

Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
10 November 2011 at 14:00 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 10 November 2011 at 14:00 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-20111110-en.mp3>

On page: <http://gnso.icann.org/calendar/#nov> (transcripts and recordings are found on the calendar page)

Attendees on the call:

At Large Members

- Cheryl Langdon-Orr (ALAC)

ccNSO Members

- Takayasu Matsuura, .jp
- Katrina Sasaki, .lv
- Luis Diego Espinoza, .cr

NRO Members

- Carlos Martinez (LACNIC)

GNSO Members

- Mikey O'Connor – (CBUC) (co-chair)
- Rossella Mattioli – (NCSG) – on adobe connect
- Don Blumenthal – (RySG)
- Rafik Dammak, GNSO
- Scott McCormick (IPC)
- Rick Wilhelm, Network Solutions
- Forest Rosen GNSO

SSAC

- Jim Galvin (SSAC)

ICANN Staff:

Patrick Jones
Nathalie Peregrine

Apologies:

Olivier Crépin-Leblond (ALAC)
Greg Aaron – (RySG)
Joerg Schweiger.de (co chair)
Mohamed El Bashir (At-Large)
Julie Hedlund
Ondrej Filip, .cz

Coordinator: The recording has started and all lines are open. Please go ahead.

Nathalie Peregrine: Thank you, (Sam). Good morning, good afternoon, good evening. This is the DSSA call on the 10th of November.

On the line today we have Rosella Mattioli, Takayasu Matsuura, Jim Galvin, Rick Wilhelm, Don Blumenthal, Katrina Sataki, Rafik Dammak, Cheryl Langdon-Orr, Mike O'Connor, (Salees Rosen). From staff we have Patrick Jones and myself, Nathalie Peregrine.

We also have apologies from Jörg Schweiger, Greg Aaron, Julie Hedlund, Olivier Crépin-Leblond, Ondrej Filip and Mohamed El Bashir. I would like to remind you all to please state your name before speaking for transcription purposes.

Thank you very much and over to you.

Mikey O'Connor: Thanks a lot Nathalie. For those of you who don't know Nathalie does this incredibly cool complicated thing to get the audio on the bridge about 20 minutes before these calls and I just wanted to give a tip of the hat for that; it's a fabulous thing.

Welcome all. Looks like we took a little bit of an attendance hit; it's probably a bit close to the Dakar meeting. But I think we're going to keep going. We're probably not going to be doing any decisions, per se, and as a result I think proceeding with this small a number of people on the call is all right.

If we were going to be doing any kind of consensus decision making I think we're getting close to saying this isn't enough people. But given that we're mostly doing updates I think we'll go ahead. Please can read or listen to the recordings.

The agenda today starts off with our quick pause to let people update their statements of interest if anybody's circumstances changed and they want to let us know that would be a good thing to do right now.

Rick Wilhelm: Mikey, this is Rick Wilhelm. Mine will be changing after the - around the Thanksgiving Holiday here in the US in a couple weeks. So...

Mikey O'Connor: Okay.

Rick Wilhelm: ...I'll be needing to resubmit that.

Mikey O'Connor: Cool. Are you going to still be with us on the...

Rick Wilhelm: I'll be with you wearing an SSAC hat, not wearing a GNSO hat.

Mikey O'Connor: Oh excellent. I'm so glad to hear that you're going to be...

Rick Wilhelm: At least until I figure out what I'm doing next in which case then I might have to reevaluate but that's where we're at now.

Mikey O'Connor: Yes, well we should publish that on all the email lists inside of ICANN so that you could get to stay on our working group; somebody from inside the ICANN community can hire you.

Rick Wilhelm: There you go.

Mikey O'Connor: Thanks Rick. Anybody else want to update their statement of interest? Okay three things of substance. First I want to take a while to kind of consolidate

the conversations that took place in Dakar. And then we'll talk a little bit about an approach to ranking the threats and vulnerabilities that we've identified so far.

And we'll also talk a little bit about the approach to the next big phase of the work which is analyzing those. So that's kind of the plan for the day. Let me switch us over to the Dakar stuff. There'll be a short pause while I do that.

