Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
12 April 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 12 April 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-20120412-en.mp3

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
. Jacques Latour, .ca (CIRA)
. Jörg Schweiger, .de (co-chair)
. Katrina Sataki, .lv
. Takayasu Matsuura, .jp

NRO Members
. Mark Kosters (ARIN); (co-chair)

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

SSAC Members
. Jim Galvin (SSAC)
. Warren Kumari (SSAC)

Experts
. Scott Algeier

ICANN Staff:
Julie Hedlund
Nathalie Peregrine

Apologies:
Rafik Dammak – (NCSG)
Don Blumenthal – (RySG)
George Asare-Sakyi - (NCSG)
Luis Diego Espinoza,.cr
Bart Boswinkel

Coordinator: We're now recording.

Nathalie Peregrine: Thank you (Ricardo). Good morning good afternoon good evening. This is the DESA call on the 12th of April 2012.

On the call today we have Mikey O'Connor, (Warren Komali), Joerg Schweiger, Cheryl Langdon-Orr, Andre Thompson, Olivier Crepin-LeBlond, Jacque Latour, Rosella Mattioli, (Tatias Matul), (Scott Andreas), (Julie Hammas), Jim Galvin and Mark Kosters.

From staff we have Patrick Jones, Julie Hedlund and myself Nathalie Peregrine.

We have apologies from Rafik Dammak, Luis Espinoza, Don Blumenthal, George Asare Sakyi and Bart Boswinkel.

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 welcome all, the final description of what's on the screen. This is my neighbor's kitchen counter where she has three eggs that stand on end.

We had a lively discussion about why this happens and how we could test it before the call started. So for those of you who are reading the chat transcript that's what's going on.

We'll take a moment to see if there are any updates to people's statements of interest?

Okay really only two things on the agenda today. I want to take you very quickly through the report outline to give you a sense of at least the first pass and elicit shrieks of outrage if there's something really wrong and this is a good time to find it.

And then we've got a handful of threat scenarios that have come back. One from Rosella, one from Joerg, and one - and three from me that we can use to sort of stress test the compound sentence risk scenarios spreadsheet. We found some things that I will try and drive into the next version.

And then just talk a bit about sort of writing paragraphs about anything you like on the report outline at the end. And that's - that'll be it for today. I'm pretty sure that will be a pretty full agenda.

Is there anything that people want to bring up in addition to that on your minds?

Okay off we go. Here's the report outline. Oh boy that's small. Let me make that a little bigger.

Yes that's easier to read. I think I briefly walked us through this last time but I want to take a bit more time today.

I think I'm going to going to sort of go to the bottom of the hour on this and then at the 30 minute mark we'll switch over to the other stuff.

But I do really want to get reactions from folks. And in order to do that I'm going to drive down a bit into the outline and sort of give you a sense of where we're at.

There's really two big pieces. The one that I think everybody is really looking to us for are the findings.

And the findings are organized around our charter. And so there's the charter. And one of the things that we added before that was this definition of what we mean by the DNS?

And we had a pretty lively conversation about this during earlier parts of the working group. And so I just where there was work already done I've taken that work and just copy and pasted it into this report outlined.

And so one of the things that we did is we built a definition of the DNS that really focuses on the root zone, the TLD zones, and support files that go with those and said that's what we're talking about as the DNS.

And I also stapled in a memo that we talked a fair amount about pretty early in the working group they Greg Aaron wrote and I sort of took out the pithy bit there.

So one of the things that we'll want to hammer on is this definition. And one of the things that I think is nice about these definitions is that question came up in another context.

It came up in the SSRRT report and it also came up in the discussion of the board DNS risk committee.

So I think we've got a section of the report to write that a lot of people will be interested in. And it may be that it will have to get revised a bit but this is the definition that we're using right now.

So that's one big finding. And I put that in findings because I think it is a finding.

The big one, actual level of frequency severity of threats to the DNS plus current efforts and activities to mitigate these is a place for us to show off the methodology and start to define all of these things that we've got in that spreadsheet.

So for example we have our threat events that we've already worked on and I in some cases have tacked on some rhetorical questions.

