Update on ICANN SSR Efforts 10Mar2010

Craig: There are quite a few people in the remote participation so we have more people remotely than we do in person. All right, I think I'm going to go ahead and leave the door open because of the airflow it's getting warm in here.

So, I think we're going ahead and get started. There's an hour scheduled for this session. My name is Craig Rattray. I'm ICANN's Chief Security Internet Advisor. In this session one we've done a couple of times previously. It's becoming kind of a regular part of at least how the ICANN security staff keeps the dialogue going with the community about the nature of our activities, really again, as a dialogue.

It's not a public consultation. It's a mechanism for us to inform and to receive feedback on the types of programs and activities we have underway.

So, with that, I hope to do these slides. I have about 10 slides and I tend to – sorry, in about 20, maybe 25 minutes. I'm going to pose a question first though and if you can communicate via the remote participation with the people in the room.

The first few slides have to do with the strategic initiatives that ICANN plans to launch on security. We've had a lot of discussion about that this week. Could I take a poll of people in this room, and then if we'll take a poll of people on the remote chat, about how many people have actually gone over the strategic – have been in sessions where the strategic initiatives were viewed?

Raise your hand if you've seen a review of the strategic initiatives. It doesn't' look like anybody here has. So I think it's worthwhile to do that. If eight out of ten people had already heard the story, I'd probably modify the amount of time I spent on it.

Any feedback from the remote participation? All right. I'm going to assume that there's some congruence between the type of people who are in this session in person and the people on remote participation and we didn't have a lot in remote participation in the initiatives consultation.

So, with all that said, I am going to spend some time here at the start reviewing the two major strategic initiatives that we've put in play and are asking for public comment on.

So, we posted for public comment last month two – a paper that describes two strategic initiatives and a longer paper that describes the business case for a domain name system computer emergency response team or CERT.

The background for those initiatives, we can go into greater or lesser depth, but the growing list of domain names security and resiliency, things like the emergence of the Confikr worm where ICANN and many TLD operators were involved. ICANN most information sharing mode, the DNS registries involved in a much more operational fashion making responses to a portion of the malicious code that was part of the Confikr malware that had spread and that activity continues.

But it's a good example of how domain name system can become at least part of a mechanism for the spread of large amounts of malware. The Confikr worm is estimated of upwards of 5 million infected computers as we speak.

Also, we’ve seen clearly increased evidence of domain hijacking both with social engineering as well as technical exploits. One of the things that has occurred in this hijacking is it comes in spades. Hacker groups realized that certain types of vulnerabilities exist in registries or registrars. They go in the structured sort of campaign to hack those vulnerabilities.

The word doesn’t necessarily spread as easily as it could related to those activities to allow people to effectively protect themselves in advance by what has been seen in other – previously in other similar sorts of situations.

What e have had, particularly in the DNS annual symposium that we started last February in Georgia, at Georgia Tech, was growing community calls for some sort of systemic domain name system security planning and response. This was also highlighted in a number of the Confikr-after-action discussions that have been had and even the formal reviews of that contingency.

The idea is that many of these threats now require a more – a capacity for the community to inform all of its constituent players as to what is the nature of these threats, and then also the length of a particular operators to potentially secure the organizations that have the resources to help deal with these threats.

ICANN has undertaken – signing something called the Affirmation of Commitment back in the beginning of October of last year. One of the major areas of those commitments is security, stability and resiliency. One of the particular commitments that ICANN makes is to coordinate contingency planning for the domain names system security and resiliency. One of the initiatives is to specifically pointed at that.

Then operational good practice tends to indicate if you have a contingency plan you need to have the ability to pull together a response. I think a DNS CERT is part of the picture about how you actually provide for response in contingencies.

These initiatives were called for in the ICANN Strategic Plan. One of the things that’s important to note is that the organizational models and resource approaches, particularly the DNS CERT are not determined. Both initiatives come with a price tag that is identified in the paper. But exactly who pays the bills and particularly with the CERT how it’s organized is not defined. It’s open for community input.

We knew very much that there were varying views about the proper way to do that and how to organize both governance and resourcing. So that is an open question that we hope to get feedback on.