Here's the mine map that we've been using to plan that meeting and also summarize the results of it. Let me just very quickly take you through what I know so far. And while I'm doing that if those of you who got feedback from Dakar want to think about things that you want to add that would be good.

I'm going to start with the DSSA meeting itself just because it's up there. And the one piece of feedback that I got from myself and others is we're never going to do that remote leadership thing again. That was a really bad idea. I hear Cheryl chuckling and I, you know, that was just not a good plan.

Cheryl Langdon-Orr: It worked well as a voice of God though; I did like the whole deity-like...

Mikey O'Connor: Yes well that's not my aspiration is to become the voice of God. So we'll figure something else out for DSSA meetings in subsequent ICANN sessions. That's really the only feedback I got on that meeting. And I think it's very important that we - if anybody ever thinks about doing that again in any other working group that we cite this experience as an example of why you don't want to do that.

Moving on to the updates that we got from the supporting organizations and advisory committees my remote session in the GNSO actually did elicit feedback. That one went better partly because it was much shorter, I think, and partly because it was not intended to be anything but an update.

And we got a - several pretty specific ideas that you can see listed on the screen there. One was don't forget about the other DNS providers like for example (Dine) DNS or any one of, you know, there's - I don't know how many, at least a dozen of those - that we might want to invite some of them to join us in this conversation.

We had a pretty lively discussion about reputation systems which then jumped over to the list. So some of you who saw that conversation - mostly between Bill Manning and Jim Galvin but others joined in as well - that we will probably want to fold into the analysis somewhere.

We had a conversation about the scope statement because in our work we've sharpened - I don't think we've changed but I think we've clarified the scope statement from our charter to make it clear that there's a fairly substantial part of the DNS universe that we are excluding from our analysis.

And we got some commentary especially from Jeff Neuman who's one of the vice chairs of the GNSO, that we want to make that very clear in our work, in our - especially in our report.

And the sense that I got from listening to Jeff is that there might be some disappointment from people on that. And in fact then in our meeting - our DSSA meeting Rod Rasmussen came in and expressed that disappointment.

That said unless anybody really gets excited about it I think we're going to continue on the course that we've got. I'm mostly saying that because I'm wearing my project manager hat and my concern is that if we broadened our scope to handle everything we would never finish. And I think that we just need to acknowledge that boundary and carry on. But if anybody feels strongly we can revisit that at some point.

Then in terms of the ALAC or the At Large - I should really put At Large in there instead of ALAC - we got a little bit of feedback but also a promise from Olivier that more is on the way.

And so there's either a write up or a transcript that needs to be reviewed or something so anyway that, you know, there apparently was a pretty substantial conversation in various At Large meetings about this. And I think the same is true for the ccNSO. So I think we've got some outstanding work yet to come back from those two organizations.

I'll put Jim and Rick and some of the other SSAC folks on the spot. Did you all have a chance to talk about this in the SSAC? And if so was there any feedback for the group that we should be aware of?

Jim Galvin: Only to give an update on progress. I mean, we didn't - we really weren't looking for comments. I mean, in general you're more likely to get good feedback from SSAC if you give us something to review.

Mikey O'Connor: Oh okay.

Jim Galvin: There are plenty of people who are part of this who are also SSAC members. So, you know, you'll get the kind of ordinary involvement and engagement that you're looking for from a security point of view. But, you know, other than that you probably won't get anything explicit from SSAC until we actually have something to show them and put in front of them and say please comment on this.

Mikey O'Connor: Okay.

Jim Galvin: So this was Jim Galvin. I probably should have said that up front.

Mikey O'Connor: Oh thanks, Jim. Yes, for those of you - if we can identify ourselves by name for the transcript that would be great. Just going to put a stub in there for the ccNSO. Anyway that's the news from that front.

Moving around to the joint meeting the sense that I got from our meeting Thursday morning with the SSRT group is that they are pretty focused on writing their report. And while they're amenable to coordinating with us they're not really focused on that. And we had a pretty broad discussion about scope and the difference in the scope between our two project teams.

Theirs is very broad; it's a management review of sort of the whole universe of security, stability, reliability; whereas ours is much more focused and really sort of a subset of a risk management process.

