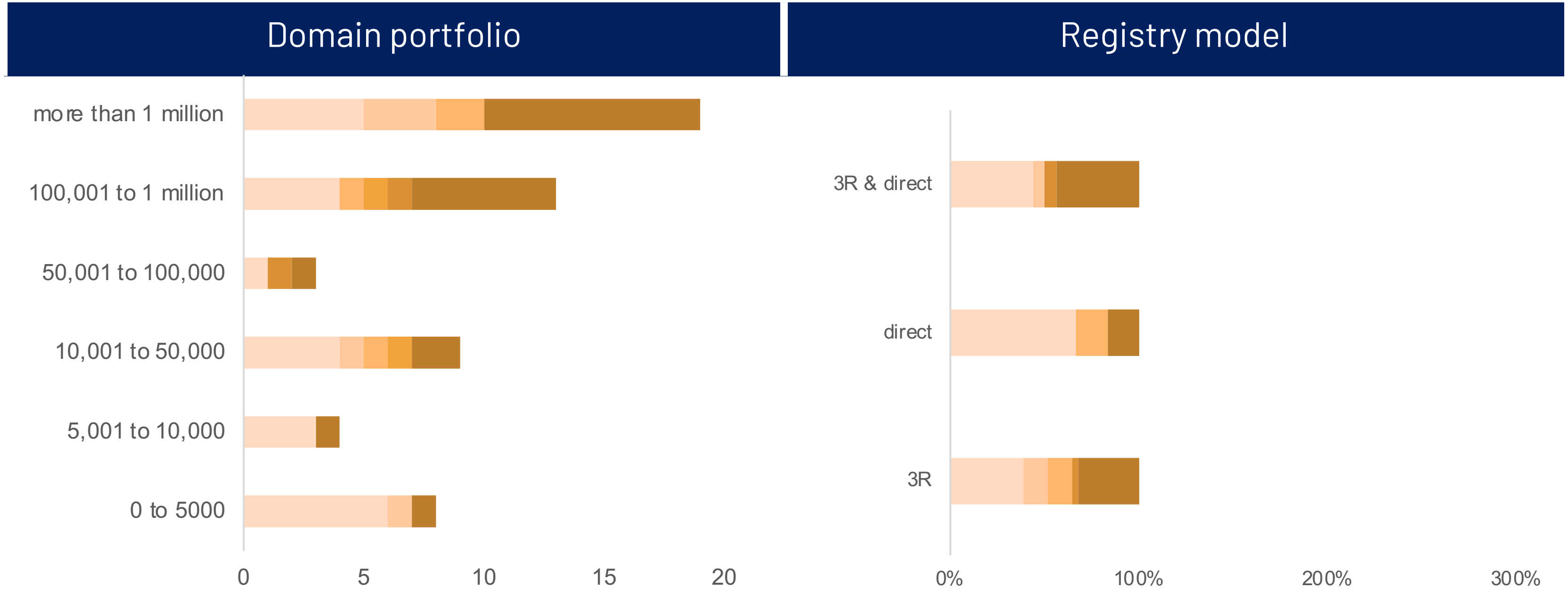
Region



Governance model

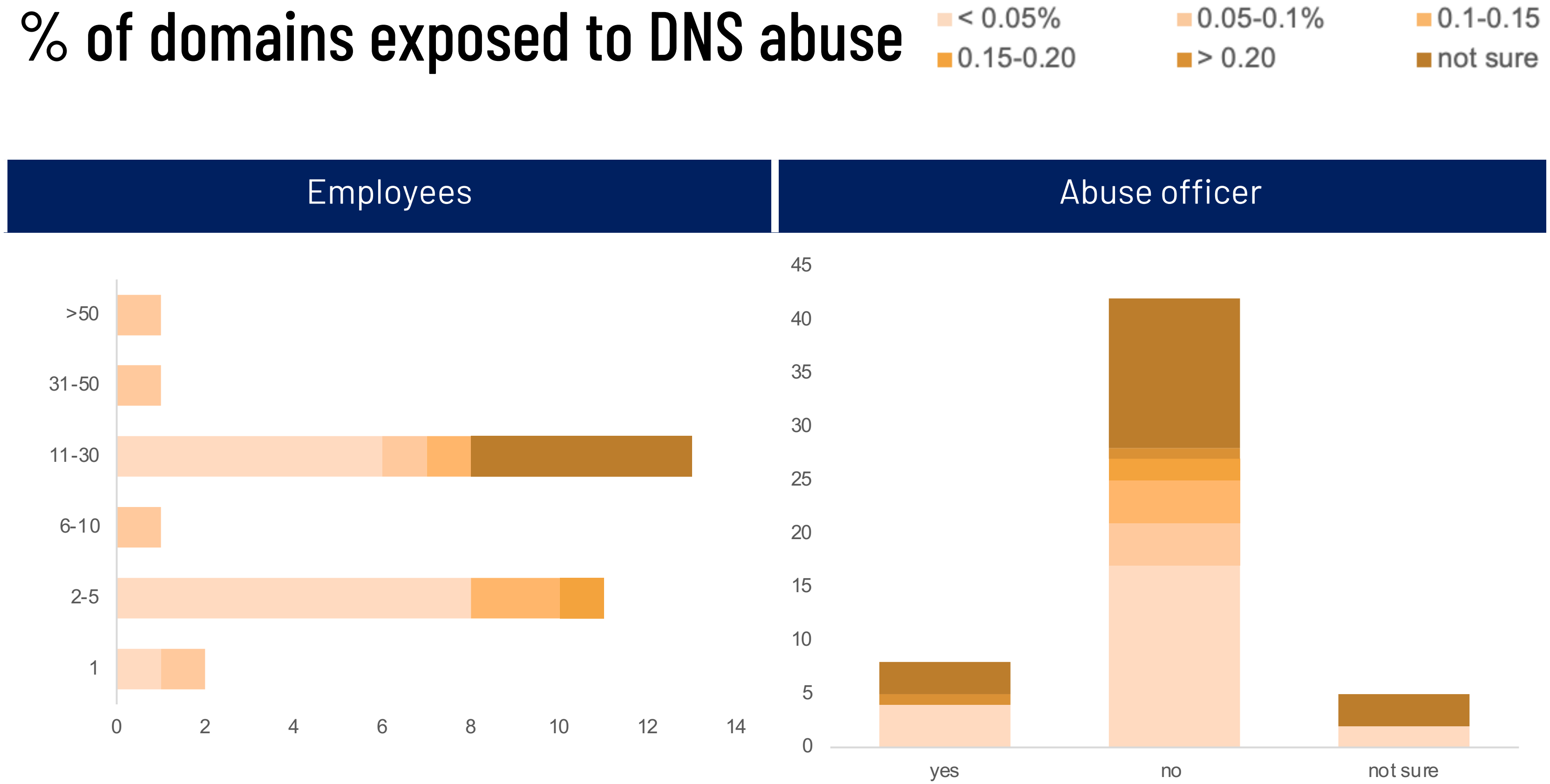


% of domains exposed to DNS abuse



ICANN | ccNSO

% of domains exposed to DNS abuse



