Board Question #4

possible courses of action that might mitigate harm

- Not list ICANN org? Leave it open?
- Maybe a more complete list of possible parties who might action?
- Note the "reserved list" in the applicant guidebook is a mitigation strategy

---

Draft Answer (workspace below)

Workspace: for data and documentation

Note that question 5 has a strong dependency ("This task will likely be highly dependent on the risk analysis of the items identified in Board question four.") on what we do with question 4.

Applicable notes from Study 1

* ICANN incident reports will have some data
* Review of controlled interruption - efficacy
* SSAC report has some other suggestions for mitigation
* Does literature have anything else?
* Verisign research on this topic? Matt is going to repost this
* Appendix A of SAC066 has 3 alternatives
* SAC062 has two broad categories of mitigation methods
* Evaluate alternatives to controlled interruption
* hacker overflow, stacker overflow - can we get these references so that Karen can catalogue them?
* DNS Oarc presentations about mitigation?
* also consider the work in SubPro

https://superuser.com/questions/958758/why-pinging-drive-gets-replies-from-127-0-53-53

https://serverfault.com/questions/626612/dns-just-started-resolving-my-server-prod-addresses-to-127-0-53-53

https://news.ycombinator.com/item?id=15270289

https://github.com/laravel/valet/issues/115

https://community.helpsystems.com/forums/intermapper/general-network-questions/3c736b35-b09b-e611-80d8-0050568473e2

Proposed Gap:
* thought exercise on our part extrapolating from name collisions that have occurred
* might be dependent on classes of collision types and mitigation types, i.e., perhaps there's a mitigation framework that would be helpful

Questions from Study 2 Proposal, Appendix 3

- Thought exercise on our part extrapolating from name collisions that have occurred.
- Dependent on classes of collision types and mitigation types, i.e. perhaps there's a mitigation framework that would be helpful.
- Why is mitigating name collisions difficult?
    - Are organizations even able to "see the problem" (e.g. transient corporate devices used on corporate networks) or even be able to reliably "trace the causes"
- Some reasonable mitigation plans:
    - Organizations using a private TLD, change it to use ones rooted in the global DNS.
    - If using a shortened name, ensure use of fully-qualified domain names in various systems.
- Targeted Outreach
    - If the applied string has certain traffic properties direct outreach to the underlying manufacturer or ISP may be sufficient to remediate the issue (e.g. TELUS, CONSUL, CBA, etc.)
- SLD Blocklist (e.g. used from snapshots of DNS data)
    - Various research reports show that statistical sampling is flawed using this approach due to time, root server affinities, etc.
    - Provides blueprint to miscreants for domains with elevated traffic (and potentially higher risk profiles)
- Mitigation Strategies
    - Underlying causes of colliding strings likely requires various strategies to effectively mitigate (or inform) end systems/users.
    - Fail hard scenarios: Database connectivity, etc. Events in which an application explicitly requires a connection to one or more services and places corresponding exception handling processes to properly raise errors.
    - Systems designed to keep users unaware of actions: DNS-SD and Zero Configuration protocols. Service configuration is done via DNS and facilitates various MitM attacks if performed surreptitiously.
- Guidance to consider:

- It's important to keep in mind that we probably won't be able to list all possible mitigation strategies, especially going forward. The advice that would be most helpful to the Board is how to evaluate mitigation strategies and considerations regarding who is responsible for the mitigation.
- What are the parameters of a good mitigation strategy?
- What are the parameters for measuring the success of a mitigation strategy?

To the extent we create categories of harm in Question 3, we consider the mitigations to those categories here.