Transcription ICANN Toronto Meeting

Joint DNS Security and Stability Analysis (DSSA) Working Group Meeting

Thursday 18 October 2012 at 11:15 local time

Note: The following is the output of transcribing from an audio. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.

Coordinator: Today's conference is being recorded. If you have any objections you may disconnect at this time. You may begin.

Man: Thank you. This is the join DNS Security and Stability Analysis meeting being held in Harbour C on October 18. And it is now 11:16 Eastern Time. Please go ahead. Thank you.

Mikey O'Connor: Thank you and thanks to everybody in Verizon who does this so well, I mean, it's amazing the kind of support we get from the bridge folks because we run kind of crazy meetings; you'll see how it goes.

And welcome everybody in the room. We're going to do a sort of combination introduction meeting to the DSSA but mostly we're going to do work. And we want to engage you in that work. So if you look at the screen and things get too tiny for you by all means feel free to move around in the room, get closer. You know, we don't do much in terms of formality in this group.

I'm Mikey O'Connor. I'm the GNSO Co Chair for the DSSA. A couple of my fellow co chairs are here and I'm going to let them introduce themselves. We haven't got quite a full complement. Mark Kosters from the NRO is not with

us here in Toronto but Jörg and Jim, you want to just say a little hello and then we'll get underway.

Jörg Schweiger: Don't want to spoil time. Jörg Schweiger, co chairing for the ccNSO.

Jim Galvin: And Jim Galvin from the SSAC although I'm not officially in any formal sense a co chair SSAC does participate actively and they recognize me as a co chair so thank you for that, Mikey.

Mikey O'Connor: I always thought you were a co chair. I didn't know you weren't a co chair.

Jim Galvin: Yeah, we're not part of the formal chartering organizations; it's the other three groups...

Mikey O'Connor: Oh.

((Crosstalk))

Cheryl Langdon-Orr: ...not chartered.

Jim Galvin: Okay.

Mikey O'Connor: You know, I only learned that distinction this week so there you go. We have a number of very shy participants who don't do anything and heckle me all the way through these and we'll let you heckle at will. I'm enlightened to announce that Cheryl Langdon-Orr is sitting in a place where there's no microphone available.

Cheryl Langdon-Orr: No, I can get picked up on Mikey's mic without any problem at all and I'll be for the transcript record so hi all.

Mikey O'Connor: Dang I hate that. All right we'll get...

Julie Hammer: Hi, Cheryl. Hi, Mikey.

Mikey O'Connor: Hey, Julie Hammer's on.

((Crosstalk))

Mikey O'Connor: Yay. Okay Oh and Kosters is on the bridge. Hey Mark, you can say hi if you want. Are you there? He's muted; he's always muted. All right I'll get it going. I'm getting heckled already.

What we'll do just to sort of set your expectations is we'll probably spend about 20 minutes going quickly through sort of the standard spiel for Toronto just to bring those of you who haven't heard this spiel before up to speed on what we've got and then backtrack and dive quite a bit deeper into a couple of the topics that we've got in this spiel.

Because one of the things that the DSSA has done along the way is built a lot of tools and those tools are out there on the Net for you all to use in your own organizations and also we've got some work that we would greatly appreciate it if you did with us and for us.

So let me just kind of go through the usual update deck and I'll try and do it quickly and painlessly, etcetera. So let me just get my mouse in the right place. I'm going to skip that one. So for many of you this is old news; bear with me because this is a bit complicated.

The DSSA is the DNS Security and Stability Analysis Working Group. It was formed after the Brussels, Belgium meeting of ICANN. It sort of arose from comments that were made in Dakar and in Brussels by the CEO of ICANN in which he painted a picture in which the sky was falling and that the DNS was at serious risk of complete collapse, etcetera, etcetera. And I'm making the staff guys very uncomfortable and they're glaring at me.

Man: Mikey, just for clarification I think the DSSA was chartered - or the charter was endorsed after the Cartagena meeting. And the groups...

((Crosstalk))

Man: Yeah, Cartagena, and then sent to them so, yeah, the comments you're referring to go back to the Nairobi meeting, right. And that takes us current.

Mikey O'Connor: Thank you. And that was Patrick Jones, one of the several pretty darn smart staff people that support us. Julie Hedlund is here too. So the charter calls out the fact that there's a need for better understanding of the security and stability of the global domain name system.

And for those of you sat through the immediately-prior meeting there's another committee that's sponsored directly from the Board that's working on a somewhat narrower content charter but a broader functional charter. And we'll get to that in a minute.

But as a result this is a joint committee that has participation from the GNSO, which is where I come from, the ccNSO, where Jörg is based, the SSAC, where Jim Galvin sits, the NRO, which is where Mark Kosters, who's on the bridge and you can heckle by chat oh except we can't - we don't have a chat window.