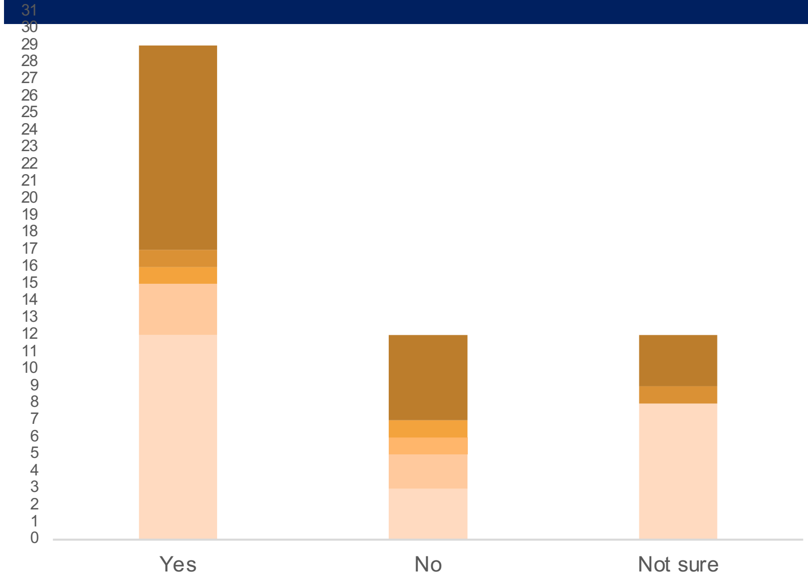
Employees

Abuse officer

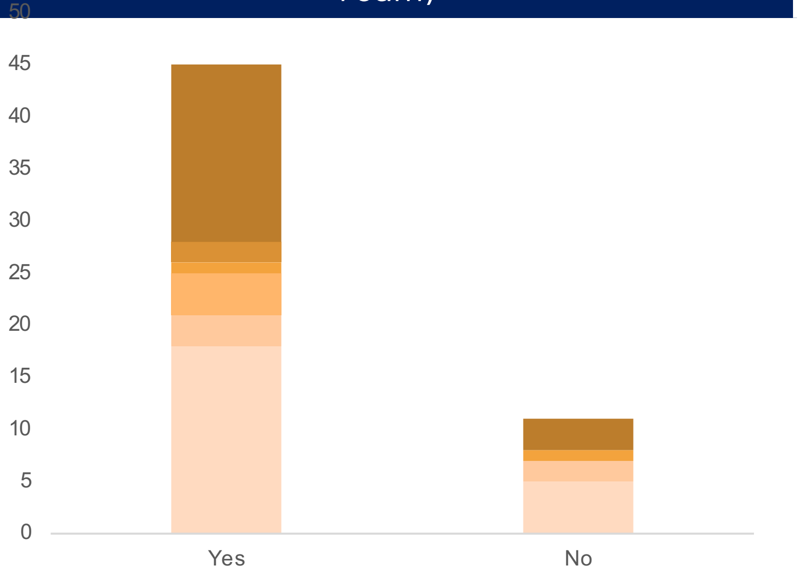
% of domains exposed to DNS abuse

■ < 0.05% ■ 0.05-0.1% ■ 0.1-0.15
■ 0.15-0.20 ■ > 0.20 ■ not sure

Subject to Data Protection Legislation (DPL)



