Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
03 May 2012 at 13:00 UTC

Note: The following is the output of transcribing from an audio recording of the DNS Security and Stability Analysis Working Group (DSSA WG) teleconference on 3rd May 2012 at 13:00 UTC. . 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. The audio is also available at:
http://audio.icann.org/gnso/gnso-dssa-20120503-en.mp3
Presentation will be posted shortly on:
http://gnso.icann.org/calendar/#may

Attendees on the call:

At Large Members
. Cheryl Langdon-Orr (ALAC)
. Olivier Crépin-Leblond (ALAC) (co-chair)
. Andre Thompson (At-Large)
. Julie Hammer (ALAC)

ccNSO Members
. Mark Kosters (ARIN); (co-chair)
. Jörg Schweiger, .de (co-chair)
. Katrina Sataki, .lv
. Rick Koeller, .ca (CIRA)
.

NRO Members
. Arturo Servin (LACNIC)

GNSO Members
. Mikey O'Connor - (CBUC) (co-chair)
. Rosella Mattioli (NCSG)

Expert:
Scott Algeier

ICANN Staff:
Julie Hedlund
Nathalie Peregrine

Apologies:
Jacques Latour, .ca (CIRA)
Jim Galvin (SSAC)
Don Blumenthal – (RySG)

Greg Aaron (RySG)
Nishal Goburdhan (NRO)
George Asare-Sakyi - (NCSG)
Rafik Dammak – (NCSG)

Coordinator: Please go ahead. This afternoon's conference call is now being recorded.

Nathalie Peregrine: Thank you, (Tim). Good morning, good afternoon, good evening. This is the DSSA call on the 3rd of May, 2012. On the call today we have Mikey O'Connor, Andre Thompson, Cheryl Langdon-Orr, Rosella Mattioli, Rick Koeller, Jörg Schweiger, Julie Hammer, Olivier Crépin-LeBlond, Katrina Sataki and Scott Algeier.

From staff we have Julie Hedlund and myself, Nathalie Peregrine. And we have apologies from Rafik Dammak, Jim Galvin, Jacques Latour, (Michelle Gabourdin), Greg Aaron, George Asare Sakyi and Don Blumenthal.

I would like to remind you all to please state your names before speaking for transcription purposes. Thank you very much and over to you, Mikey.

Mikey O'Connor: Thanks, Nathalie and (Tim). As always a great start to our day. We're looking at a pretty full agenda. We'll start it off with our usual - oh I forgot - took it off but we'll stop for a minute and look for changes to statements of interest.

Okay. And so what we're going to do is switch over into review mode today. We want to first off take a look at this draft of the confidential information guidelines and see - this is our second look at this with several hopeful emails from me to the list. So I've got my fingers crossed that this might be the consensus call on this one.

Then we'll take a first look at the draft report that's been converted to the Word version. And this is the draft that we'll be reviewing and editing sort of for the rest of the trip to Prague. And one of the ideas that came up on the

last call - Rosella came up with the idea of sort of clumping our scenarios together. And I've taken a pass at that and stuck that in here. I want to pay special attention to that.

And then if we have time it would be nice to start a conversation about some of the immediate recommendations we might want to make in this draft. Given that this is actually a pretty full report we may not want to do that but I want to spend a little time talking about that.

So that's sort of the plan for the day. And I have to warn you all that I'm in the middle of a very severe storm system today and so if I fall off the call it's not because I hate you it's because I've got a pretty risky connection.

So with that do people - I was thinking I would just take us very quickly through the whole confidential information draft one last time just because I think it's often a good idea to just run all this stuff in front of our eyes just to see if there's something that leaps out at us.

But I'm certainly not encouraging you to come up with changes. You know, I'd like to see us approve this as it stands. But at the same time I don't want to just say yay or nay because I don't think that's proper.

So I'm just going to take you very quickly through it. Do sing out using the Adobe room or if you just need to just break in as I talk if you see something that we still haven't caught.

And, you know, the highlighted thing is that - to protect the information that's being shared by information providers. So this process is a bit tilted towards their needs over the needs of the rest of us.

Then we go through the sort of background of why these sub groups could get formed. And one of the things that we've added just the last round on this one is that last bullet on the page; information providers can specify

additional changes to these guidelines while they're in it because again we don't want a situation where an information provider is trapped in a process that's making them extremely uncomfortable with no way to fix the problem.