You want to rearrange the Adobe room so we can get a chat window in there? That would be good. People will be mournful if they can't heckle us by chat so no urgency on that but if we could pick one of the formats where we got a chat window that would be good.

And then our fifth is the ALAC and Cheryl, are you representing Olivier? Oh cool. God, I'm going to have to give you a microphone aren't I? I hate that. Anyway that's our - the basis of our membership.

And unlike most working groups we are a group of people that is selected and delegated by our respective constituency so unlike most working groups in ICANN we are not an open group; we're constrained in terms of our numbers and it's a more formal process to get us in this. And that's partly because of the nature of the work that we do which involves, in some cases, extremely sensitive information.

And so this is not the typical super open transparent process and in fact we have in our charter language that allows us to become non-transparent in certain pretty limited circumstances.

Okay so now we've got a - going to take a break here for just a minute while I rearrange the chat room for just a minute. And share my screen again. There. Somebody's got their phone the bridge not muted and I hear you rustling about. Do you want to speak while I'm fooling around with the...

Cheryl Langdon-Orr: Because it'll stop him mumbling.

Mikey O'Connor: Yeah, the mumbling is...

Cheryl Langdon-Orr: That's the other thing that'll happen if we've got dead air, mumble, mumble, mumble, mumble comes in on the recording. So...

Mikey O'Connor: And Cheryl keeps me on the straight and narrow in that regard. I'm rearranging the chat room just a little bit. I hope that my colleague can stand it. Just get this tuned up to my personal satisfaction and then we'll get underway.

There's Kosters. See I know - oh is there a way to turn up the audio? Is the audio okay now or is it - am I mumbling? Could be mumbling, Mark, so give me a cue on the audio if it's okay or not. Oh it was Julie. Oh okay.

Well anyway I can now see your chat and welcome to the gang. I'll try and make the screen a little bit bigger for you. And then we'll get going. And for any of you who want to watch this silliness on your screens don't do it because everybody has to go easy on bandwidth in this meeting because the access point in this room gets overloaded and it keeps knocking me off the air.

Okay here we go. So a quick summary of sort of what we've done - essentially in the last two years what we've discovered is that before we could actually do the risk assessment that we're chartered to do we needed to build a lot of tools in order to do that risk assessment.

And so this is just a list of the stuff that we've done. I'm not going to go into a whole lot of detail on that. This is what we've been doing a little bit more recently. And we are sort of in a refine, coordinate, align ourselves with the Board effort phase. And for of you who were at the previous meeting you can tell that there's really no daylight between what we're doing and what the Board Risk Management Committee is doing.

But the interesting phrase here is the still-to-come and then in parentheses, if needed. We are going to wait and go into sort of a lower energy mode between now and Beijing because we don't want to get too far out in front of what the Board Risk Management Committee is up to and they're going to do some stuff that we may be able to steal and take advantage of so we're in kind of a take it easy mode.

But once that's done then we're going to make a choice as to whether it's necessary for us to keep going or not. And we want to defer that choice until we've got a little bit more information. So there's a little bit of a conditional branch there.

I'm going to give you the high level version of our methodology right now and then this is one of the slides that I want to circle back to and show you the

tool that we built and encourage you to steal it from us. Because we think it's pretty good. And if there's any way that you can use this within your own respective organizations by all means do so and I'll show you how and where to steal it from.

But basically this is methodology to do a risk assessment that's based on the methodology that comes from NIST, the National Institute of Standards and Technology that's a part of the Department of Commerce of the US.

And it can be read as a compound sentence if you read from left to right. And it says, an adversarial threat source and then - so the blobs - the blue blobs - are the thing - the noun. And the fairly hard to read - and I apologize for that - but the black type underneath it is the scales on which we'll evaluate these things.

And I think it'll probably be easier to see a lot of this when we come back to the actual methodology that we use. The scales for adversarial threat sources are the capability that that threat source has, the intent of the threat source and how tightly they target it.

And we're having a little trouble with that runaway microphone again. We've lost our guy. There may be a volume control on it; if there is maybe we can turn it down? I'm going to keep going.

Man: (Unintelligible).

Mikey O'Connor: It is turned down. For those of you on the bridge we may lose you for a little while and if that's the case just hang in there with us; we'll come back.

The other kind of threat source is a non adversarial threat source. Adversarial threat sources are the ones that get into spiffy newspaper articles, hackers, etcetera, whereas a non adversarial threat source is something like a storm or an act of God or, you know, an error or something like that.

Then there's a whole series of sort of context-setting things that you can do, you know, to what extent are there preexisting conditions that either increase or reduce the risks. There are security controls that you may or may not have implemented in your organization. And there are vulnerabilities that may be relevant.

Ah, the person who knows about this runaway - it's this one over here.