Oh Cheryl I was going to use your version. Darn it. Well sorry, next time. Cheryl came back with a version of this that's got some commentary. And I spaced out that I was going to use that one. Sorry.

But, you know, we've got some puzzlers, you know, whether we want to add availability to the - or it's not availability it's confidentiality. We may want to talk about that or just leave it open.

And then in here we had a discussion especially in Costa Rica about, you know, the whole security. At one point we had security out at this level but we moved it down a level and put it in the incorrect category.

You probably need to finish that discussion because, you know, there's a pretty lively discussion to be had there.

But those are the threat events that were focusing on right now and that's the that's what will right in our report is the definitions around that.

Got it pretty big chunk of work already done on the - what the adverse impacts are that we'll want to write in paragraph form.

But I think we've got a pretty dense outline already there. I think, you know, I think we'll want to see this in paragraph form and then probably again edit it a bit. But I think this one's pretty close to ready in terms of being something that we can start to write.

And then we get into some of these are scales. And I think when we write the report we'll probably want to make scales subordinate to the things that they're scale of.

So for example I think rather than having likelihood of impact be a separate thing I think we'll probably want to pull that up in there. And in fact I think I'll do that right now so that I don't forget because, you know, I think the scales are important. And here's the scale that we've written so far.

But I don't think that they are so important that they should be way up at the top of the pyramid.

The ones that I think we have done less review of and let's work on start at vulnerabilities. In prior parts of the report we've done a lot of work on technical vulnerabilities.

We have the D DOS spam recursive data poisoning. These are words and phrases that came from our prior work.

And may we may want to expand these but I'm not sure that we're in terrible shape there. I think we've done a lot of work on those.

We have a fair amount to say and somebody in the technical community it would be lovely if you would start thinking about volunteering for writing some of these paragraphs because I think we do need paragraphs underneath these.

We've got sources for some of these that could be used to write those paragraphs but they're not really in paragraph forms yet. And so we could use some volunteer writers on that.

Ones that are less reviewed and less fleshed out are the managerial level vulnerabilities and the operational vulnerabilities.

And to clarify one of the methodologies makes the distinction between operational things are things that are done by people and technical things are things that are done by systems.

You may want to pull that up into this. It's going to show up in a minute in the controls but, you know, we may want to make a parallel there.

Some of these vulnerabilities come from other places. They come from the SSRRT report or in some cases I stole some things from the board risk committee, the board DNS risk committee.

And in those cases we may be able to lift paragraphs. But some of the others just come straight out of the methodology.

And there are - I will volunteer to write these paragraphs because there are paragraphs in the methodology already they we can use as a starting point. And I know where they are and so I'm comfortable taking on these paragraphs because I can plagiarize from somewhere else and that will give us something to edit from.

But I'm showing this to you because if there are things in here that drive you crazy and it would be good to start thinking about that and talking about it.

Not now. I want to take you through the whole outline before we do that but start thinking about things that are making you uncomfortable.

Predisposing conditions is straight out of the methodology. That's the - what the methodology has to stay to say. And again this is in the same hierarchy managerial operational and technical.

In some cases I've started adding things in here based on methodology. You know, a lot of these aren't from the methodology but are rather things that I've thought of that, you know, and they're written in such a way that they could either be positive or negative effects on risk.

So these paragraphs I will probably also volunteer to at least write a first draft of just because these are phrases that came for me.

But again if we have especially technical but technical and operational predisposing conditions that people want to either add or write paragraphs about that would be great.

The controls and mitigation part comes from a different methodology. And I think I mentioned this on the last call.

There's a companion methodology to the 800-30 that we're using. That's the - it's actually the 53 Series. But there's also a 37 and 39 series that I haven't actually taken a look at yet.

The ones - the one that I started really stealing from from the controls list, the 53 series. And that's where this - these lists that came that you saw in the spreadsheet came from.

And again these are easy ones to write first paragraph from because there's in each case they're in the methodology There's a paragraph that we can start from.

And so again I've got sort of a massive paragraph writing exercise in front of me that I am going to start now.