Which brings me to sort of the words of the week for me which was risk management framework, you know, that term popped up a lot in any number of discussions.

And before I get to that one other development that I added to this chart is that the Board has formed a security subcommittee that's also taking a look at security, stability, reliability kinds of issues.

And we talked a little bit about this on the op/leadership call earlier this week. Patrick, are you on the call today?

Patrick Jones: I am on the call today.

Mikey O'Connor: Oh cool. That's - then I'm going to throw the ball to you to sort of summarize this particular topic for the group. It seems easier than for me to do it since you're involved in all three of these groups. And, you know, could you kind of give us a sketch of what's up with that and...

Patrick Jones: Yes.

Mikey O'Connor: ...where things are headed?

Patrick Jones: So in - and this is Patrick Jones for the recording. In Dakar the ICANN Board approved a resolution to create a DNS risk management framework working group. And it's a Board-level working group but it has participants who aren't on the Board; some of them you'll - those on the call probably know quite well.

Bill Graham is the Chair of this group but it includes participation from Patrick Fältström who's Chair of SSAC, Roelof Meijer who's the CEO of .nl, Ram Mohan, Ray Plzak, Bill Woodcock from the Packet Clearinghouse and Suzane Woolf.

It's not real clear to me yet what this group - where they're going to start. But in Dakar it - they approved a charter or the Board approved the formation of this group. They have a charter. I think they'll start to have their initial call.

And one of the things that they'll do look at the work of existing groups including the DSSA, you know, the work that's been done so far by the Affirmation Review Team for SSR and then other groups like it.

Now I'm not sure beyond that what the plan is because they were just announced in Dakar. I would think there should be a - some kind of coordination call between this new group and the co chairs from the DSSA and we're going to try to set that up.

Mikey O'Connor: I was on mute, sorry about that. Thanks, Patrick. Perfect. So I think that what comes out of Dakar at least for me is this notion of a risk management framework. And we are chartered to do a subset of that kind of work. And we talked a bit about this on the ops team call on Monday that our situation is actually the simplest; we have a nice clear charter. We're just going to keep going.

And the nice thing is that we seem to be doing work that people approve of. We got lots of feedback that what we've done so far is good stuff; please keep doing it so we will.

And as the other groups either finish the SSRRT or get up to speed as the Board group does we'll certainly share what we're doing and do everything we can to help those other groups get their job done. But in terms of where we're at we're fine. And so we're just going to keep going.

On the other hand as the other groups produce stuff we're going to steal everything that they produce if it bears on our work. And so I think that there is opportunities to do a lot of good collaborating and maybe get this stuff done faster; that would be great.

So any thoughts or comments about all of this stuff before we move onto the next chunk of the agenda? Okay.

Next on the list - I'm going to switch us over to another view of my screen so there will be a short period of mumbling in Cheryl's honor while I do that.

((Crosstalk))

Cheryl Langdon-Orr: ...to insert appropriately.

Mikey O'Connor: Yes, thank you, Cheryl. I have to figure out how to do this again. Okay. What you see on your screen and what I will see on my screen in a moment is the first draft of a spreadsheet that I've developed.

During the meltdown of our main meeting in Dakar on Thursday around lunch time Jörg did a brilliant save where as the meeting crashed and burned he said why don't we pass around the one pager and let people indicate their priority preference, which I have to acknowledge Jörg's brilliant idea.

But one of the things that I want to do is get a more detailed and complete view of that set of priorities from the working group. And so I've built a little spreadsheet. I'm going to show you one of two; there's a comparable one for vulnerabilities but it's the same idea.

In which if this passes the sort of reality test with you all I will write up instructions and send this to the list. One technique when ranking things is called forced pairwise comparison ranking or basically in simpler terms you take every option on your list and you compare it with every other option on your list and you decide which of the two is more important to you. That's the forcing.

You can only choose one; you cannot say these are equally important. So sometimes it's easy and sometimes it's difficult. But by making the choices in pairs, only two at a time, it changes the way people think about things. And the thought that I am thinking here is that we're not quite done with our development of the list of threats and vulnerabilities but we're close enough that it would be good to begin to get a sense of which the most important ones are so that we can maybe focus in on where to start.