Then once you've sort of set the stage you decide the likelihood that this threat event is going to be initiated.

((Crosstalk))

Mikey O'Connor: I can certainly use that, yeah. See how this one's - oh, listen to that. Stereo. Yeah, and we could actually use this all the way through the meeting if you need because we can just use it like a token and hand it around. So if it's really complicated to fix those table mics let's just go with the handhelds for now. That's fine.

Anyway so we essentially work our way across how likely is it to be initiated, what the threat even itself is and then what the results are and the impacts are. And this has been - this - just like the preceding meeting described this is fairly familiar methodology for those of you who do risk assessment.

I think the key to this one is that we've tailored it a bit for people who function in the DNS. And so you, who are actually involved with delivering or participating in the DNS ecosystem, may find this a handy gizmo. So I'm going to circle back to this a bit later but that's sort of the high level view.

What happens then is that we gave this a sort of preliminary run. I'm going to have to put the mic down for a second.

We gave it a preliminary run and we came up not with actual risks but we came up with essentially risk topic areas that we're interested in exploring more deeply if we continue to the end of this project.

And starting at the bottom are the sort of more technical ones. And as we work towards the top we get more up into the Layer 8, political layer kinds of things.

So one of the - at the bottom of this chart is an inadvertent technical mishap brings down the root or a major TLD, a configuration error or a - just a mistake on the part of a root server operator of some sort or another.

Working our way up is the sort of traditional adversarial threat source; attacks and exploits technical vulnerabilities in the DNS to bring down the root or a major TLD.

In the middle is the traditional non adversarial threat, a widespread natural disaster brings down the root or a major TLD. And then up towards the top of this list we have two that are a bit less technical; one is reductive forces such as security, risk mitigation activities or controls through rules splits the root. And then finally way up in Layer 8 is gaps in policy management or leadership splits the root.

So you can see that the range of things that we are thinking about taking a look at is pretty broad ranging from very technical issues all the way up to very almost organizational kinds of issues. But these aren't - you should understand that these are topic areas that we're interested in. We haven't got much to say about them yet because these are just the areas that we want to work on some more.

Try that - yeah, that's better.

Another one that we're going to spend a bit more time on in this meeting, because this is one that we would like your help with, is the - essentially a map that we are trying to draw of the DNS - the roles and responsibilities within the DNS ecosystem.

And this is a map that we began drawing in our Phase 1 report, which is out on the Net right now. And what we realized that this map is interesting and complicated. And so let me just walk you through this very quickly and set your expectations. We are not in charge of this map. We are merely interested in understanding it better.

And so if you start with the circles most of what we all do in terms of the DNS happens at the edge, you know, I'm from a coalition of ISPs and I consider our members players at there edge. We deal with customers, we deal with peers, we deal with other organizations in the infrastructure. And we do some of these things as ISPs but not all.

Then we, as ISPs, are also interested in sharing and so we participate in what we're calling the glue layer, that's the sort of bluish stuff towards the middle, where we share tips and techniques, we share contacts and so on and so forth. And with a few exceptions we do not participate in the core or steering of the DNS ecosystem.

I just fell off the Adobe room for those of you who are online. I'll show up again in a bit but the access point in this room is severely overloaded and so I apologize for those of you who are online. A lot of you have heard these words before so I'm not feeling too bad for you. But for those of you who are new hang in there.

So that's sort of the layers in terms of the structure of it. But then around the outside are all of these different things that people do. And this list keeps getting longer and longer. In our report the list was only six things long; we're now up to about 10.

And one of the things that we really want to emphasize is that this is a work in a work in progress and it may be wrong. We are sort of in the IETF hack policy mode. We kind of view this as running code but we don't think it's perfect and we're really interested in hearing from you about things that we can do to make it better.

I'm going to jump back on the Adobe room real quick here so that folks online can see it.

So I'm going to come back to this in a lot more detail in a second as well. But do recognize that we aren't in charge of deciding who does what; we're just interested in learning who does what. And we're asking people to tell us what they do and what they want to do. And we've built a gizmo that you can use to do that if you want; if you don't want that's fine.

And one of the things about that is some of you may do things that is something that you don't want to share with the world. And we have a mechanism to help you share the information with us in a confidential way and I'll circle back to that in a minute too.

The slide that's on the screen now is exactly the same except that you can see the preliminary list of participants that we've already identified. There are a lot of people who participate in this ecosystem and we don't think that's the full list. That's just the number that I could fit on a slide without having it be so small that you can't read it.

So if you don't find you, yourself or your organization or your type of organization on that list don't feel bad about that; we still want to hear from you. And so that's just a - our first try; I think we're up to about Revision 5.

We generally don't think single digit revisions are anywhere near close to done; we like them when they get into Revision 10 or 15 on some of them. So don't feel like you're excluded just because you're not on the list.