Then there's our glorious picture. Actually going to point out that that black blob in the picture actually has some text in it; it didn't show up in this PDF. But that black square is the thing we're trying to prevent which is the most sensitive kind of information - the Type 1 information on the left going directly out to the public. That's essentially what this whole process is designed to prevent.

Then we kind of explain that diagram. We haven't changed that much in quite a while so I'm going to scream through that pretty fast. This is a relatively new addition principally stolen from Julie Hammer but a really good idea which is the notion of a data repository where we keep track of this information.

And then the - probably most important part is sort of how these sub groups are formed. And we modeled this after the (ORARC) process but not entirely; changed it a bit.

This part hasn't changed a lot although the second paragraph where we talk about initial sub group members selected by the co chairs. We did add the information providers to that group of people - the selecting people again tilting this process in their favor.

Another thing that we've done is we've highlighted the fact that these groups don't necessarily get very big. The thought is the more people in the group in the more likely there is to be a breach. And so to the extent that we can keep these groups small the better - a change that's fairly recent.

Haven't changed the roles much. Olivier points out that this version isn't on the wiki and that is my fault. I was looking for it this morning, Olivier, and

realized that I haven't updated the wiki. So I'm planning to do that right after this call. Apologize for that.

So there's - let's see, what have - oh I think the most contentious part was the business about the third bullet on this list where people can be removed if they don't have two people vouching for them. Clarified that a bit so that it's clear that people simply need to maintain a level of two; they don't have to maintain the exact same two. But again this is really tilting it towards the information provider group.

And so there you go. That's the extremely fast recounting of our consensus-proposed version of this. And this is the speak now or forever hold your peace moment on this one. Anybody have concerns about this? I don't actually want to put that kind of pressure on you; if you have concerns this is a consensus process and we'll keep working at it until we get there.

Olivier, go ahead.

Olivier Crépin-LeBlond: Thank you, Mikey. It's Olivier for the transcript. Could you scroll back to the diagram please?

Mikey O'Connor: Sure, hang on a minute. Do this slowly enough that your eyeballs don't fall out. There you go.

Olivier Crépin-LeBlond: And the page just before that one? Okay thanks. I just wonder whether we shouldn't have a little intro or a brief description of where we're going to discuss that diagram because I wonder if the diagram is in the proper place or - because at the moment the diagram is by itself on the page with no explanation around it. And it's not self-explanatory.

Mikey O'Connor: Yeah, maybe what I ought to do - essentially it's explained by this section.

Olivier Crépin-LeBlond: Yeah.

Mikey O'Connor: But what if I moved that major heading number two up above the diagram and then wrote a little...

((Crosstalk))

Olivier Crépin-LeBlond: Yeah, and explain right after the diagram, you know, we will be explaining this now.

Mikey O'Connor: Yeah.

Olivier Crépin-LeBlond: So it's something which links the diagram to the text effectively.

Mikey O'Connor: Yeah.

Olivier Crépin-LeBlond: Because otherwise you'll have people who'll just - of course the diagram captivates your audience. They'll look at that and they'll go I understand a thing; what's going on here.

Mikey O'Connor: Yeah. Yeah, I get that.

Olivier Crépin-LeBlond: Just for ease of access.

Mikey O'Connor: I will put that in. Yeah, I think that's a good idea. So (draw) diagram. And I'm going to consider that a non substantive change that doesn't change our consensus; it's just a clarification.

Julie is typing. So is Mark. Everybody's typing. People can speak. Speaking is good. Julie says it looks fine. Good deal. Rick says it looks fine. Cheryl says - oh I'm reading backwards; my goodness, there's all kinds of stuff in the chat. Mark Kosters says it's okay. I think we're getting to final approach. Cool, I think we're in good shape here. Last chance to say yikes.

If not we'll call it consensus and I'll post it to two places. I'll post it to the consensus items and I'll also post it to the section of the wiki that talks about handling the confidential - just writing myself some notes - remind myself to do both of those.

Cool all right so now we're going to leap into - share Mikey's screen mode and again this is going to be a little risky today because of the shaky connection on my end so we'll see how this goes.

But sharing this document was very difficult today. For some reason Adobe Connect was not willing to let me push this up to the room. I don't know why. So this is the very, very really super ultra first draft of the report in Word format. This is one of the milestones on our little series of milestones pre-Prague.