Cooperation (e.g. Computer Incident Response Team)

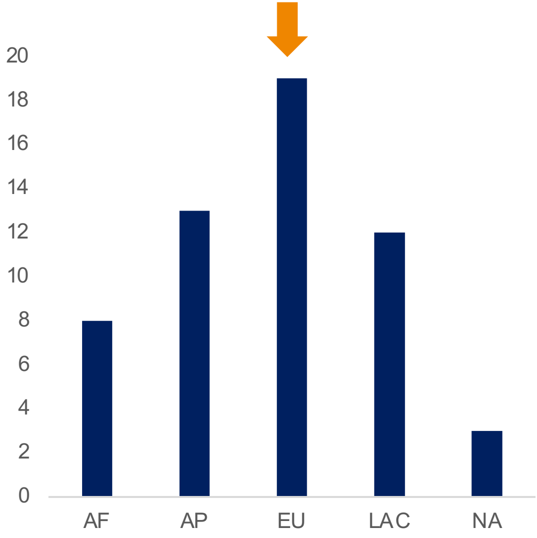


ICANN | ccNSO

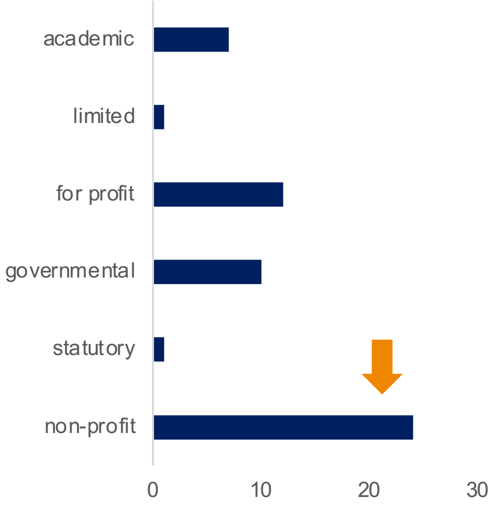
My ccTLD performs pre-registration verifications