This is a picture of the worksheet. I'm going to skip this because I'm going to actually - one of the reasons I'm sharing my screen rather than letting somebody with a more stable connection do this is I want to actually open this spreadsheet and walk you through it so I'm going to skip this for now.

But I do want to highlight the things that's on this slide which is that our goal, the DSSA's goal, is simply to complete our report. But there is another goal that's much broader for the community and that's the goal that's come out of things like the SSRT report where there's a broader policy call to refine and clarify the roles and responsibilities of various players when it comes to the DNS.

And I want to make the distinction that we're just curious; we are not the policymakers about this. And so we are gathering what we hope will be useful information for the policymakers but we aren't that policymaking group.

Wrong direction. The conversation that the prior meeting talked a little bit about who's doing what. Let me recap that briefly here. This is a diagram that sort of describes the difference between what we're doing and what the Board Risk Management Framework Committee is doing.

The three pieces, assess, mitigate, monitor, that you see sort of in the background of this slide are a ham-handed attempt, mostly by me, mostly out of a textbook, to give you a sense of what a risk management framework could look like.

The folks from Westlake are a much better source of ideas for that. I've fallen off - for those of you online sorry I just fell off again - whenever I get back on I'll return.

The only thing that's at the top describes what we're up to. We're doing a part of that work; we're doing the assessment part. And we're doing it for a broader scope than the Board Risk Management Committee. So the Board Risk Management Committee is really focusing on ICANN, the corporation and the boundaries of that, whereas our focus is much broader; ours is the DNS in a broader sense.

So we have sort of overlapping scope in different ways. And we, in the leadership group, are pretty confident that we know what we're doing. But if you see something that's going on that you think is goofed up let us know. We're sort of hacking the policy on this as well.

And so that's just a picture that sort of describes the boundaries between us. I'm thinking I'm nearly done. I'm going to skip this one because this is really an inside the working group document. I don't know that it's terribly useful for you all. But if anybody wants to get into details about how the two groups are managing in parallel with each other we can dive back into this one as well.

So if this was sort of a normal update this is where I would stop and I would ask you for questions and so on but I'm not going to stop there for very long except to you give you a chance to ask questions about this sort of high level stuff and then we're going to take a deep dive into a couple of these topics where - we're actually going to open spreadsheets and drive around in them and talk about them.

But from sort of the update standpoint are there questions from the room that come to your mind that you'd like to talk about now? Because (unintelligible) - yeah, we're going to do this token ring style so there may be another mic floating around that could pass around the audience and meanwhile we'll token-ring this along on the table.

Woman: (Unintelligible).

Jörg Schweiger: So this is Jörg Schweiger for the transcript record. I just want to make sure that you do not get the impression by what Mikey's been saying that this group is meant to analyze each and every risk that we have been identifying. We, for sure, couldn't do that.

What we want to do is - we want to pick up at least one example and figure out whether or not the management or the risk management framework we use and the assessing method that we are using that this is working.

And as this project is determined to end in the near future...

((Crosstalk))

Jörg Schweiger: ...there's going to be something following up. And we might come up with mechanisms and suggestions on how to follow on. So just take your time and do not expect too much of this working group if it comes down to risk analysis of the DNS in its full sense. Thanks.

Woman: (Unintelligible).

Mikey O'Connor: You can tell the way this working group works together. Mikey goes out on a limb, says something stupid and the rest of the guys straighten me out; it's perfect.

The one thing I want you to take away from this slide - and it's now back in the Adobe room as well - is that all of the stuff that we're going to go through from now on is on our Website and that's a short URL to get you to the Website. So you might want to write that one down. The best part is the X-4 alpha, baker, 5 part.

We are actually somewhat overwhelming in the way that we keep that Website up to date. If you go there you're going to find probably more

information than you can possibly swallow. But it's been a pretty valuable - it is transparent.

And it does show you how many iterations we go through, you know, because you see every single draft all the way back into the early (marking) history. And unless you're just really masochistic you don't want to read the early drafts because some of them are pretty rough.

Any other questions from the room before we take a deeper dive? Hang on a minute.

((Crosstalk))

Mikey O'Connor: No those - none of the table mics work so, Julie, you get to cover the rest of the room. Sorry about that.

Robert Gara: It's Robert Gara. I'm with the SSAC but I'll be speaking in my capacity as someone from Citizen Lab. In regards to the organizations that are involved, you know, there was research and there was incidents so I'm just wondering if you've made any outreach to the academic community that is working on some of those issues. And if so great; and if not we do some work in regards to that so it'd be keen to follow up afterwards.

Mikey O'Connor: Thank you, Robert. That's a perfect example of what I was hoping we would do in this meeting which is to say here's what we're doing and then somebody say but wait, we do that too. We play on that picture; we have a role to play. We really want to hear from you.