And from now on we'll review and edit in the Word format rather than the mind map partly because I think it's less confusing and partly because it's really hard to move these things from the mind map that I was using into Word. It took the better part of a day to get this across. So we're going to stay in Word from now on.

And you can see that there's some holes here at the beginning. Cheryl, you may not recall this but I do. Would you be interested in writing that 3a section that talks about sort of the events that led up to the formation of the DSSA? You mentioned at one point that you'd be interested in doing that.

And I don't want to necessarily hold you to it but it would be helpful to me because I wasn't there and so if you would sign up for that that would be just darn nifty. I'm getting a loud silence from Cheryl so she may be going what? Was Mikey hallucinating? Ah, she's saying okay, okay. Up for this (unintelligible) work right.

Everything in brackets is just notes so we'll do a global search on this document for square brackets and make sure that we've done all of our stuff when we're done.

So the first part is talking about the overview. And these are really just notes at this point. And I'm sort of dragging you through this because at least for me I know a lot of times it's awfully hard to find the time to actually review these documents that I keep sending to you. So I'm just sort of dragging you through it and telling you which parts are notes and which aren't.

But the next part isn't notes; this is actually pretty close to final because these - this definition of the DNS that we've come up with is something that we hammered on for quite a while. And so I just want to sort of highlight it for you. This is the picture of it that we came up with.

And then underneath that is the list of pieces just written out and also a list of the things that we're not taking a look at. And again this was a long conversation so unless people feel very strongly about this this is actually in consensus-approved status already.

Another piece that's not consensus-approved but that we talked about at the - let's see, which meeting - I think this was at Dakar that we came up with - this was a document that we developed for the meeting with the SSRT group because it became clear that they were thinking that we were doing a bit more than we really were.

And so we drafted this up to sort of give people a sense of the whole security management pile as opposed to the little tiny risk analysis pile that we're working on. And again this is not yet approved by us so this was something that was developed by the - pretty much by the Ops group. And the - you know, we never really ran this by the full DSSA so this is one to take a look at with a little bit more care than normal.

Yeah, Cheryl, I'm afraid that my connection is to blame for the dropping in and out problem. It's raining to beat hell here. So anyway then the next section is pretty drafty but it's - these are the high points that I'm looking to expand a bit that sort of describes how we did the analysis up until now and also highlighting the fact that we did a lot of work on process here.

And so the - it's interesting to me that the outline is still a little bit goofy. This is a whole huge section, 4c. And it needs a lot of filling in. Then what we've got is the meat of it; this is the actual level frequency severity of threats. This is one of our four charter items.

And this is the part that today I want to slow down because I stole an idea from Rosella. Oh, sorry, Julie's got her hand up. Go ahead, Julie.

Julie Hammer: Hi, Mikey. Sorry to take you backwards a couple of pages. But that diagram where you had all the boxes with the - that's the one exactly. I was just having a little cross check with the charter - well I think I've got - I'm not sure if I've got the final charter or the draft charter of the working group.

But it also - unless it was removed in the later version - it also made reference to identifying the gaps in current security response which - and - which doesn't seem to be encompassed in this diagram there. And I might be looking at a wrong version of the charter...

Mikey O'Connor: No you're absolutely right. And I think it's - it's - my immediate way of addressing that would be to add the gaps phrase to the stuff that's in scope on that diagram; say something like analyze risks, identify mitigation and repair actions and perhaps say something like identify gaps and mitigation and repair actions - something like that.

Julie Hammer: Okay.

Mikey O'Connor: Yeah, that's a very good catch. I will add that to that picture. Good one.

Okay so onto the two kinds of scenarios that we have been doing. I drew sort of a spiffier full color version of the picture that was in the methodology because the way that we've structured our compound sentences changes the picture ever so slightly; it's got all the same words it's just that the boxes and arrows are in slightly different order.

And the thought was that we would use this picture to sort of introduce the clumped scenarios. And so the way that you would read this is an adversarial threat source that has capability, intent and targeting in the, you know, blah, blah, blah you can just read across from left to right. Eventually creates risk. And that's what we're about is taking a look at the - at the situation there. Oh man is it raining. It's like monsoon season here.

So then what I did - and I'm not pleased with this word yet because it's not clear. But what I did is I clumped - I did the same clumping that we had on that spreadsheet last time. And I took the three scenarios that we put in the sort of splitting the root clump. And I took the narrative part and put it - put the three scenarios together - yeah, right out of the worksheet.