The first initiative deals with the need for systemic risk analysis contingency planning and exercises. We very much see this as a community-based effort, not run out of ICANN – supported by ICANN as in many cases providing the right staff both analytically and logistically in order for a community-based effort to undertake both the creation of a risk framework as well as its – we believe that it’s necessary to undertake regular risk assessments at the systemic level as to the security and resiliency risks to the DNS.

One of the things that came out of the root scaling study that was issued last summer and is still under consideration by the ICANN’s SSAC and RSAC – they probably should say root operator information sharing system – but that it would be very useful as one understands risks to the root system in particular to have an information sharing of those operators more fully with the community. We in part want to address that through this initiative as well as contingency planning based on key scenarios.

Again, this was specifically called for in the Affirmation of Commitment that ICANN is a party to. In general, the notion that we've identified the key risks and then conduct planning as a community on how we would address those risks. Again, this is an initial concept, the specifics of what constitutes a DNS contingency plan but certainly would need to be worked out.

Then finally, when you have contingency plans you need to conduct exercises. One, you need to understand whether the commitments made in plans, the practical operational people can follow-through on simply talking to each other, let alone conducting activities outlined in the contingency plan. Having my operational experience indicates that this is an essential part of actually insuring that you can do the things that you need to do in difficult situations.

One thing I do note on the slide is this would build on existing efforts. There is a growing amount of exercise activity that either involves the domain name system or the domain name system operators are conducting on their own. We think we need to map that and figure out if there's additional efforts that might be necessary.

We've also issued again an initiative that relates to the formation of a domain name system CERT. Given the vigorous feedback I've received over the course of this week, I do want to make clear that this is not again considered necessarily something that ICANN would staff or run them by ICANN. But the question on the table is does the community need the creation of some sort of organization that provide mechanisms to provide CERT life functions?

Rod Baxter, my ICANN CEO very much has directed me, at least in the formation of these initiatives that the label of CERT is the right label in terms of getting policy makers and governments who maybe need to understand the organizational model for what the domain name system community is doing in terms of organized structured response.

He thinks that label resonates better than a title that isn't as clearly well-branded. Like "collaborative response center" was another label we considered. But Rod's take was that would be less clear to outside stakeholders exactly what that meant, that people know what CERTS are. They know what the domain name system is. Therefore, it's pretty – they can think through on their own what a domain name system CERT might be.

The question is however what form should that take? What missions and capabilities would that provide that aren't already provided? It is clear to us the business case makes clear that we understand that there are a number of organizations conducting these sorts of activities already are – many of those are volunteer. A few of those are standing. Not all of those – many of those don't deal with incident response but they provide very important capabilities in terms of a structured incident response capability.

Few, if any, have a global focus and reach to the less-resourced operators. One of the voices we've heard strongly is that in areas such as this area, where we held a workshop last week in conjunction with CERT, that the operators of ccTLDs in this area a bridge to the types of security resources that some of that better resourced and security aware domain name operators have.

The operational focus we believe should be determined by the stakeholders, both the operators and domain name system and then the collaborators who would have it in the cyber security community. And how this CERT would fit into existing activities and provide value-added.

We planned, as I've been discussing this week, a workshop in early April with representatives of hopefully most if not all of the stakeholder groups that we think were important. Run them through some key contingencies that we believe would involve activities for a DNS CERT and understand where it fits into the existing ecosystem in terms of DNS security.

Again, we've issued a DNS CERT business case. Uri Ito who for those in the room, is to my left on the ICANN security staff has really been the point person on this effort and will remain so as we work through the public comment on it.

As I mentioned, on these two security initiatives we're seeking feedback. We discussed it in a focus session. I also discussed it at length with a governmental advisory committee. I will say that the feedback on Monday, there was a lot of concern that we needed to make sure this fit well with the existing set of efforts that the funding model and the relatively large bill which was tagged at $4.2 million for the initial year of operation.

Why is that bill at that level? Get more granularity on the specifics of staffing and operations and infrastructure that require that level of effort. Again, we planned to do that in a relatively rapid fashion and hope to have more detail on the table in preparation for the Brussels meeting.

With the GAC, there was generally more support of notion that with a real challenge from their perspective was how this fit with existing national level CERTS. We've planned a considerable amount of continued dialogue and how national levels CERTS fit with a domain name system CERT. And again, we certainly need to address the organizational and funding approaches.