And so the next part of this meeting I'm going to show you how to get to the little data collection document that we've built and strongly encourage you to fill one out. You'll find that the data collection document is pretty well structured to keep you out of sensitive information territory.

This is not a document that we want to use to collect secret stuff; we just want to collect feedback on how you or your organization fit on that chart and it's our hope that, A, we will find some new people today and, B, that you'll tell your friends and that we'll find even more new people through the sort of six degrees of freedom effect of all this stuff. So thanks a lot for that comment, that fits right into our goal.

Patrick, go ahead.

Patrick Jones: Patrick Jones for the transcript. So this - it's going to be useful as our team takes on the SSR Review Team Recommendations and there is Recommendation 4 which obligates us to document the roles and responsibilities of the different actors in the community or in the greater emphasis that touch on SSR.

So having this type of information showing which groups would be good to involve and where there are gaps and groups that are missing would be very helpful for us and also helpful for the different SOs, ACs, stakeholder groups, identify who else should be involved in the conversation.

Mikey O'Connor: If you could just keep talking, Patrick, I'm frantically trying to do something with one hand. Does anybody else have a comment to help out the meeting chair while we get the spreadsheet loaded at the moment? How we doing here?

Julie Hammer: Background...

Mikey O'Connor: Oh background music's good. Yeah, hit it, Julie. Julie and I can talk Minnesota accent if you'd like that later.

((Crosstalk))

Mikey O'Connor: All right. There will be a short pause while I actually get on with my job. Hang on there for just a minute. No respect. No respect. Yeah, I get the respect I deserve. Thank you very - thank you very much. I am such a spaz.

The trick is that I've got this screen with lots of pixels; that's why I have to make everything incredibly small before I go - ah, getting better at this. Okay here we go. So in a minute it will show - there we go.

This is the lag between what's in the room and what's on the Adobe Connect room. This is the spreadsheet - I'll show you in a minute how to get to this. But I just want to walk you through how it works. And I apologize it's fairly small on everybody's screen but you'll just have to accept that this is as good as I can do.

This is very simple stuff; this is - an Excel spreadsheet that we've tried to make work in all the open source formats. If you run into trouble when you're filling it out please do let me know and I will get you a version that fixes whatever trouble you've got.

At the top of this - when you download this you're going to see a tab on the bottom that we're on right now that's the data gathering example. This is the one that I filled out for my colleagues in the ISP community that I represent. We thought it would be useful to see an example of an answer so that you get a sense of the kind of information that we're going for.

And again I want to emphasize this is not about secret stuff; this is sort of what do you think your role is and what role would you like to play? And so at the top is a little bit of, you know, data gathering stuff. We do kind of want to know who you are, who you represent. And we've given you a place to describe how close to a final draft you think you've got.

This one started out at extreme draft; it's sort of down to somewhat draft. It still hasn't really been reviewed by ISPs as much as I would like. And it would

be useful for us to know sort of your take on this. It's perfectly delightful to give us an extreme draft as long as we know it's that way. You know, we won't take it as gospel. And it gives you a way to say look, I haven't checked with everybody yet.

And then what we - you remember that the - the other document had those - that circle thing. Let me bring that circle thing back up so that you can see what I'm talking about. Are you leaving us?

Cheryl Langdon-Orr: Yeah.

Mikey O'Connor: Hot damn.

((Crosstalk))

Mikey O'Connor: I'm wide open. I can do anything and there's no accountability.

Cheryl Langdon-Orr: (Unintelligible).

Mikey O'Connor: Oh dang. Thanks, Cheryl. Thanks for being here. No worries. So I'm going to jump back to the spreadsheet in a minute - well less than that. But just keep this picture in mind. There's a copy of this picture in that file so you don't have to keep track of it.

But what we're basically going to do is work our way around the outside of this diagram and let you describe the role that you or your organization either plays today or wants to play. Let me - get back there. Okay. So the first one is the topic research and analysis regarding the DNS. And then you see that what there are is there's those layers. There's two at the edge and then there's the glue. And then there's the sharing one.

And what we've tried to do is give you a hint over here as to what we're asking you for. So we'll just - we'll work through a few of these just - I'll just

talk them off and then if people have questions I'll drive around in this and try and answer them for you.

But, you know, if we say well - oh and for those of you on the Adobe room sorry I'll see you soon; just fell off again. What we're doing in terms of the research and analysis at the edge for internal operations is we're saying describe the role of your entity in SSR research and analysis of the DNS.

Focus on SSR topics that impact your customers and internal DNS operations in this box. And then if you have DNS research that you do that impacts your organization - your peers or partners describe that in this next one. We've got sort of two layers to the edge because we realize that there's sort of a customer-facing edge and then there's a peers and partners edge and it was useful to sort of make that distinction.

