**SSR2 Subtopic**

**Future Challenges - Meeting #1**

**24 July 2017**

**1400 UTC**

**Attendees:** Noorul Ameen, Kerry-Ann Barrett, Eric Osterweil, Mohamad Amin Hasbini, Denise Michel

**Staff:** Yvette Guigneaux, Jennifer Bryce, Steve Conte

|  |  |  |
| --- | --- | --- |
| **Action** | **Owner** | **Expected Delivery Date** |
| Input draft text to [Google doc](https://docs.google.com/document/d/1DWoT4VoMlT5Dvcy78EXI-O5tQFqa9CblwsDEV6go51s/edit?usp=sharing) on vendor security and performance security sub-sections. | Mohamad Amin Hasbini | 28 July  |
| Circulate Doodle poll to determine subgroup regular call time slot  | ICANN Org | 25 July  |

**Review of** [**Google doc**](https://docs.google.com/document/d/1DWoT4VoMlT5Dvcy78EXI-O5tQFqa9CblwsDEV6go51s/edit?usp=sharing)**:**

* EO: Currently high-level categories with some more detail. Could use input from team.
* EO: Questions for the group. Do we think this is at the right level or right scope for the future challenges sub-team? Too far on the horizon? Too near-term?
* Doc is a comprehensive list of what EO and DM worked on in Johannesburg.
* Goal is to get a longer view of what is important. Review what is relevant today and what will be relevant in the future. The approach would be to determine how we review the information and future forecasting and what will be the technology will offer in the future and how this will impact future operations of the DNS. In looking at the ICANN security operations we would need to consider as new technologies emerge would need to examine what the threats might be.
* KB: There is a need to look at the future challenges broadly as well and not only tied to emerging technologies as this may change rapidly and the review cannot just be focused on the technology but general threats.
* EO: List of Top Identifier System attacks. Please provide feedback if it can be closed off. The specific attacks may be addressed by another subteam. Do the attacks we know now pose future challenges?
* DM: We’re trying to project down the road to see if ICANN aware of the future challenges and do they have planning and other resources in place to address these challenges and does the team have recommendations for what the team are seeing as the expected challenges that ICANN will face. Internet governance issues are quite broad.
* MAH: Suggest we look at performance specific IT challenges e.g. IOT and provision of hardware and software from the provider side. It is different from attacks but relates to the security of services. Vendor selection and management of solution and vendors. We can highlight how SLA are managed and implemented.
* EO: Need to ensure it is within the purview of ICANN itself. If it has nothing to do with ICANN directly we need to justify it and tie it back to ICANN specific role for the protection of the DNS.
* MAH: We can develop and highlight it as a challenge and then create a small roadmap for ICANN to implement.
* EO: Other aspects of the DNS management structure - the list can grow.
* MAH: There is value in examining the vendor management aspect and more the security aspect.
* EO: Any comments on the structure of the future attacks list?
* SC: I understood the future challenges sub group was to look at the future challenges threats to the SSR of the DNS and unique identifier system that ICANN manages such as block chain, etc. and not necessarily the organisation?
* KB: The idea is to look at not just the technology but to ensure the management process if the mitigation measures not implemented it would be a future threat.
* MAH: Not about analyzing SLAs, more of recommendations towards technology selection.
* EO: Review of Top identifier system attacks list.
* MAH: Clarification - if we can project these it would be that these are currently happening and can be found through DNS pocket inspection and traffic monitoring.
* EO: Many of the concerns are inspired because of existing challenges, so our job here is based on the known attacks and challenges will this pose a threat in the future based on how the DNS will be use dint he future. If some of the proposed new uses do take off then how can we predict future challenges based on known attacks.
* DM: For everything on our list we should go through it and see if there is applicability if there is a relationship between ICANN SSR and DNS SSR, and then flag the things that don’t apply to our group and discuss where the overlaps are. We should examine if these should be capture in the ICANN or DNS subtopics as well.
* SC: DDoS is old as the sky, but 10 years ago (or so) we saw the first reflector attack which abused the DNS to amplify (and mask) DDoS attacks, there will be new ways in which to abuse the unique identifier environment.
* EO: Old things will evolve and the threats that may evolve as a result.
* EO: New dependencies. In the future we may want to worry about new cryptosystems. New uses for DNS. Today something works one way but it might work differently in the future and therefore affect ICANN in this way.
* KB: Should be loss of confidence AND adherence in standards bodies.
* SC: Potentially cause and effect.
* ICANN org to circulate a Doodle poll for regular call slot availability.