And then what I did is I combined all of the rest. You know, so if I switch over to that worksheet it's going to be hard for you to see but here's the clump that we were looking at so there's the narrative part that I stapled in the front.

And then what I did is I took all of the vulnerabilities and I smashed them together. And I took all the predisposing conditions and I smashed them together, etcetera. So that's how I - oop - that's how I came to these lists of threat sources, vulnerabilities and so on for the three scenarios.

And I sort of want to stop and circle back to Rosella because, Rosella, this was your idea. And I wanted to see if I had done what you wanted me to do when you - oh good so Rosella is saying that, yeah, I'm on the right track, cool. All right.

Now I want to plant a question in your minds collectively. And that is we could leave the report at this level of detail basically just a series of bullets. And I'm not going to drag you through them all because it'll take quite a while. But it's pretty easy to follow in the draft.

We could essentially leave these bullets at this level of detail and just say that we're going to define these in much more detail during the next phase, the go-deep phase, which is my preference as your Secretariat on this one. Because I think that defining these, you know, and writing paragraphs about them is actually a pretty substantive piece of work and I'm not sure that we have time to do that between now and Prague.

But if people wanted to we could have a go at that. And if you want to do that then I'm going to have to split this job up because, you know, there's quite a lot to defining these I think. And so my tendency would be to say these are the ones we've identified. We will go deep in defining them and assessing them in the next phase but this is our topic list for our next analysis.

So you can think about that. We're certainly going to come back to this discussion again. You know, mostly today what I want to do is introduce you to this so that you can start thinking about it and highlight the smashing together that I did.

So that's the first clump. Then the next one is really straight out of the scenarios that the ISOC developed. And they had a standard consultant's two-dimensional matrix. And these two scenarios are the half of the matrix that addresses what they call reductive forces which is the sort of over use of security risk mitigation control through rules, etcetera, to split - that eventually inadvertently in some cases lead to splitting the root and then the two ISOC scenarios that describe those.

And again same thing smashing together the vulnerabilities, etcetera. And so on. So I'm going to leave this section of the report. I just wanted to introduce you to it. But it's quite long and if I go all the way through it it's going to take the rest of the call.

Then we do the exact same thing with non adversarial threats which the diagram is almost identical. Really the only difference between the two diagrams is in the far left chunk. A non adversarial threat source doesn't have the same analysis dimensions. They only really have a range of effects; they don't have capability, intent and targeting.

So these diagrams should look to you almost the same because they really are. But it's I think always good to remind ourselves of the sentence that we're trying to fill in.

And then we really had two clumps in this one; we had the natural disasters clump and in our examples they were both power outages but I think we might want to, in the next phase, expand some of those. And again here we go through the combined list.

And then the last clump I put a title on of inadvertent technical mishaps. And we really had three - oh I'm not sure that's really right. I think that's one clump and then there's another clump because we - well that's it, yeah. So anyway those are the five big clumps of stuff that we are saying we're going to take a look at.

And then in part - this is a whole - this again is a very large section of the report that we haven't really started working on. And so I just wrote myself some little notes here and I'm inclined to say that much of what we say in this section will probably have to wait until we go deep. Although I did write myself a note that we may find some pieces of the SSRT report that we want to mine and put in here.

And then this is also the place where we start reminding our readers that this risk analysis may look different depending on where you're standing in the community of DNS providers. Root server operators may have a different perspective than ICANN who in turn may have different perspectives than gTLD operators who in turn might have different perspectives than ccTLD operators.

And I think that one of the things that we're going to want to highlight in this draft of the report is this notion that while our charter says that we are supposed to come up with a unified view of this that may be very difficult to do. And we may want to essentially come up with several perspectives on this - especially this section of the report and this next one which is the risk mitigation activities. So these are really just notes at this stage of the game.

And then another big, big section - and I think the last big, big section - is the - sort of the approach section. And this is where we - we'll talk a bit about go fast versus go deep and the fact that this is the go fast report. And this is the pyramid that I'm referring to in that note. This needs to get revised so that it makes a little bit more sense for what we're talking about.

But I stuck it in here just as a placeholder. It sort of gives us a chance to say, you know, we're at the top of this right now and we're planning to go downward in the next phase based on these scenarios that we've developed. So this is very sketchy.

And then another part of this approach section is where we'll talk a lot about the methods that we, you know, that we selected, the NIST 800-series methods.