And so what I said to the ISPs is ISPs are especially active and interested in sharing their DNS expertise with research efforts that focus on SSR issues with regard to the DNS that impact our customers and our internal.

So our role is participant in that research. We don't - we, the ISP community, don't generally do research about the DNS; by the DNS we're talking about, you know, root and TLD operation DNS. We certainly, as ISPs, deliver a lot of DNS but that's out of scope for what the DSSA is working on so that's a little bit of a distinction there.

And again in the edge with peers and colleagues ISPs are especially active and interested in sharing their DNS expertise, because we do have a lot of expertise, with research efforts that focus on these issues especially as they impact our relationships with other peers and partners like other ISPs, registries, registrars, root server operators and so on.

And here is another thing that I did in this example that you may want to do. It turns out ISPs sort of have two roles. We have sort of the mainstream ISP

role but we are also - well this is a bad example of that other point. I'm going to skip that point for now.

Then we get into the next layer of our little model, which is this glue and sharing layer. And the description of that is, describe the role of, in this case ISPs, in activities to share and collaborate on SSR research efforts with others in the DNS security community.

Note: This is what - this is where you describe what you share not the actual information that you share but the kinds of things that you share. And where the ISP - at least this preliminary draft answer lands is ISPs participate in this. We participate in it especially in topics such as emerging threats and responses, proactive mitigation strategies, collaboration and so on.

You know, we do a lot with mitigating a lot of the front line stuff like botnets, you know, one of my colleagues is headed off to the (APWD) - coming meetings in Puerto Rico to talk about that and so on.

And then finally there's this steering layer. And here the template is describe the role of your enemy when it comes to actually steering the direction of - in this particular case - research. And whereas before I've been saying that we participate in this one I say that we tend to consume.

You know, we are satisfied to leave the steering of this research with others as long as we can be confident that we can get access to it, that it's going to be of high quality and that it's going to be timely. And this is where there's a parenthetical note, ISPs really have a second role. We are also a local Internet registries and telephone number mapping entities.

And here we probably would want to tend to steer a little bit more because we're right on the front lines and participate directly in the DNS. And so that's a way to hedge, if you want to put more than one entity into your response by all means go ahead and put little notes like this on there.

So I mostly wanted to drag you through this not to show off what the ISPs think but just to show you the mechanics of this thing. Now there are two other things that I want - well one other thing I want to show you and that is that when you get to these little roles things there are little dropdown menus that aren't working. And so snickers are coming in through the peanut gallery.

I imagine that's an artifact of the screen stuff. I'm not going to belabor this but it's going to kill the next part of my presentation because that's where I was going to show off all the dropdown menus in the methodology so this pitch may get a lot shorter.

Let me just run you through all the rest of them, you know, now we work our way, you know, what about standards, tools, techniques, what about education, training and awareness. And you can see that all the way along ISPs have some sort of a role in this. Sometimes it's more, sometimes it's less.

But, you know, that's what we're interested in from the perspective of whatever organization or even, you know, if you want to participate in this as an individual that's fine because there are some individuals in the security space that contribute as individuals.

Anyway so I think with that I'm going to stop sort of belaboring you with this and just do one other thing and sort of show you how to get to this. And again I'm going to have to ask your indulgence while I actually get to it and then shrink it down to a miniscule size.

Are there any questions while I'm sort of fiddling around with my Web browser her? Julie, I see that you had a question. You want to jump I while I play with my gizmo? You may be muted if you want...

Julie Hammer: Which Julie are you talking to? This is Julie Hammer.

Mikey O'Connor: Go ahead, Julie.

Julie Hammer: No I just made a comment oh probably 20 minutes or so ago on the chat that when you had the big circle up and you were calling it - talking about it as the map I just put a little comment in the map - in the chat that one of the things that we can think about is whether those functions depicted on the map could in fact be considered to form part of a risk management framework.

And as Von and (Colin) are developing their thinking the traditional risk management framework's really sort of only got - like there's five or six elements that were on their slide. But maybe in thinking about it a bit more deeply some of the ideas presented on that map could be thought about.

Mikey O'Connor: Thanks, Julie. And I think that's a very useful comment. You know, you're getting - you can't see anything right now because not only did I fall off the Adobe room but I got unpromoted so I can't even get back in. So I'll give you a hint.

Julie Hammer: It's Slide 8.

Mikey O'Connor: So for the remote participation manager who's sitting at the back of the room if you could re-promote me to host that would be great. Oh there I am. The map that Julie is talking about is coming soon to a screen near you on the Adobe Connect and it's up in front of the room.

And I think that one of the interesting puzzles for the - the guys from Westlake - they were applauding you, by the way, you couldn't see that - is that which of these things are part of the risk management framework and which of these things are just functions of, you know, rather than a risk management - which of these are in the framework and which are not is going to be an interesting discussion for them.

