Christmas Island Domain Administration Limited (cxDA)
HIGH RISK REGISTRATIONS IDENTIFICATION
PROACTIVE ABUSE MITIGATION

Tools provided by:
CoCCA
SECURE DOMAIN FOUNDATION
ICANN56 | HELSINKI
Initial Try 2012

Mandatory manual domain activation with the central registry

Enforcement
- Registrants received an email from the registry with a one-use link
- The link lead the registrant (or admin) back to the registry where they had to confirm their contact information and agree to the TLD policy
- Until they did so the domain remained un-delegated

Goals
Ensure the registrant email was valid/active
Ensure the registrant agreed with the AUP and other TLD policy

Problems
- The Registrant, having registered the domain via a registrar or reseller often did not recognize the sender (the registry) and was confused or suspicious
- The email was lost in spam folder and never received, forcing the registrar to activate a domain on behalf of the Registrant
- Reputation or risk factors were ignored
Refinement 2014

Escrow deposits inspection against abuse databases (paid service)

Implementation

Daily escrow deposits (already being made in ICANN gTLD format) were inspected and compared against various abuse databases by the escrow agent (NCC).

The email notification was sent to the registrant in case of any possible abuse.

Drawbacks

• No integration into the registry system (requires abuse staff to read and interpret the daily emails), abuse data is not stored in the registry.

• Significant delays between the registration, deposit and the abuse notification.

• It did not prevent abuse, it simply prevents abuse from occurring for an extended period.
Automatic activation for low-risk registrations.

Implementation
Domain registration flow is unchanged from the perspective of the registrar, but domains are not delegated until checked against the Secure Domain Foundation database.

Using the SDF API, the registry operator can identify high-risk from low-risk registrations shortly after registration (within a minute). Low-risk domains are automatically delegated, *high-risk domain are flagged for manual activation.*

Benefits
No delay in delegation for domains that are considered low-risk.

Significant reduction in the registry – registrant communications - which can cause confusion on the part of the registrant and increases the manual workload for registrars.

An additional step allows registry review the high risk transactions manually if desired.
What CoCCA looks for at registration and renewal

E-mail

Has the full email address (name@domain.tld) been associated with abuse?

CoCCA will then dig a little further …

• Has the domain or user name associated with any of the contacts the email been associated with abuse?

• Has the mx server associated with domain been associated with abuse?

Name Servers

Has the name server, or the name server IP address been associated with abuse?
What CoCCA looks for in manual activations

- CoCCA tracks/logs the IP address of the entity activating the domain.
- IP is checked against the SDF database
- When IP is associated with abuse an administrator at the registry level (or the registrar depending on the policy matrix) will be required to activate the domain.

Continuous Scans

In addition to the checks shortly after registration or renewal, CoCCA performs a continuous scan of the SDF database and comparison with the SDF database so that if there is evidence of abuse after registration it will be picked up.

In case any matches, CoCCA sends an email to administrators and abuse agents to review.
Policy Considerations

TLD / registry manager will likely have to assume a more active “trust but verify” role mitigating abuse at the registry level.

This “trust but verify” approach may require some modifications to the registrant agreement (if the TLD manager has one) and/or the registrar agreement.

With the increasing use gateways the registrants often do not know who the registrar is, they are only familiar with the reseller they registered through.

When the registry is communicating with the registrant, if the registrant has registered via a reseller the communication should mention the reseller.

The above is only possible if the registry system allows the registry to create and associate registrations with a reseller as well as the registrar.
How to Configure

The SDF API can be connected to by any registry operator.

If you are using the CoCCA software the SDF integration and activation tools are built-in to the current version available from https://wiki.cocca.org.nz

Configuration in CoCCA:

Step 1 - Configure the SDF connection
Step 2 - Enable “Require Activation” for the zone
Step 3 - Select “High Risk Only” on the Activation configuration page.
Step 1
Configuration > External Verification Systems

Step 2
Zone > Details
Step 3
Zone > Activation Settings

- **Base URL**: The base URL for the activation site. This will be put in the email to registrants.
  - https://coccaregistry.org

- **Completion URL**: The URL to send visitors to when they have finished activating their domain. It's a thank you page.
  - https://cxda.org.cx

- **Pending Activation Zone Generation**
  - What should zone generation do with domains pending activation?
    - Exclude from the Zone

- **Activate All Domains**
  - Require Activation for all domains, or just those deemed high risk by the ext
    - All Domains
    - High Risk Domains

- **Resend Schedule**
  - The activation emails will automatically be resent every so often, until the domain is deemed active.

If a registration is flagged, admins will get an email and it will appear in the top right menu when you login.
CoCCA
Manual Activation
Step 1
CoCCA Manual Activation Step 2