And so this is straight out of the update text, the rationale that we used, you know, that we thought we'd get a better work product by using this, etcetera, etcetera. Came up with, you know, took a look at a bunch of them. I've listed them here so, you know, some of this is getting fairly close to complete.

And then, you know, a lot of talk about - this is kind of repetitive. And I have to sort of compress out the repetitive part because a lot of that has already appeared. But then talking a bit about the tailoring and the trouble that we had with the scaling problem that we ran into earlier on because...

((Crosstalk))

Mikey O'Connor: Somebody want to break in on me? Okay. I'm going to carry on. Then we've got the confidential information thing. This is showing the actual black text that I mentioned in the earlier one so that'll get in.

And then beginning to sketch out what go deep looks like. And this is very (outliny) at the moment but if you're comfortable with where I'm headed with this I'll go ahead and begin filling in some of these gaps.

One of the questions that I think we do need eventually to get back to our charterers on is are we going to do one more iteration and then call this done, in other words are we, you know, basically a project? Or are we the beginning of something that goes on essentially forever? I think that's a profoundly important question for our charterers to think about. And I want to pose that question in this section and sketch out sort of the way each of those would look.

The first section of this is talking about the next iteration, go deep. We'll do, you know, more depth into the scenarios; we'll break into more independent teams. You know, I think the only way we'll be able to get through those scenarios in any reasonable amount of time is to break into separate teams to tackle each and sort of keep each other up to date on what we're doing.

Then I stuck the work breakdown structure in here but I'm planning to also put a whole bunch of detail of the tasks. This is - this next bit is straight out of

the methodology. And so I won't review this a whole lot. But I do want to highlight that this part I think we should do again for the next phase.

In a perfect world this would all have been done before we, the DSSA, got started. And I think that we owe it to the next phase team to do this for them in this phase so that they have the answers to these questions before they start.

And I'm going to take a stab at that in this - in the next couple of drafts of the report because part of the reason we struggled so much is because we didn't have the answers to these information and I think it would be really helpful to the next iteration team if they did.

Then this next part is the part that we did or will do in the next phase. You know, we've sort of done a very, very preliminary version of this but the next phase we'll do a much deeper version. And then in the methodology this is where the idea of an ongoing entity or an ongoing group or an ongoing effort or something that continues beyond the project part of the DSSA really starts to creep in.

And some of the interesting questions that come to my mind is - are things like well who would do this? And what would this group look like? Who could participate in this ongoing monitoring, these ongoing updates to the risk assessment?

And so I - with my white socks on the veranda looking out over the cloud forest of Costa Rica invented pretty much out of whole cloth what such an ongoing group could look like. And one of the reasons that I think it's really important to go back to our chartering organizations is that it's a bit different than the DSSA as it stands today.

And we need to - if we go in this kind of a direction we need to make it clear to the chartering organizations what we're proposing. And I'll just briefly today

highlight some of those differences and then I'm expecting that on some subsequent calls we'll go into this topic in a bit more detail before we publish the final version of the report.

But there idea that I had was that, you know, we could describe the purpose of this ongoing thing with those three bullets that, you know, this group - this gang, whatever it finally looks like, unites around this idea of keeping an eye on the existing and emerging threats to the DNS partly by doing sort of deep analyses like what we're doing now but partly by also collaborating on some monitoring kinds of activities.

And that this would be a community - a trust community that could share these ideas and develop resources. I think one of the things that we can take great pride in in this round of the work is the tools that we've developed and especially that sort of one-page worksheet that anybody can use to develop risk scenarios on their own very quickly.

And I think that we've got a pretty good track record in that regard and could use that just as a springboard to kind of carry on. As I thought about that then I came to several sort of next conclusions. One - and I think this is one that ICANN struggles with across the board; I don't think this is just a security struggle but it's sort of the roles and responsibilities thing.

And the great caution that the community has about imbuing a lot of power and authority in the middle at the core and saying - and so I tried to put that in words here and say look, you know, authority should happen at the edge; it should happen as close in our case to the DNS provider as possible.

And that the core is really the place where we coordinate and share ideas but there's not a lot of authority or power in the core. The authority should remain with the people who are closest to the problems to be solved.

And then this is another one that we'll certainly need to go back to the ACs and SOs and talk about. You know, we saw this in Costa Rica where there were people who were saying hey this is a - this is an organization or a group that I'd like to be a part of. And why did they - why did they want to be a part of it? Well because they agree with the purpose; they feel like they have something to contribute to this ongoing monitoring and analysis of threats to the DNS.