I've had three or four other projects finally wrap up so I've got some time to pivot back to this one and start drafting stuff for you to review based on this framework. And I have a lot more time available now.

So that's kind of the controls part. Then we have our old friends, the threat sources. And we've done a fair amount of work on these before.

This one is straight out of our work for example but it also turns out to be pretty closely paralleled in the methodology. And this one is in some cases out of the methodology but we've added a few like the root scaling stuff.

We probably have a debate about where some of these go whether they're adversarial or not. That'll be an interesting discussion.

It's right now in non-adversarial but some of the scenarios that I wrote are based on scenarios from other places like ISOC and kind of a gray line between adversarial and non-adversarial threats there. So we've got a discussion on that to have.

These are scales so I think these will get pulled into the respective chunk. And then overall thing is the sort of score at the bottom.

I think I stuck risk models in here. That's probably badly placed. I'll probably fix that in the next round.

Anyway that's the, you know, that's the findings stuff is or series of scenarios plus these chunks. And see what we want to do, add scenarios to these.

Got that now so I don't forget because I think the scenarios that we're working on now are a major finding and we want to get those pretty - actually pretty high on the list.

Then I think another big finding is this whole approach thing that we did. And this is a compound sentence model plus the - I started writing - this was written back in Costa Rica right after the meeting so my thinking has evolved a little bit.

So we're in the middle of doing that now. So I think what we'll maybe want to do is revise this a bit.

And then the gaps and additional activities I have just begun to sketch out material in these sections. So, you know, partly because I think we don't - we'll start to see the gaps come clearer as the risk scenarios evolve.

And we may also want to take a look at some of the other reports like the SSRT report and pull some of those things in here as well.

One of the evolving things, and again I think that our report in this iteration may have to be a little bit forward-looking sort of thing.

Now we're not going to talk a whole lot about risk mitigation at the technical level unless there is some really obvious one.

But we may be able to talk a little bit about the managerial and operational level especially given the fact that the SSRT has already kind of given us a springboard to talk about this.

And clearly one of the things that's coming through from everybody is the roles and responsibilities discussion.

And as we go through our risk scenarios we may want to keep an eye on that as well as the methodology that, you know, we're pioneering but lots of parts of the organization are thinking about the risk management framework. And we may want to comment on that a bit.

So that's the findings part. I think it's going to be a pretty substantial report actually. We've got a lot to say there and that I think people will find useful in the community.

Then I think we need also to document our approach what we did and why we did it and so on.

So we had a conversation about go fast then go deep. These are kind of notes to myself. There's a diagram that I'm going to steal next round of writing so it's a little cryptic but it makes sense to me that will describe sort of the difference between go fast which is what we're in now and go deep which is where we're headed.

I wrote another note to myself that said that we probably want to go back to our respective chartering organizations and check.

And so in order to do that I think we need to describe the next phase in some detail so that we can go back and check.

We need a better name than go fast than go deep. And maybe we'll put the eggs picture on the cover of that probability thing.

Then this part is sort of the documentation of what we did. This is the whole why we picked a methodology.

I think there's a lot of good work that's already been done. For those of you who have been with us for the whole run you've seen it in every update practically that we've done.

And we didn't just write that down in words. This is a list of the methods that we took a look at so this wasn't a choice that was made in a vacuum. You know, there really was some work that was done there.

And I think that it's important that we do this because I think that this is a big decision that we made and it needs - the way we made it and the reasons we made it need to be documented. And so this is a section of the report to do that.

And I'll take a whack at some of these paragraphs as well. I'm going to write a lot of paragraphs in this because so much of this is buried in notes that I took. It's easier for me to do it then it would be for you all to find the places that it's documented.

This is the risk model business and some notes to myself just sort of defining again these are paragraphs out of the methodology.

And I'm seeing some duplication here. This - by this time I've been in the cloud forest for a week. And my brain was turning into mush because I was having such a good time that some of this is a little repetitive. So I'm going to go through this, fix this.

I think another big piece that we need to put in this part the approach part, is this protocol for confidential information that we've been building.