And I think that what we're seeing from the DNS Security and Stability Analysis Committee is it would be good to touch on these and say whether they're in or out. And if they're in or out why they're in or out. And also touch on this and say are there anymore because, you know, we'll hack those into our work as well.

So, Julie, I think your comments being pretty well received here in the room and now you can actually see the slide that Julie was talking about there. Thanks.

Julie Hammer: Thanks, Mikey.

Mikey O'Connor: Mark is pretty enthused about being able to see again. Sorry about the choppy stuff going on in the room. It's just one of those days, you know?

Any comments and questions from the room about all this data gathering stuff that I was talking about a minute ago? Jacques. Julie, do you want to be the microphone runner on this one? Hang on, Jacques, you can't use the table mic that's over there.

Jacques Latour: Hello, Jacques Latour with CIRA. So I tried to fill in the spreadsheet on my own and it was a bit confusing. So I think if you go back to the picture - the (unintelligible) slide - I think the idea behind this was this is the ecosystem, these are all the functions you need to do within the DNS. And then we have different organizations with different roles.

And we wanted to do a risk assessment is we wanted to figure out which organization should do what function within what role. And then have the organization compare themselves to what the best practice is and then you do a gap analysis. So if we fill in the spreadsheet right now the idea is that you go in and if you're a ccTLD ideally you should research and analysis.

It's a do - that's something you should do. And then when, as a ccTLD, you go in and you go I don't do it, I just support, then there's a gap because you're not participating in the ecosystem like you should be. Does that make sense?

Mikey O'Connor: Yeah. And I think one of the things that we need to make clear though is that the DSSA is not in the business of telling you, as ccTLDs, what to do in terms of best practices. This is a tool within which to have that conversation. But we're not prescribing, we're not saying these are the things that ought to happen. That's probably a conversation that should take place within the ccNSO in terms of deciding what the best practices should be.

What we're interested in in the DSSA is figuring out what's being done now and sharing that with folks so then they can steal it and decide which ones are going to be their best practices. And that's a subtle distinction that I'm making up on the fly because I'm a guy and when I don't really know what I'm talking about I just make things up and say them with a great deal of gravitas and hope that I get away with it.

But, you know, I think it is important to make the distinction between the DSSA, which is really interested in mostly finding out what's happening and identifying those gaps. And we do have a clause in our charter that if we find the gap that's particularly worrisome we can make recommendations about what to do about that but it's pretty far down the road for us.

And so to the extent that people want to go ahead with out us - especially in the ccNSO and the GNSO I don't think that we would feel badly about that. I've fallen off the air again. So for those of you who are downloading gigantic documents because I'm boring you to death it's perfectly fine to leave but please don't download gigantic documents because it's making the Internet here pretty hard to sustain my little display out to the remote participants.

And, you know, as a feedback thing for the remote participation gang when you have a security group in the room you probably want to triple the amount of bandwidth that's available because we tend to use a lot because we're all really busy.

Anything else about this? This is, I think, useful. Oh I - I made it; I'm back in. Anything else? Okay I'm going to do one more deep dive into a completely different spreadsheet so unless people have other questions about this let me show you how you get to this stuff.

This goes on the never mind pile. I'll wait for another question and bring that page back up. It's one of the things that losing the Internet did is it lost my pages too.

The other thing I want to share with you is the actual spreadsheet that we built to do the methodology itself. And these are - both of these spreadsheets are out on the Webpage that I gave you before - the X/able - blah, blah, blah Baker, whatever it was; I can't remember now quite right off hand.

And again I want to make this a little bit smaller so hang on a minute. This spreadsheet is also out on the Net. And in a second I'll bring it up on my - on my screen for the folks on Adobe so that you can see it as well.

It's - you may want to sort of brand it, you know, write it on the inside of your eyeballs since I'm not sure how long I'll stay on the air. But I'm on there now.

This spreadsheet is - has many tabs but you really only need to use one which is - there are two separate tabs - oh rats. Hang on a minute while I rescale. Yeah, there we go.

And again it's kind of an eye chart for people in the room but I think it's fine if you have it on your own computer. And I'm hoping that in this one the

dropdown menus will work because if they don't I think I'll cut this really short because - oh good, they do.

All right so you remember that sentence - that compound sentence where there's adversarial threat source, etcetera, etcetera. Well this is that same sentence in a spreadsheet with multiple choice answers. It's not saying that you have to use these answers it's just saying if you're thinking about this and you want a starting point here's some - here's a starting point for you.

So in the case of adversarial threat sources if you go to the little square and you drop the menu open with that little tab you get the list that we've come up with as the preliminary list.