And they may not necessarily have a gateway path through an existing AC and SO in ICANN. And so we'll want to highlight that with our charterers and the rest of the community and see whether that's a good idea or not.

You know, I'm going to speed up a bit because we're getting towards the end of the call. But you can sort of see, you know, I actually went into a little bit more detail on that idea in this - on this section where I talk a little bit about doorways for people to get into this thing.

So I'm not sure that, you know, this is a complete fabrication on Mikey's part sitting on the veranda at, you know, after the Costa Rica meeting. This may be a complete craziness and that's fine with me.

But one of the things that - oh I guess there's one major drawing that's not done yet. But let me describe a drawing that I'm imagining which is a series of concentric circles where the concentric circles are at the center; we have ICANN staff and us and SSR thought leaders, tool builders.

Then the next outward circle is the - what I'm calling the glue layer between the center and the edge. That'd be the constituencies and related organizations like (ORARC) and so on. And then the edge would be the actual deliverers, providers, consumers of DNS. So that would be the circles.

And then the spokes or the pie slices, the sections of these circles, could be risk assessment, maybe education, tool building. I threw this in - this is

straight out of sort of traditional security methodology that would probably be pretty sensitive if there was a lot of audit authority at the core. That's not what I mean.

What I mean is the core might develop audit tools but, you know, I think the responsibility tends towards the edge for actually doing the audits and deciding where an organization might be out of compliance.

I don't have any enthusiasm for the idea that there's a centralized audit authority that comes out of this project. I think that that runs us right into the same wall that ICANN ran into a couple of years ago when they proposed a centralized cert. And so I'm not trying to imply that at all.

But anyway that's the diagram that's not done yet. And in fact I'm going to write myself a note that it needs a diagram because otherwise I'm going to forget because I have no memory.

And then in the appendices - I think the appendices in this report are going to be pretty large. We actually have a bunch of material ranging from a whole lot of background material that are sitting in a really disorganized mind map right now to the methodology, to, you know, I'm thinking the details of the confidential information protocol may go back here. We've got a building glossary.

A lot of this is pretty mechanical work that I feel pretty comfortable in doing. But I wanted to drag you through this outline stage by stage today because I know that it's pretty long and it's pretty tough for you all to find the time to review it except on these calls.

So I want to stop now and check in with you and see if you think I'm on the right track with this because this is kind of the point at which if there's something major missing this would be a good time to remind me of it or if you think I'm crazy this is a good time to tell me that.

Julie, go ahead.

Julie Hammer: Just a few ideas that occurred to me as we're going through, Mikey. While we're on the appendices there I do agree that it's really good to push as much of the background and supporting information as possible into the appendices.

And particularly I think with regard to the methodology because to digress into explaining I guess the process that you came through to select the methodology might break the flow of the report.

So I would almost be inclined to put some of the discussion that seems to be in the main part of the report about the different methodologies that you considered and why you selected the one that you did I'd almost be inclined to put that into the appendix so that the flow of the report doesn't digress, if you like.

But - and also with the confidentiality I think just a short paragraph saying, you know, we have developed appropriate protocols to manage confidential information and that's explained in the appendix. I think that's a really good approach.

One of the things that I have been wondering about - getting back to thinking about the scenarios themselves how - the way those scenarios have arisen in the last couple of weeks is that various people have put their minds to work and put a lot of effort in and developed some examples and then they've been logically grouped.

So I guess my question is how - is there some sort of a systematic way that we can think through all of the possible potential scenarios to make sure that that's a complete set for this report and make sure that there aren't' some

serious gaps? Or do you think that it's a reasonable thing to just put those out to the community and ask the community to respond as you've said?

I guess I'm just wondering whether there's some sort of a systematic thought process that the group could go through to see whether those examples are a really robust set?

Mikey O'Connor: The problem we ran into is the one that's on the screen in front of you, Julie. And I think we ran into this just before the...

Julie Hammer: I joined...

Mikey O'Connor: ...Costa Rica meeting. And what happens if you - what the methodology says to do is to start with each of these layers and develop them all and then progress through the layers. And what we ran into was that with each additional layer the branches in the trees grew bushier and bushier and bushier and we wound up with horrendously long lists of things that were very difficult to get through in any reasonable amount of time.

And so the way to break that log jam was to go to the other side of that diagram and look the other direction; essentially pick a point on the right side of the diagram and then select the layers that supported that point.