And the process that I'm proposing but I'm more than interested in your reactions to is that what we would do is essentially spend next week each of us filling out a copy of this hopefully by and getting them back to the list by Tuesday of next week or maybe Wednesday so that I can summarize the results.

And the thought is that what we're going to find is that there will be areas where there's a lot of agreement; people will say oh yes this is extremely important or this is extremely unimportant or it's in the middle but we all feel the same way.

And then there will be others where there is substantial disagreement; some people feel something is very important and others think it's not important at all.

And then what we would do is start taking a look at that on the next call and essentially quickly disposing of the ones where we all agree it's either important or not.

And have a conversation about the ones that we have differing views so that we can understand why those views differ and maybe arrive at a better consensus view.

So let me walk you very quickly through the mechanics of this thing so that you can see how it works. And then I'm very interested in your reactions. Nathalie, can you jump down and let folks into the room because I'm pretty distracted with...

Nathalie Peregrine: Sure.

Mikey O'Connor: ...doing this. Thanks. So if you look in this first cell the choice that you would be making is which is more important to you as a threat, system failure, for example hardware or software failures and so on, or governmental interventions, for example seizure, blocking and so forth.

That's the choice for that cell. And the cell will only allow you to choose, Number 1, which is the system failure one, or, Number 2, governmental intervention. So if you try and type anything but 1 or 2 into the cell it's going to complain about it. So I'll put Number 1 in there just arbitrarily.

And the job of folks, you know, for all of us is to go through all these cells and make all these choices. And you'll see that you can scroll this around so that you can, you know, if you're working on this cell you can bring it close to the edge so that you can see where you are and so on and so forth.

But once you've completed this work then you can go to the next tab and you can look at the ranking that's been tallied from your results. Right now there's only one done so as a result my work so far has ranked system failure as my Number 1 priority. And when I get done then I will be able to take a look at my list and maybe modify it before I save it and send it along.

And then what I, Mikey, can do at the end is take this column that's got all these rankings in it and smash them into a single spreadsheet and do, you know, the usual statistical analysis what's the mean, median and standard deviation and get a sense of where we agree and where we have differing views and get that back to the group before the call next week. And then we'll pick up the conversation based on what we've learned.

So this is another whacky Mikey idea. And I ran it by the ops team and they - nobody objected violently to this. So I thought I'd try it out on you all today and if it feels like a good thing for you all then I will go ahead and write fairly detailed instructions to go with this spreadsheet and mail it to the list.

Cheryl, go ahead.

Cheryl Langdon-Orr: Thank you, Mikey. Cheryl Langdon-Orr for the transcript record. I'm more than happy to go through this particular exercise, Mikey, but it does help us sift and sort the middle issues from the outliers and the outliers are always the easiest to establish; those that everyone vehemently agrees with and which vehemently disagree with.

And it's the latter part that's going to get exciting, you know, deliberations later. So, yes, I think this is a good first filter and be happy to do it. I would be keen for us to recognize it - especially if we do it and I'm happy to do it in something like a weekly format where at least the results of this will be sort of public at some point.

I think we need to be careful that this is seen as an exercise as opposed to ironclad output or consensus agreement on anything because we will always get this huge gray area in the middle which is always going to be a subject to a debate. And I think as long as we use these tools for whatever is (suit) for purpose I think they're great.

I've done an awful lot of risk management in some areas which some people would think are fairly important, i.e. life and death of other humans. And there always gets to be a point of sometimes risks which appear unacceptable in certain circumstances are acceptable in others.

And that of course is the classic triage decision; the difference between a well appointed and normal situation where all facilities and requirements are running in the norm versus those in a disaster. And very different decisions and risks acceptability's outcomes are made in those two very different scenarios.

So as long as we keep the scenario outlined really clear so no one misinterprets the results of these activities out of context I'm comfortable. Now that's a huge rider but I think it's a really important one.

Mikey O'Connor: What if I put - because, you know, presumably these spreadsheets would be flying about on our publicly accessible email list. What if I put a disclaimer on the bottom or the top or somewhere prominent on each page of this spreadsheet that made it clear the context that this is being done in; that this is a preliminary assessment of views.

