Board Question #6

potential residual risks of delegating Collision Strings even after taking actions to mitigate harm

---

Draft Answer (workspace below)

Workspace: for data and documentation

Applicable notes from Study 1

* Careful consideration of the "long tail" problem of the existence of risks even with the mitigation of known risks
* Consider actual harms and reputational harms that may manifest

Proposed Gap:

Questions from Study 2 Proposal, Appendix 3

- Risk analysis of mitigations taken as a result of known collisions is likely to influence our response.
- What is the effect of time on mitigation, i.e., does risk go up or down over time after mitigation has been applied?
- With most of the mitigation efforts, despite taking the mitigation actions, there is a risk that the collisions will still occur (lack of attention? Lack of realization that mitigated steps have been taken? Or Lack of caring)

We have 8 years of data re: strings that have been delegated regardless of what we knew about collisions and/or mitigations. This isn't so much a thought exercise as is an evaluation of real-world activity; it's what we know.

- We still need to consider what are the long-tail issues.
- How long is mitigation required?

- Thinking about the kinds of harms that can occur, there's a long tail here. What is our responsibility for protecting those users?

This question may be predicated on previous questions and us having solid answers to those. Specifically, Question 2 and questions around mitigation frameworks. If we can't understand how negative signals impact the question, and if we don't recognize the mitigation framework potentially offering its own signal, then we may not be able to use the last 8 years of data. Unless the mitigation has prevented issues, there are still MitM issues where end users may not get the information they need, and we may not be able to detect the collision issues.

- Key may be that you can't give one answer to everything. how well did the mitigation work for a given collision, how broad is the scope of the collision, what are the harms being done through this collision? There may be collisions in the long tail we don't care about because the harm is of an acceptable type or level.
- If we treat this as a purely academic exercise with no hard evidence (e.g., MitM attacks, bad registry operators) then we are alarmist. Our answers should be clear as to where our theories are not provable unless the action is actually taken
- If we decide there is a collision we need to mitigate, then this question says "are we ok, or we need to do something else" - we need to look at each case, and not give broad answers. Analysis has to happen case-by-case.
- If the string is delegated after the mitigation, how do we collect additional data to learn about the effects? If there is a mitigation strategy, is there an obligation on the part of the registry operator to report back to ICANN? What monitoring would ICANN do with those reports? What action would ICANN take over time?
- What about wildcarding during controlled interruption, to force the response to get people to look things up? We're not allowed to have wildcards at the gTLD; it will likely have to be a very compelling argument to allow it given the reasons its not allowed now.

Would it be possible to determine whether there are DNS abuse reports filed with registrars that might have resulted from a name collision situation? Do we assume that all fraud complaints don't involve any name collisions?

- Would it be possible to determine whether there are DNS abuse reports filed with registrars that might have resulted from a name collision situation? Do we assume that all fraud complaints don't involve any name collisions? (second-level is out of scope)