My ccTLD performs pre-registration verifications

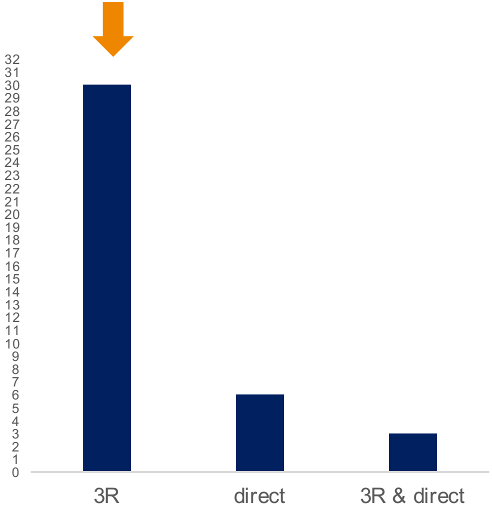
Region



Governance model

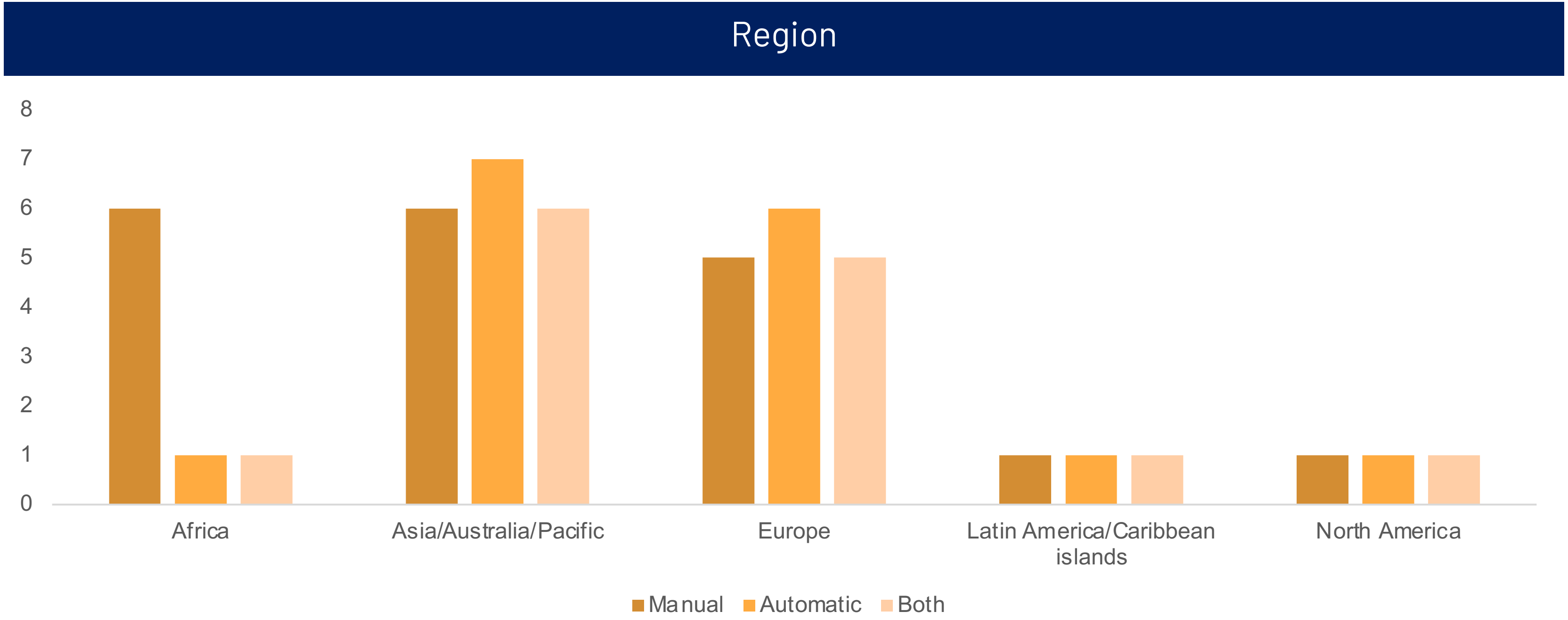


Registry model



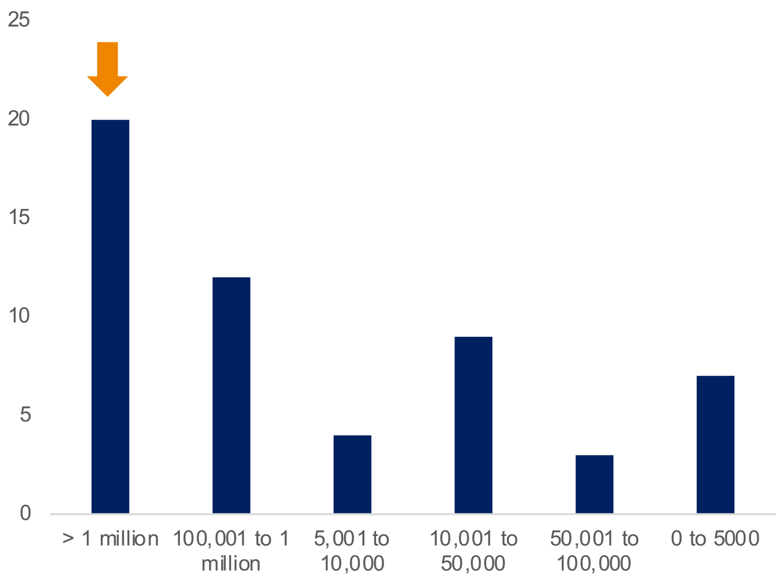
ICANN | ccNSO

Pre-registration verifications : how?