And so let's say we take a rogue element as our adversarial threat source. Well then the question is what's their capability? What's their intent and how closely are they targeting your organization?

And again you have dropdown menus that you can choose from where you can say this adversary is very sophisticated, has all kinds of expertise. They're very well resourced. They have all kinds of capabilities. And so you can give them a very high score or you can give them a very low score. And all of these scales are documented in the spreadsheet so that you can sort of have a common language to talk about this.

Again we're just (unintelligible) policy here so if the scales are wrong they're all in tabs; you can change them. This is just our umpty-umph iteration at this. And we are more than interested in hearing your reactions to these. And we'll drive your reactions into the next round of this.

So let's give this - let's give this adversary a kind of a moderate capability. Let's say that their intent is pretty low. And they're targeting your organization specifically. They're really zeroed in on you. They're phishing, they're social

engineering, they're doing the whole ball of wax to try and hack inside your organization.

And a good example of this might be the DotIE event that happened a few weeks ago where it appears that there was some pretty targeted social engineering kind of hacking going on to get in there. That's - this is the kind of place to document that kind of a risk.

And what you see going on then, in this column over here, is that the arithmetic is being done for you. This is a standard kind of technique and a methodology where you do this outrageous math and at the end you wind up with wildly varying scores as to how severe the risk is really going to be.

And we're not entirely happy with our arithmetic yet. This first attempt tends to wind up with sort of exponentially huge numbers sometimes and teeny tiny little numbers on other ends of the scale. And so I think the next time through we'll probably make this a little bit more logarithmic.

But the arithmetic is there and it's all - it's just in the spreadsheet so if you decide to go ahead and fix that on your own please send us a copy of your version and we'll probably steal your stuff and fold it back in in the next iteration of this.

I'm not going to take you through the whole thing except to say that, you know, all of that compound sentence that you saw in the pretty chart is in this one page of this spreadsheet. And so you can very quickly build risk scenarios. And they're easy to modify. One of the things that we like about this is that unlike a lot of these methodologies where you basically have to grind away for weeks to get scenarios built this produces scenarios very fast.

I mean, we could build on in probably about 10 or 15 minutes here. And you can kind of imagine doing this in a room like this with the screen lit up like this and a bunch of colleagues either from your organization or a shared interest

group and just build one of these on the fly, save it off to your disc drive and, you know, begin a conversation.

So the goal with this is to very quickly capture a couple of things. One is the scenarios themselves but another is to capture the questions that say well wait a minute, that dropdown list doesn't include something and that's important to us. And capture those things that are missing from the methodology and easily fold them in.

Again this methodology is available on our site - that same one with that funny - that funny URL. And I can get back to the URL pretty easily although I'm going to have hard time actually getting to the site. So let me put the URL back up on the screen because those tools are all sitting on that site - the X4 able, Baker, 5 site underneath the community at ICANN.

And by all means steal them, share them with your friends, share them with us if you feel so inclined. And let us know how we're doing on this stuff. I think that's enough about that. I could beat this to death. We have certainly done that in the group. I'm getting smiles out of my co chairs here.

Are there any questions about this from the audience? Because I think this is sort of the point at which we'll think about ending - we'll end just a little bit early probably try and wrap up in the next few minutes. Any thoughts about this?

Okay I think with that we'll call it a day. Oh I've fallen off the Net again anyway. I think it's just a little bit of a clue that maybe it's the - maybe it's the remote participation manager giving me a hint that ixnay on the alkingtay. Okay thanks all.

Oh yes, absolutely, thank you again. There's one last thing that we really need your help on and that is that we wrote a very extensive report about all of this and we've been out for public comment for some time now. In the first

round of public comments we got precisely one comment. And the comment was a misfire. It was some fellow with some product that he wanted to promote that didn't have anything to do with our report.

And so we are - we are all fanning out to our respective constituencies and saying please comment on the work that we've done so far. This is an unusual work (unintelligible) that it's cross-constituency. And so the participation by the constituencies has been quite active. And at least in my constituency everybody said well, Mikey, you're doing fine why in the hell do we have to comment?

And the answer is just say so because otherwise we've got no echo from the community on this. And so by all means take a look at our report. The links are on our site. Please download the report. It's easy to comment; all you have to do is send an email. It can be really short; it can be a paragraph that says looks good, keep going; looks terrible, please stop all the way up to you can attach documents if you want to rewrite our report.

But it would be great to get some public comments on this work. Thanks for reminding me of that, Mark. Anything else from anybody? Jörg? Jim, you want to chime in? Getting head shakes there.

I think with that we'll call it a day. Thanks very much for coming. And you can end the recording at this point and we'll shut down the room and see you around the Net. Thanks.

Julie Hammer: Bye, Mikey. Bye everyone.

Mikey O'Connor: See you, Julie. See you, Mark.

END