It's not to be considered by any means a final decision of the working group; it's simply a mechanism by which we are identifying areas of agreement and disagreement.

Cheryl Langdon-Orr: And if you get the word perspective in there that would be brilliant. Thank you.

Mikey O'Connor: Thanks Cheryl. That is really a huge help. I'll listen to the transcript of the call and pull that out and get that on there. Now I think the perspective issue that you raised - I'm going to put Patrick a little bit on the spot. And, Patrick, you know where I'm headed with this so I'll fill for just a minute with some conversation while you frame your reply.

But one of the things that's going on that I think is going to be hugely helpful to us especially in the Board level committee but also in the SSR Review Team is the development of a notion called the threat landscape.

And your point, Cheryl, about triage and the circumstance I think fits right into that because...

((Crosstalk))

Mikey O'Connor: ...you know, there are more dimensions to this puzzle than simply the threats and vulnerabilities. And with that I'm going to throw the ball to Patrick to speak to the extent that he can.

One of the difficulties that Patrick has got of course is that he knows about stuff that he doesn't have permission to share with us yet. And so as a result I'm going to limit my conversation on this and let him take it from here. Patrick, over to you.

Patrick Jones: Yes, thanks, Mikey. So Patrick Jones from staff again. In the Board Risk Committee meeting in Dakar, which is a separate committee from this new Board-level working group that was formed in the Dakar meeting, we worked through a new - a different view of the ICANN risk landscape.

And this is from a perspective of risk to the organization not DNS risks at the broad level that the DSSA is - has been focusing its efforts. But there is general agreement from those on the Board Risk Committee that the

document should be shared more broadly with the community sooner rather than later.

So I'm working on making that happen soon and so that this group and others can benefit from at least the initial thinking. And I'm not saying it's perfect but it's at least a look at the ICANN functions, a taxonomy of threats in a basic way with an added dimension of severity of impact and timeliness.

And it's sort of a four-dimensional view; it's going to take a high level. It's not going to drill down into line by line details at least not in the version that would be made public. But if that's something that's beneficial and people are interested in it I'm trying to accelerate the release of those materials so that it can be open and transparent.

Mikey O'Connor: Perfect. Now to Cheryl's point it seems to me, Cheryl, that we'll wind up doing is we'll probably go through this exercise several times because I think what we're going to discover as we do this first pass of ranking is we're going to find some holes in our own analysis that we'll identify.

And then as this other stuff comes out we're going to go oh that's good stuff; we need to add that as well. And so I think we're going to wind up iterating towards a final ranking. But I think the reason to do it soon is because while we finish up our lists of threats and vulnerabilities we're also going to want to start doing some analysis of one.

And by picking one well we can get going on the analysis while we wrap up the listing. And in so doing we get to do some stuff in parallel. So that's sort of the context of all this.

Now I see your hand up again; is that the old one or is that a new one? You want to go ahead and respond?

Cheryl Langdon-Orr: Yes that's a new one, Mikey.

Mikey O'Connor: Okay.

Cheryl Langdon-Orr: Thanks Mikey. Cheryl for the transcript record again. I like the way this is heading; I just think we need to recognize that we may need to use a number of sources like any good process and analysis should to get us to our final end game.

And I'm not sure that we've even established what our final end game is meant to be in terms of the analysis and outputs. There is going to be a set of, in my totally biased view, what I would refer to as critical control points, in other words, points of potential failure which may or may not need to be managed differently.

And that's where there'll be a need to look at the risk landscape specific to each one of those. We're not there yet but doing this type of exercise will help us get to there.

And there are always, I guess, going to be probably more things in the footnotes and the disclaimers than there are on the pretty little diagram in the middle of the page. But then again that's okay as well.

Mikey O'Connor: Well and that last point that you made, Cheryl, I think segues - provides us a transition into the next agenda item really gracefully which is the question of how shall we do this analysis that's coming up.

So I sort of want to hold that last point that you made, Cheryl, and just check with the rest of the group to see if there's anybody that feels that this idea of sending out this spreadsheet is a bad one.