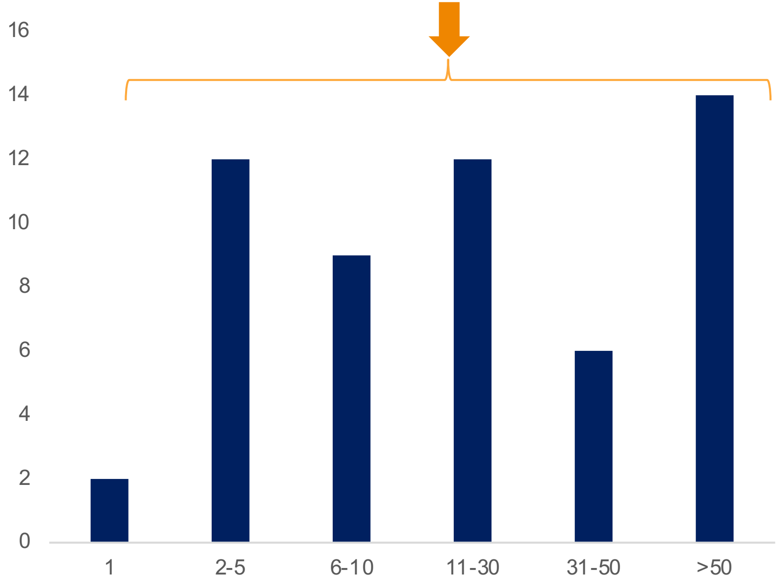


My ccTLD performs pre-registration verifications

Domain portfolio



Employees

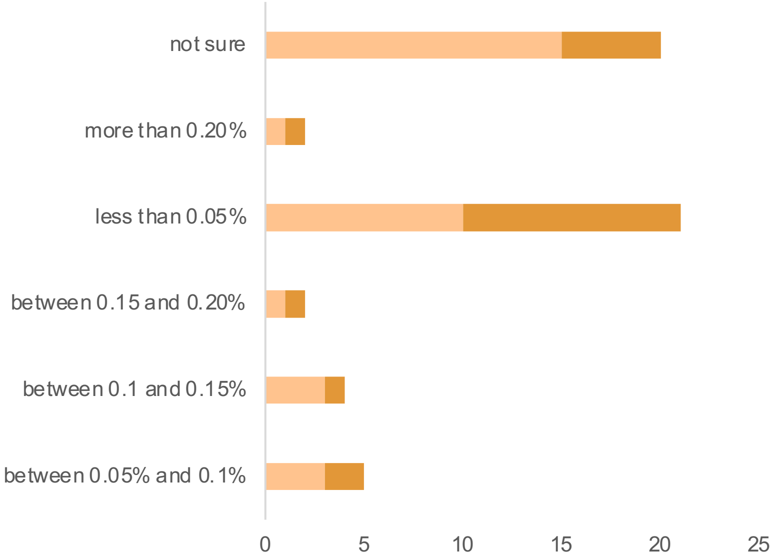


ICANN | ccNSO

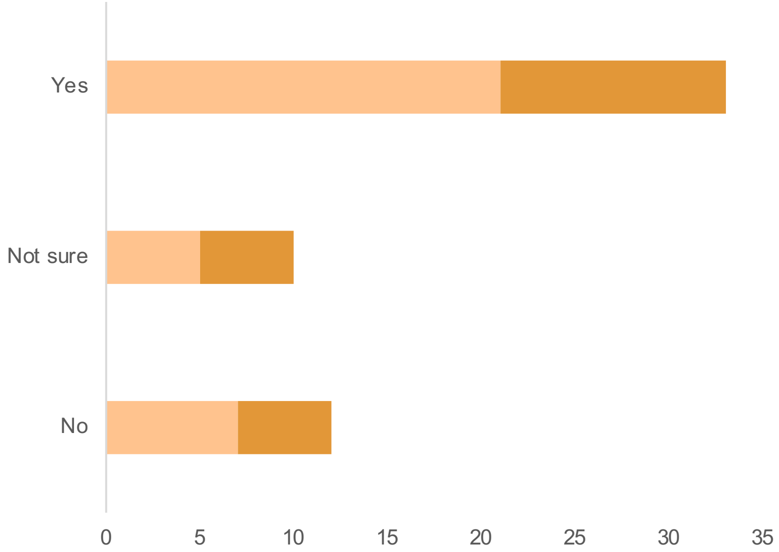
My ccTLD performs pre-registration verifications