So, for the security team in ICANN, conceptually a lot of our effort especially the last three months has really been around the initial consultations about how this might work. Articulating that and putting them out for public comment. I think in tandem we'll need to spend a lot of our effort in the near term with the community about whether these are the right things to do. And if so, what is the right way to do them?

All right. I do also want to turn to a broader set of things. Just again, inform the community about the types of things that we've got ongoing. For those who've been tracking kind of ICANN's activities in this realm, and particularly it's public articulation of those activities, we last year formulated the first version of what's called the ICANN plan for Enhancing Internet Security, Stability and Resiliency.

It went through a public comment period. It was approved by the board at the June session. This has now become explicitly the basis for the Affirmation of Commitments review. The review will involve seeing what was in the plan? Did we accomplish what we said we did in the plan? Is the plan, again, by an outside, independent review properly focused on the right activities for ICANN?

So, for myself and my staff and then across the ICANN staff and to the board making sure that we get this plan right in terms of our role, not over-scoping it, whether we can execute on the commitments made in this plan is its major focus. We'll be working on that in the upcoming trimester. This will also be out for public comment with the notion that it'll be part of what the board reviews or hopefully what the board approves at the Brussels meeting as well.

Turning a little away from planning and initiatives, we've started last year as I mentioned, an annual domain name System Security Stability and Resiliency Symposium. This year that was conducted in Kyoto about a month ago. This one focused on measuring the health of the domain name system where really about 50 expert participants – it's an invitation only working session, not a conference where there's information dissemination but you go in with kind of a predisposed agenda and workshop sort of notion.

We really focused on what are the key parameters for DNS health? And then base lining for those parameters, sets of metrics and measurements that are occurring in different organizations, what's well-covered and understood. What's almost not covered at all and ill-understood. That will be documented in conference proceedings that we are currently reviewing with the steering committee for that.

The participants at that session hopefully get that out within, Uri, the next month probably. It will be posted on the ICANN website for everybody's visibility and probably even kind of a continued sort of feedback on this particular aspect of the problem.

In the sense that we need to do risk analysis in contingency planning obviously being able to measure where we're at in terms of health and security as a fundamental precondition to doing that well.

We're also developing a set of key contingencies. Somebody has called for by our strategic plan in the Affirmation of Commitments. We plan very much to try to drive those into the efforts we're doing on response and exercise planning, both with the community at-large as well as when ICANN does its own internal like continuity exercises. We've got a continuity exercise recently where we projected an outage for the INS services.

Then finally there is a – many are not as aware except for the gTLD registry people themselves. We have a gTLD continuity plan, where the real focus of that is if different sorts of failures or disruptions occur, the services in a gTLD registry. How do we ensure that registrants are protected in terms of their data being transferred effectively to somebody else so that they stay in play in the domain name system?

It's probably a forward meaning effort in terms of a broader sort of notion of what is domain name system continuity and resiliency mean? So for those who are interested we can either discuss it further. I can point you to the right place in the ICANN website to take a look at where we're at with the gTLD continuity planning.

Looking at the formation of new gTLDs, there's getting to be about a year-long history. About a year ago, at the Mexico City meeting four over-arching issues related to the formation of new gTLDs were documented. One of those was the potential for increased malicious conduct as we bring on new gTLDs.

My team as well others on the ICANN staff, particularly in the registry services staff, have been involved in a dialogue with the community about what sort of measures could be put in place as we bring new gTLDs on board. That would help mitigate the potential for malicious conduct.

Some of those measures are already included in the current budget of the Draft Applicant Guidebook. So for the new gTLD *officianodos*. That's Version 3 we're currently working on input that would be included in Version 4 of the intent being that Version 4 will be out for comment prior to the Brussels meeting.

So, some of the things that are already considered requirements in what we call the "DAG", are the requirement for registries to implement new registries to implement DNSSec at the start of their operations. Prohibition on wild-carding which is a recommendation from this ICANN Security, Stability Advisory Committee as well as requirements for background checks on background registry applicants so that the notion that a registry – we have some idea of who is running a registry in addition to the actual operations of a registry.