And so you're right, the way that we arrived at the 12 or so scenarios that are really now clumped down to five was idiosyncratic. I mean, we basically just threw that idea out to people and said come up with your scenarios and we reeled them all back in and then combined them.

I think in the go deep section one of the things we're going to have to do is keep working this issue to make sure that we don't have at least major gaps. I think that we will always have some gaps because it's just the nature of the beast. But, you know, we've really struggled with this. And I'm watching my screen...

Julie Hammer: It's very difficult, yeah.

Mikey O'Connor: Yeah.

Julie Hammer: No that sounds fair enough. And I can see that there is logic in that approach in that the really important scenarios will come out. And, you know, with sufficient number of people looking at it then I think you're right, you're not going to have any important gaps.

Mikey O'Connor: Yeah, and I think that one of the things that this conversation tells me is that writing this section is going to be very important for the group in the go deep phase. Because we don't want to present this list to the go deep group as the definitive list...

Julie Hammer: Yes.

Mikey O'Connor: ...but rather as an example list that they should look at very hard to make sure that there aren't gaps in the - oh, somebody just came in with their speaker turned on. Spectacular.

Cheryl Langdon-Orr: No it's me. I've been very quiet because my system is echoing. I just wanted to reiterate - and I can do it with an echo, Mikey - it's Cheryl for the transcript record. This has to be highlighted so sort of upper case and underlined type highlighting.

Mikey O'Connor: Right.

Cheryl Langdon-Orr: Now I'll turn my mic off again.

Mikey O'Connor: No, I think that's right. And this is exactly the reason that I wanted to go through draft section by section. And - clearly this is basically what we're

going to do now for the rest of the time before Prague is keep coming at these sections sort of one at a time, maybe two a time on each call.

And then, you know, I will go off and do some drafting over the weekend and get something out to you to take a look at because this is very helpful for me as the Secretariat...

Julie Hammer: One other thing that is sort of still unclear in my mind as well - and I'm not sure that it necessarily needs to be addressed in the report but maybe it is something that will puzzle other people as well is I'm not clear in my own mind what the relationship of the work of this group is to the - well I don't think it's up and running yet - the proposed board DNS risk management framework working group.

Mikey O'Connor: Oh I should...

Julie Hammer: Because they sound like quite similar sort of focused groups. I saw on some - it's mentioned in the SSRT report that the board has agreed that they're setting up a DNS risk management framework working group. Cheryl, is that - am I remembering that correctly?

Mikey O'Connor: Let me speak for Cheryl since she's got a...

((Crosstalk))

Julie Hammer: Yes you are.

Mikey O'Connor: Go ahead. You want me to do it or do you want to do it? I'll go ahead and do it. The person who's chairing that is Bill Graham; he's a member of the Board. And Bill and I have gone back a few times - back and forth - trying to work that out. And the note that I'm going to take is to write a section that also describes the relationship because...

Julie Hammer: That would be really helpful I think and would clear up confusion for people reading this report.

Mikey O'Connor: Yeah, yeah. Because I think that part of the puzzler in this is that the Board committee is still sort of trying to arrive at their own conclusion about that. And so their charter is changing a bit. But I need to circle back to Bill and see about that.

Okay we are down to the last minute on the call so I think I have to cut it off at this point. Julie, did you have a couple a more bullets that you could just throw at me and then we can pick them up next...

Julie Hammer: No, that was everything. Thank you. Sorry to hog all the time.

Mikey O'Connor: No, no it's precisely the reason that we do this is to get these ideas so that I can steal them and then I'll feed them back. And for the rest of you basically this is what we're going to keep doing so if you've got ideas that you've come up with that you didn't get a chance this time do write yourself some notes or something to remind yourself so that we can pick right up again where we're breaking off now.

And we'll just work these things in. Effectively we've probably got somewhere between two and four more meetings of this sort of intensely improving phase to the report. And then the rest of the meetings are going to be the final touchup before we release it to the community.

So we've got at least two or three, maybe four more meetings where we can add big ideas like the ones that Julie came up with today. And so don't panic; you'll have a chance to add your thoughts. And feel free also to post them to the list if you want.

I think with that, Nathalie and (Tim), we are going to call this one a day. Thanks ever so much to all of you and we'll see you in a week.

Julie Hammer: Thanks, Mikey.

Nathalie Peregrine: Thank you, (Tim). You may now stop the recordings.

END