Because we've got a very close to final draft of that that we need to tie up before we get to the report and then we can pretty much put that in this section of the report.

And then the - I think that this actually moves up into the findings because I think that we're making good enough progress on the risk scenarios that we'll be able to take these out of the test case and move them up into findings.

I think one of the questions that we need to answer in a preliminary way and then take back to our ACs and SOs is is the SSA going to do one more iteration?

Are we going to go do deep once or are we at the beginning of something that's an ongoing effort?

The reason this got into this outline is because if you read the, especially the SSRRT report carefully and take a look at the way that the DSSA group, the way we are referred to in that report they're a little bit ambiguous about whether we're a one-time thing which is the way we're chartered, or an ongoing thing.

And so I think we need to highlight that question and take it back to the group, the chartering organization for some review and commentary.

So then I think we need in our approach section to talk, you know, to talk about the next iteration in the work plan and stuff like that.

And a lot of this is coming out of - this is straight out of the methodology so no need to write much there.

But then this part is if we decide to do an ongoing organization we might want to start thinking about what that looks like. And so I started thinking about what something like that could look like.

This is something that you'll want to look at and ponder. We could propose that there is an ongoing thing that had this purpose which is essentially our purpose now plus some sort of ongoing community stuff that says, you know, is this ongoing thing that has a community of people within it that shares ideas and resources and then, you know, provides tools and models and best practices and all sorts of things?

This is a conversation that we may be able to use to resolve some of the dilemmas that plagued ICANN ever since its beginning which is the dilemma as to what is the authority of ICANN to do anything?

And one of the ways out of that is to say that the authority tends to be at the edge. And we started to get into this a little bit in Costa Rica.

And that the model building and resource sharing tends to be in the center but the authority to do things is at the edge.

So I do commend - I'm noticing that I'm at the bottom of the hour and I want to switch gears and go over to the risk scenarios for the rest of the call.

But I wanted to dig you down into this report outline enough to let you know that there's a fair amount of content buried in here already that you should ponder and react to.

I think I'll take just a minute or two to see if there are any sort of shrieks of outrage. But I don't want to spend a lot of time today on this. I do want to switch us back to the risk scenarios because I'd like to see if we could drive to getting a bunch of these in by the next call so any sort of cries of tremendous pain? Pull the whole thing up so that you can...

Okay I'm not seeing any hands shoot up so good. And as I say I think there are a lot of paragraphs that I will write just because I know where they are and I have models for them.

But if anybody would like to volunteer for some all ears, just pound your volunteering into the chat and we'll capture that.

Okay thanks to Rosella and Joerg we've got two risk scenarios besides the three that I created to look at so we really have five to take a look at today.

And started taking notes on things that I'll try to fix for the next iteration especially the problems that are created for people when you use OpenOffice, didn't realize that those drop downs didn't work in OpenOffice so I'll try and figure out a workaround for that.

(Warren Komali): Actually this is (Warren). If...

Mikey O'Connor: Yes?

(Warren Komali): ...people use Libre Office instead which is also free, the drop-downs seem to work okay.

Mikey O'Connor: Oh which office? What was that one?

(Warren Komali): I believe it works on all platforms L-I-B-R-E. Libre Office which I think is an offshoot of...

Mikey O'Connor: Okay. Well let's just pound that into the chat.

(Warren Komali): So it may only work on Macs but as far as I know it's free and it works fine with drop-downs.

Mikey O'Connor: Cool.

(Warren Komali): Don't mind me, I'll just randomly interrupt.

Mikey O'Connor: I love that unless everybody starts doing it then it'll get a little choppy. But I will take a look at the Libre Office and if it does work then I'll - and it is open source across all platforms that would be a great help because the drop-downs are really hopeful.

The other thing that Joerg pointed out is that the way the drop-downs work they don't make much of a distinction between the headings and the content in the tables. And that I can I think fix with some better labeling. So I'll drive that into the next one.

But let's just take a look at some of these. Those are pretty hard to read. Hang on a minute.

This is bigger. This is Joerg's. It's kind of readable. Let me go up one more notch which may make it...