There are two major working groups ongoing. We just finished a consultation in this room on the working group, not the work group related to zone file access. The notion there being in the generic top-level domain space registries are required to provide access to their zone files.

However, with 10 registries you can do that one-on-one with a set of people who want access to that zone file. People like law enforcement, and incident responders trying to deal with malicious conduct are concerned that if the number of registries increases to 200 or so…just pick a large number that having separate agreements with a large number of registries to get access to zone files is a less scalable proposition and then hopefully that with ICANN helping coordinate for some sort of common way to access zone files in gTLD registries can be created.

So this working group has made a lot of progress. They've put four models on the table for consultation and hopefully will be making recommendations about which approach and the cost of that approach. The governance approach, the zone file – centralized zone file access will occur.

We also have put out a concept paper back in the fall about establishing a voluntary high-security TLD verification program. The notion here and this was actually put out consciously as not just new gTLDs, but how does one set to determine what the right set of controls would be in a TLD?

So, the registry would obviously be the responsible party but it would also include obligations in that TLD for registrars and even potentially registrants related to both vetting the types of people that had those roles within a given TLD. As well as technical and operational controls about the formation of zone files and the publication of zone files with the idea – and this was really brought to us by the banking and finance community that in certain industries or sectors that there needs to be confidence and an increased level of trust surrounding the operation of a given TLD.

So, we have a technical expert advisory group working on that. The notion is to really have them focus on the potential list of controls which are more cost-effective, which are already existing within other sorts of efforts. And then bring that back for determination of whether such a program should be constituted, what ICANN's role in such a program would be.

Moving to another area, really some of the operational activities and capacity building that we're doing in relation to the increased risks and threats that we've experienced, one of the things that we've spent more time on over the last six to nine months is working closely with first the global forum on Incidence Response and Security teams as well as national CERTS.

Our notion here is that the first line of assistance for a ccTLD operator or domain name – somebody that's a got a domain name system security problem may well be a CERT. In many cases should be a CERT at the national level or potentially even in an enterprise level in a given context.

But that some in the CERT community and I understand that business models differ and we've had discussions with people that are in the room from Nairobi. Some CERTs are tightly tied with their TLD operators and are very aware of DNS security concerns.

Other CERTS, even in relatively well-resourced portions of the globe have much less awareness of the types of malicious activity and technical concerns that have to do with DNS security. So growing the understanding of the CERT community about domain name system issues we believe presents a scalable approach to how ICANN provides value in the security and resiliency realm.

For example, we just conducted a joint session here in Nairobi. We had 35 students, most of whom were associated with either Internet more broadly or a TLD operation specifically in East Africa. There's both efforts at the national level but they're looking towards the formation of an East African Computer Emergency Response team. We gave them four days of training, both on the creation of CERTs but also on technical-level challenges to include DNS security-technical challenges.

We do plan a survey in the near term on how ccTLD operators are working with national CERTs, just really to get a base line on how well that's going and where the gaps might be as we try to focus our efforts in trying to build a national CERT capacity related to domain names systems security.

There is going to be a DNS security workshop at the first general meeting in June. Uri, what's the date for that workshop? We're going to confirm this before I mis-speak. We think it's the 13th of June? So, on the 13th – on Sunday, June 13th in Miami which is where the first general meeting is this year, there will be a one-day workshop on DNS security; again, with the focus of teaching the CERT community, first community more about DNS security issues.

This just builds on a series of briefings and other sorts of collaborations we've had with that community in the past six to nine months.

We do operationally continue collaboration as part of the Confikr working group and are trying to be involved in lessons learned efforts from that effort. Some of the follow-up efforts that are going on in terms of trying to mitigate bot net formation and actually our particular role really being focused on abuse of domain name system by bot nets for command and control.

Then, again, Uri here to my left is the lead for us in terms of security. Our security team, we do have an incident-reporting mechanism. It's really kind of a precursor hopefully to some sort of more structured ongoing incidence response capability. We have a mechanism for those in the community if they think they are systemic DNS security incidents.

It’s a challenge for us and a challenge for anybody who sets up a CERT is really what the lower bound of incidents. The domain name system is so fundamental to the Internet that almost any hacking incident to some degree involves a domain name system. Really, ICANN’s concern is at the level of systemic issues that involve the DNS, the Confikr level abuse, attacks on DNS operations, particularly at the TLD and root level.