If everybody else is okay with this I'll go ahead and get this underway and then we can talk about the approach and methods that we're going to use on

this analysis for the rest of the call so just a quick stopping point to see if anybody else is uncomfortable with where this is going. Okay.

I'm going to mumble some more for Cheryl while I change to yet another document. But I think this time I've already loaded it.

Cheryl Langdon-Orr: Mikey, Cheryl here. You just used a word that we probably need to put in our glossary and our vernacular and that is loading.

((Crosstalk))

Mikey O'Connor: Yes, loading. Yes. Not to be confused with loaded wording for anything like that. Okay what's on your screen is a giant long document that I am not letting you navigate.

But as we had the conversations in Dakar it dawned on me that if indeed what we are about, if we the DSSA are really doing the subset of a risk management process, which seems to be what's going on, then others have developed methods to do this that we don't have to invent this all.

And we in fact have a choice to make. And I'm throwing this one up on the screen because I - this is the first one I found with a Google search of the term risk management methodology.

This is by far - this should not be considered anything but an example. And we began this conversation on the ops call. But it quickly became clear that this is something that we should take up with the whole group which is what method should we use to do the analysis that's coming up?

And that's back to the point that Cheryl just made which is Cheryl, you were clearly - when you made that point about critical control points...

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: There was clearly a methodology there that that idea came from.

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: And I'm very interested - and we the leadership group - are really interested in identifying possible options for methodologies. The one that we focused in a bit on the leadership call was the ISO 27 series, the 27001, 2, 3, 4 series of standards.

And so at least right now that's kind of the front runner. But, you know, if other people have ideas about good risk management methodologies that are out there that we should be looking at and trying to decide what to use I think this is a good time to start that conversation.

And I see that Diego has got his hand up. Diego, go ahead. Oh you're only on Adobe. I don't know - we could try something really weird which is up on the top of the Adobe screen there is a button - no, never mind. I'm looking at it and I don't think - I was going to say Adobe can take audio from your computer, Diego, but I think it would not work.

Cheryl Langdon-Orr: Yes, it works it's just got to be set up the right way and it doesn't - sorry, Cheryl for the transcript record - it doesn't appear that it is set up the right way. Nathalie, perhaps you should talk to Gabby or Kristina from ccNSO world because we're running the Framework of Interpretation Workgroup now in that methodology.

And what it means is that there will be a microphone next to each of our (said) participants when it is set up that way. But it could be quite useful for this workgroup to have that option. And it means then that people, if they're using their Apple iPads or whatever don't even - and have a decent Internet connection they don't have to make an audio bridge connected or - and it's been quite satisfactory.

((Crosstalk))

Mikey O'Connor: Okay, Nathalie, I'm going to throw that one to you to explore. And I'll cheerfully help with that if you want some help.

Nathalie Peregrine: Oh I don't think there'll be a problem.

Mikey O'Connor: Thanks. I think that would be useful because we do have a fair proportion of our callers that are coming in only through Adobe and I think that would be a really helpful thing.

So, Diego, I'm going to sort of leave you - oh so, Diego posted to the chat a risk assessment matrix. Can you, Diego, if you can find a Web URL or a link that points to the - to that methodology? Cheryl has gone one in there. Actually Don is talking about other possibilities - it's Don Blumenthal in the chat.

Any of you, Rick Wilhelm is got one.

Rick Wilhelm: That one was yours.

((Crosstalk))

Mikey O'Connor: Oh that was mine. Oh okay that's the link to the one that's on the screen. Thanks. I think that one of the interesting puzzles that we inherited and I didn't realize it until Dakar is this methodology choice. And I'm quite delighted to take a small process detour because I think that the choice of the method by which we analyze the risks and vulnerabilities is quite important.

And I don't want to just arbitrarily either pick one or just start using one. I think that the framework by which we make these analyses is actually substantive part of what we are doing.

So if people could send along examples I'll start building another one of these mine maps of the options and we can start setting aside a little bit of time maybe on the list but also on the calls to talk about the merits, pros and cons, of each of these to see if there's one that we feel works the best for what we're chartered to do.