■ No ■ Yes

Domains affected by abuse



Subject to Data Protection Legislation

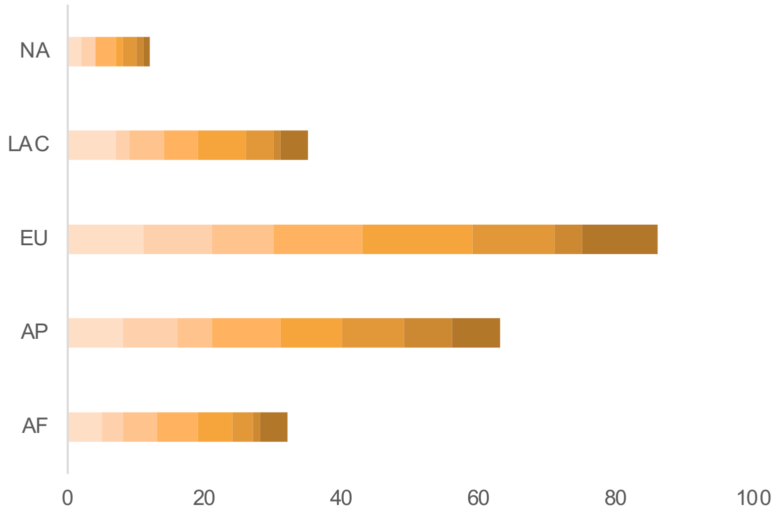


My ccTLD has abuse mitigation techniques in place

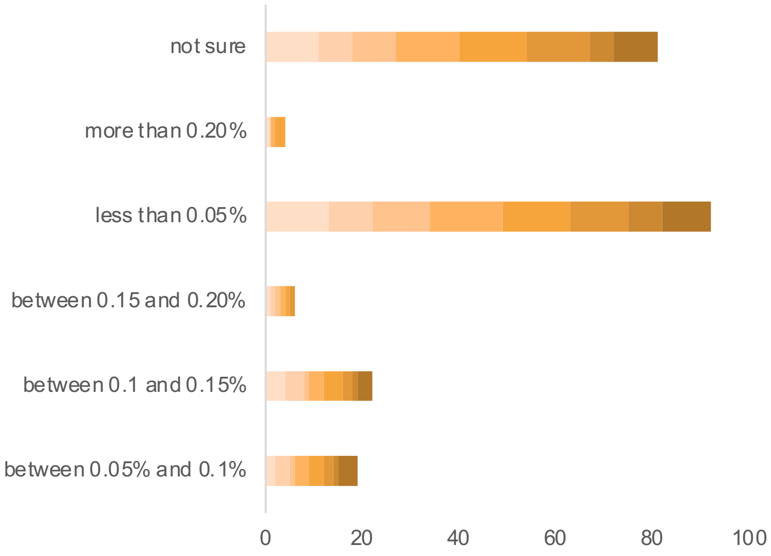
ccTLDs with mitigation techniques

- reg. policies
- tools
- consumer awareness
- complaints procedures
- collab with CSIRTS
- collab with LEA
- Collab with trusted notifiers
- Procedures