In terms of training programs, we’ve got some collaborative efforts. Really the main one has focused on working with the regional TLD associations, all of them: Center in Europe, AFTLD here in Africa, Latin American TLD Association, obviously in Latin America, the Asia/Pacific TLD Association.

We’ve sponsored a series of attacking contingency response workshops, really focused on the managerial level which is threat awareness and contingency planning. In the last six months we’ve done one in Seoul, Korea and did one recently, just a few weeks ago in Amman, Jordan.

I don’t have it at my fingertips the number of these sessions that have occurred but they’ve been going on for approximately a year and a half. I think the number is somewhere in the 8 to 10 of the ACRP workshops that we’ve done.

We’ve also initiated a joint technical training program for registry operations with ISOC. ISOC really focused on the registry operations at the basic and advanced level. Then the ICANN piece of this is really focused on the security level of this where we’ve just started sessions.

So, we’ve had them in Santiago, Chile, Dakar, Senegal, and here in Nairobi we ran a separate session than the one I previously referenced. The Nairobi one was a good example, about 25 attendees representing 8 ccTLDs. In the last six months I know for sure that we’ve reached over a 100 people working in DNS ccTLD operators in 41 ccTLDs around the globe.

I slipped the last slide. Not as huge focus area but there’s obviously a growing interest in just ICANN explaining what it is doing in this role as well as the limits of its responsibilities and roles. As I’ve mentioned, we’re working very closely with regional TLD associations to try to explain those things. They have been fundamental to our consulting on the DNS CERT concept.

We also work closely with ICANN’s Global Partnerships Team to enhance their regional outreach activities. For example, we’ve participated in Interpol workshop that’s really focused on combating cyber crime. But really again, our limited role was the domain name systems potential for facilitating abuse and how ICANN plays a role in trying to understand and limit that.

We also have been part of what’s called the Asia/Pacific Economic Cooperation, usually referred to the APEC Telecommunications and Information Working Group. Again, providing them information about what they’re doing as they raise their understanding of what’s going on in the cyber security realm.

Then we have an MOU with a Russian organization called the Institute for Information Security Issues, which holds an annual forum in April in Garmish, Germany. So we are again co-sponsoring a day long session with them. When is that? It’s the 12th and 13th I believe of April in Garmish. Again, just trying to explain to a more global audience what ICANN does related to cyber security.

We solve global sovereign security issues but that we are part of the collaborative set of organization involved there.

So, with that, I probably ran longer than I wanted to, and I also talked pretty fast because I wanted to explain the initiatives up front. So I will conclude my remarks here and go ahead and take questions from either people in the room or you'll monitor people in the remote participation regarding any questions. I will stop.

Questions in the room?

Alex: My name is Alex Curoo from Kenya. Thank you very much for that nice presentation. First of all, I want to ask in lieu of some of the DNS abuse of DNS level threats that you have been addressing here. I'd be happy to hear sort of like a Kaminski flow. Maybe what can you do about that? Are you following it? Is it of interest to the progress?

The number two thing is that bearing in mind that I've been involved in some of and continuing being involved in East Africa policy development with the governments, in Kenya and East African region. What should – was there any government people, just students. They did not have an affiliation.

I'm wondering about the private sector because I'm aware at some point I was asked to try and think of how I can assist with a CERT.

Craig: Okay.

Alex: And that would be a very good entry point which is with my last question, which is how can one get involved in what you're doing so that they can continue being updated? Thank you.

Craig: Maybe I'll take those in reverse order. In terms of what we're doing, we have a security team portion of the ICANN web page will provide you where that is. The thing that we need a lot, that's most helpful from my perspective and, Uri, you're more than welcome to give yours.

We put these concepts into play. We try to create a dialogue with the community. We need feedback. So when you see things related to security that are going on in ICANN, hey, from our perspective we could use your feedback. If that includes "I need this sort of information", we might tell you this sort of organization provides that information or we may see that as something that ICANN can do.

Moving back up your list of questions, Uri, the question was with the attendees at the just held workshop, first ICANN workshop, were there governmental representatives there? I think that there were questions to try to link into what's going on with some of that.