And so I encourage all of you to think about this and send us links. One of the things that is a little puzzling about the ISO standards, the ISO 27 series standards is that they cost money and have licenses associated with them.

And that is a little complicated given the sort of open transparent nature of what we're doing because we might splash a lot of proprietary licensed information around on our publicly assessable email list and that could cause us some trouble. So I'm interested in navigating all of this in a way that we can move pretty quickly but at the same time not run afoul of proprietary licensing rights.

So I'm seeing a lot of good stuff coming in the chat. Thank for those links. Diego has got one in Wikipedia that's pointing to his risk matrix - a picture. Cheryl has got another one. So this is super; please keep going on this in the chat.

And what I'm sensing is that my intuition is correct which is that there is an interest in the group in having a conversation - a process conversation before we just dive into the analysis itself. And so let's keep going on that.

And I'll leave that on the agenda for a week or so and I'll take the links out of the chat plus anything else that anybody thinks of that they want to send to the list and I'll start building a matrix of - or another one of these mine maps of our choices and see if we can get that moved forward.

Anybody got any comments about this other than my long ramble about it?
We on the right track here? I think we are.

Cheryl Langdon-Orr: Mikey, Cheryl here.

Mikey O'Connor: Yes, go ahead, Cheryl.

Cheryl Langdon-Orr: Sorry I didn't get my hand up in time.

Mikey O'Connor: No worries.

Cheryl Langdon-Orr: Cheryl for the transcript record. This is one of those grab bag of really useful tools and links to really interesting points for us to look at, mull over and come back and discuss later that I'd like to see aggregated into one of the publicly accessible wiki spaces.

It appears to me that putting together a selection of resources worthy of at least looking at, which is going to probably be analysis of what other bodies have done. I mean, obviously here Standards of Australia have done something resulting in the A and Zed and IST have done other things.

There's going to be a reasonable amount of overlap. But I think there could be advantage of anything we find from our own group as being emeritus to be put somewhere but also to allow comments to come in from others outside of our own somewhat limited group, despite our size, just in case there's a gem we haven't picked up on. I just think a bit of crowd sourcing might be useful here.

Then we get to pick and choose obviously. But I'd had to think that there was some, you know, incredibly useful system that we could use specific to our DNS issues that we just haven't tripped over because we're living in our fallows.

Mikey O'Connor: Yes, that's very well put and aligns perfectly with where I'm coming from. And so my habit with these mine maps is that I - when I create a whole new topic, which is what I'm thinking I'll do with this methodology discussion, I create another page on the wiki and then start posting the drafts of these as we develop them.

And I think that your idea of doing a little crowd sourcing around this especially I think, you know, for those of you who are part of the security community, you know, to identify the options in terms of methods for analysis and gain insights is - like Cheryl said, it would be a shame to come back in a year and discover that there was one that we missed just because we were too limited in our reach or our imaging.

So I think this is feeling pretty much where - I had this intuition and it sounds like it was a good one so we'll keep work on this. And I think at the same time what we'll probably do is - I'm anxious that we not get totally stuck in process. So I think what we might do is sort of a quick rough look across a number of these and come up with some early steps for the analysis process and get started on that even before we've finished choosing.

Because, you know, I am still really anxious to get us going on, you know, the analysis. So I think we'll do sort of a lot of stuff in parallel. We'll do picking in parallel. We'll do the method stuff in parallel. But we'll, at the same time, keep striving to get going on the analysis of at least one of these topics.

Because I think we're going to uncover other things that we're going to need to fix as we get started on an analysis like this. And so that's kind of where we're at.

I think that's about it. It's three minutes until the top of the hour. Anybody got any other thoughts either about this or anything else? Okay I think then we'll call it a day. Thanks all and I'll see you all in a week. Bye-bye.

Cheryl Langdon-Orr: Bye. Thanks.

Patrick Jones: Thanks, Mikey. See you.

Nathalie Peregrine: Thank you, (Bart).

Rick Wilhelm: Thanks Mikey.

((Crosstalk))

Nathalie Peregrine: ...the recordings.

Mikey O'Connor: Thanks, Nathalie. I think...

END