Region

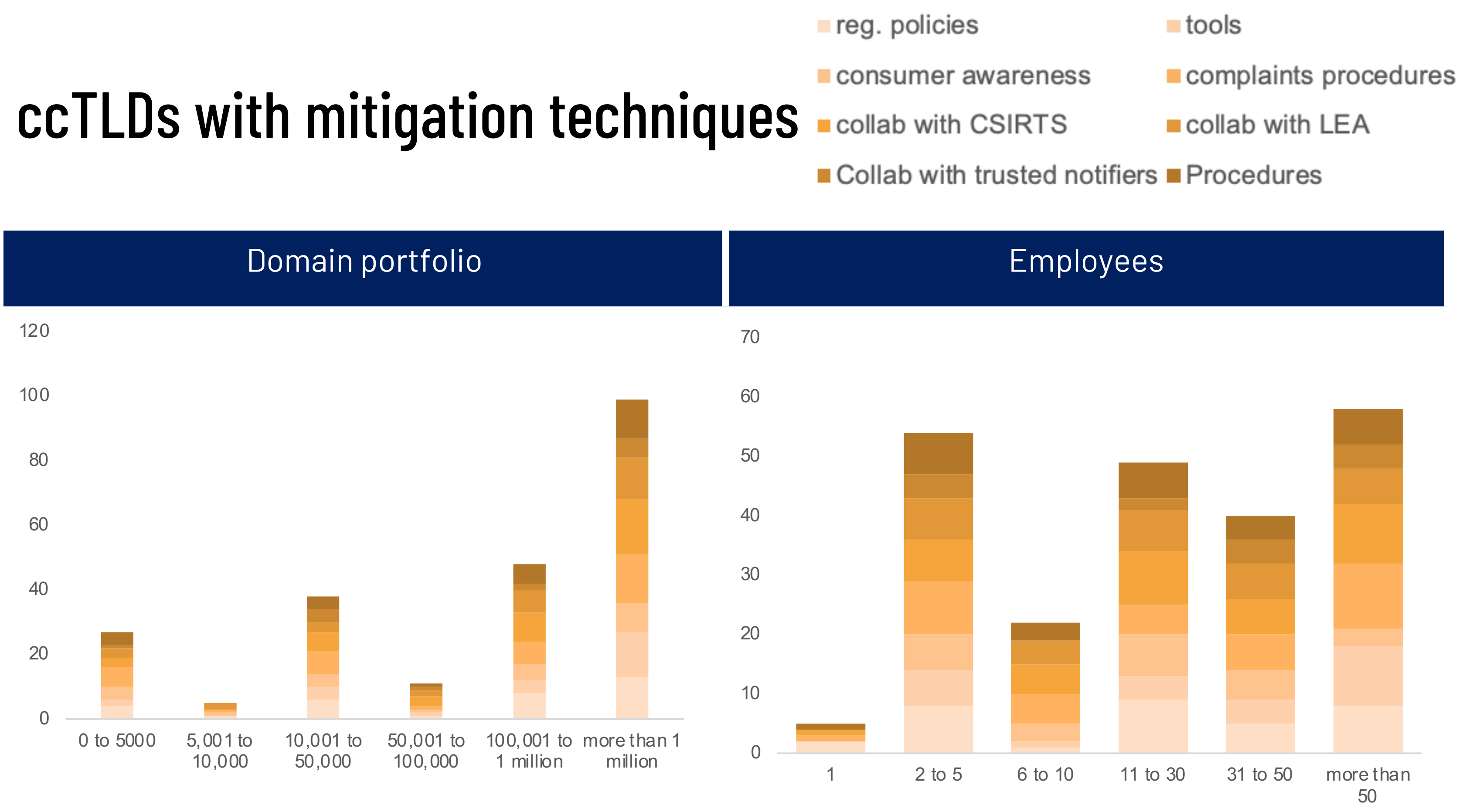


Domains affected by abuse



ICANN | ccNSO

ccTLDs with mitigation techniques



Main Findings

- Overall, relatively low levels of abuse for ccTLDs
  - Many ccTLDs do take action, despite respondents saying they have limited resources, and do not have access to tools
  - Different types of ccTLDs do perform checks, regardless of their region, governance model, registration model, domain portfolio size, number of staff.
- Checks could happen prior to registration, but are more often done shortly after registration, or when abuse is being detected

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)

Info about DASC and its two subgroups:

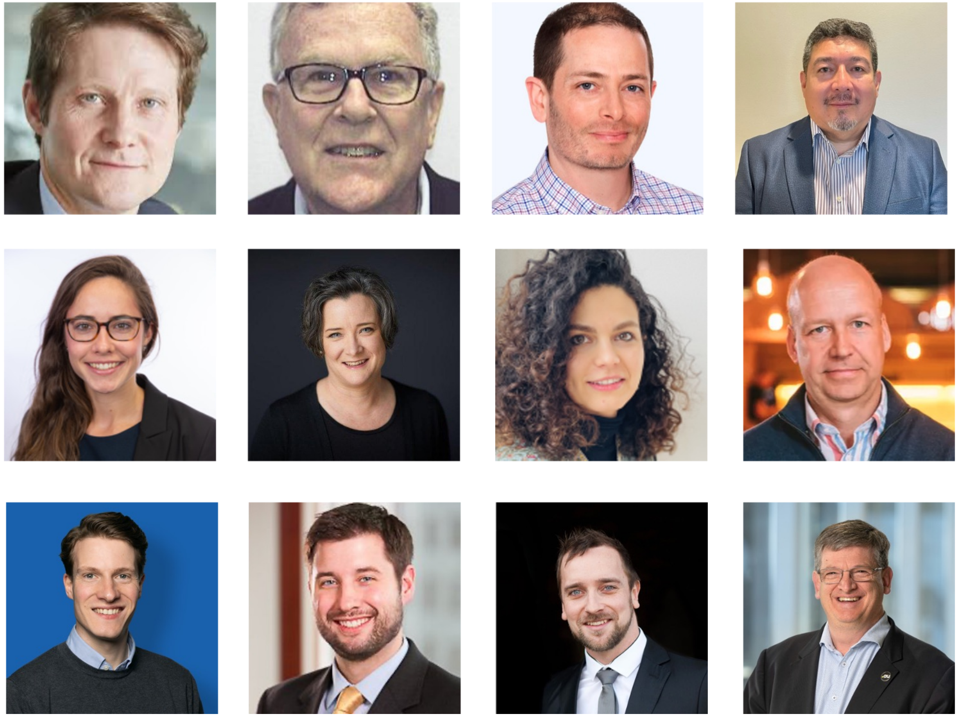
https://ccnso.icann.org/en/workinggroups/dasc.htm

ICANN78: Tools & Measurements | Wed., 25 October (11:15-15:15 UTC)

Learn more about different perspectives on tools and measurements of DNS Abuse. DASC reminds the ccTLD community about its repository and invites ccTLDs globally to contribute. Finally, DASC is proud to launch a dedicated email list at ICANN78, as a useful resource for ccTLDs.

Session chair: Nick Wenban-Smith (.uk)

1. Welcome & introductions
2. DASC resources for ccTLDs: repository and e-mail list
3. Tools & Measurements: different perspectives
4. Dialogue between GNSO and ccNSO DNS Abuse Working Groups on similarities and differences
5. Wrap-up & Closure



ICANN | ccNSO

Thank you!

ccnsosecretariat@icann.org

ICANN | ccNSO