Uri: It was 35 participation from East Africans, mostly government representatives and regulators and also Kenyic or Kenyaian registries and some private industry as well. But these are invitation-based. Letter invitation sent by CCK. It was handled by the local Kenyan…

Craig: Right. Maybe the easiest thing is to put him in contact with Vincent and Michael, to follow-up on who was participating and how you can get engaged…

[*Two people speaking off-microphone*]

Craig: So, I've managed to lose in the fray of moving back up the queue, what was the first question? Oh, Kaminski. So for those – I hope that many in this session are aware. Back in the summer of 2008, Dan Kaminski announced – he had actually worked for months previously with people that do DNS software implementations CERTs, vendors, a vulnerability to most basic implementations of the DNS protocol.

That vulnerability allows for something that is generically known as "cash poisoning" which allows one to – you basically gain control over how DNS resolution occurs and misdirect DNS resolution, grave opportunities for phishing. Very difficult to detect, certainly at the user level so you could be misdirected to a phishing site that looks very much like the site you thought you were going to, download malware, a lot of potential for malicious abuse.

The principal mitigation, systemically for that is the institution of DNSSec, right? So that effort goes on. I actually realized that when I made this presentation, ICANN is working at DNSSec implementation at the root level. That's preceding – that's hoping by July of this year that that will be fully available. That's just the start of a much longer systemic process of different portions of the DNS resolution tree enabling DNSSec and working through its implementation.

Down to the user, both enterprises and individual users have to basically enable DNSSec in order to stop that cash poisoning through that particular mechanism. ICANN's particular role is on that root zone signing. We're doing that in conjunction with VeriSign and TIA.

Oh, the other thought that was in my head is that we've historically also provided a lot of information on just good practice with DNSSec implementation. There's a DNSSec implementation working group. They held a workshop. I don't know if you were able to attend. That workshop was actually this morning.

But at every ICANN meeting there's a workshop on DNSSec implementation. We can certainly get the link to the DNSSec implementation web page basically, if that's useful to you.

Okay. That was a long answer to one set of questions. Anybody else in the room? Questions?

Male: Thank you first for this quick outlook and very clear as well. My question relies on – I was reading the information commitments paragraphs that are referred to when discussing about this initiative.

It's true where we [inaudible – 36:52.3] to basically say, "What is ICANN doing?" The review will be on what is ICANN doing for DNS security?

My concern is that within the ICANN community we only have a very partial view of the DNS system. A lot of the DNS is actually handled by ISPs. Not here?

Craig: Right. Yeap.

Male: Broses software editors not here either. I haven't seen in your documents how you reach out to them.

Craig: There's good and bad here, right? The bad is that it's not structured yet. Maybe a little more good is growing awareness that we need to do that in a more structured fashion.

One of the ways we learned that is our participation in the Confikr situation involved parties from vendors – Microsoft actually led that because it was their software that had a vulnerability to allow Confikr to kind of get a toe-hold and propagate – they also obviously the [inaudible 38:03.6] resolvers that Microsoft puts in its various software, a big part of how users experience the DNS.

Certainly, with a bigger vendors like NL Net Labs and ICS for Bind, we have an ongoing dialogue with them. One of the ways we hope to put some more structure to them is to get all those stakeholders involved in the DNS CERT.

The working group we have planned is going to involve ISPs, is going to involve software, vendors that are focused on DNS applications to try to get a more mature approach. This is a system as opposed to, again, ICANN's limited view tends to be about root operations and TLD registry/registrar operations.

So, again, that is a work in progress. I think it's a point well-taken. We'll see how we do on the review which starts in October of this year. But we're trying to make progress there.

Any questions from the chat room, Uri? Okay. I will give those who are out there in remote participation another 30 seconds to a minute or so to try to come up, if there's a question that we want to field from remote participation. Then anybody in the room? Any questions?

I don't see really any so unless we see something in the chat room here momentarily, I think we're going to call this session concluded. I appreciate everybody attending. Again, we got one specific set of follow-ups we'll do here.

But again, if you go to the ICANN web page and you click down through the – it's a one-click through the different staff organizations. There is a security team web page. It's not the most advanced at this point though. We're working on it.

So, please feel free to contact us either as individuals or through that web page if you have any concerns. Thank you.