Custom, there that's pretty close. That's about as good as it's going to get unless I cheat, cheat. There's the mumbling Cheryl. How about that?

All right, so Joerg wrote the D DOS attack on root servers risk scenario and sent it out to the list and his take was that rogue elements and that, you know, you can sort of read for yourself.

They're pretty capable. They've got pretty good intent and they're sort of in the moderate range on targeting.

This is the issue where that's a heading rather than a specific thing. And you have sort of an interesting debate.

It may be that the headings should stay in just so we can capture the whole category of technical vulnerabilities.

This, you know, got some ideas about the - this one here. I'll look at that. Anyway so I, you know, I think that it worked. Joerg do you want to share any observations about things that didn't go well for you when you were doing this that I should...

Joerg Schweiger: Yes.

Mikey O'Connor: ...Bring to the next round?

Joerg Schweiger: Yes sure could do that. Joerg for the transcript.

I think the one thing that spring into my mind has already been mentioned by you and that was the sub columns part.

Another thing that could be interesting for example when - could you please move up to the threat events column?

Mikey O'Connor: Threat event, yes.

Joerg Schweiger: Sorry, threat sources.

Mikey O'Connor: Threat sources yes.

Joerg Schweiger: So where we have rogue elements. I would have found it easy if I could just not only pick one but pick more because I think the assessments on capability intent targeting and vulnerabilities sense of force might not only fit just rogue elements, it might fit other threat sources as well.

So if we wouldn't want to end up with a whole like reams of papers of threats describing more or less or consisting of roughly the same information in the other columns it might be easy if we could not only pick one threat source but more than one.

So for example geopolitical groups might be more or less the same assessment with risk (tactical) capability and (ten) targeting and so forth but that was just an example.

Mikey O'Connor: So there's the way I would solve it is that because I fear of the - I think the easiest way to solve that in this particular context is to simply type the ones that you want to add into the box.

Joerg Schweiger: Yes fine with me.

Mikey O'Connor: And I think that, you know, and this is a really good point that you're raising and it's a - I like the idea of treating the drop-down list as sort of a starting point but that there is something that you can tailor so that if you find that, you

know, it's rogue elements and geopolitical groups and some and, you know, even put in examples if we want.

Because I think that the way to treat this framework at least on the left side is that this is something that we don't necessarily have to stay rigidly in these categories but rather use it as a way to document the scenario that we're trying to describe.

And it - and the other thing is that it's going to be really hard to build a spreadsheet that's not really confusing that allows, you know, multiple choice in there, you know.

So I kind of like it from a technical standpoint as well. Jacques you want to add onto this or have you got another point?

Joerg Schweiger: Yes. So for the (unintelligible) and the main music and put the title in uppercase and then start the individual like them or like dash, dash and then whatever...

Mikey O'Connor: Yes.

Joerg Schweiger: ...where you can make a distinction between...

Mikey O'Connor: Yes I - that is precisely the way I was thinking about doing it is that I would change the table just so - so for example what Jacques is I'm going to switch over to a different - one of the things that's interesting of about Joerg's is that it lost all of the drop-down menus altogether.

And so if I go to this - this is the template where I'm fixing things. And I went like this and put dashes in front of each one that - sorry, one example.

Then if we go back to our gizmo drop-down menu now makes it painfully clear that something's not right.

Never mind anyway I know what you're talking about Jacques. I'll fix it but I won't do it on the call.

Okay other thoughts?

Now one of the things that I was curious about is -- and I'll test this out on Joerg and Rosella -- is whether since Joerg you did the very first D DOS attack one whether you would like to be the editor-in-chief of that scenario until it's gotten to consensus?

So essentially start to split up the scenario editing job so that I'm not editing all the scenarios. And I was curious if you would be - if you and Rosella would be game for doing that?

Is that something I could foist off on you guys as work to do or would you prefer not to be an ongoing editor of the scenario that you created? Thoughts about that?

Joerg Schweiger: Oh I can give it a try.

Mikey O'Connor: I notice that you have a cold today.

Rosella Mattioli: The telephone's (healthy) but yes.

Mikey O'Connor: Rosella are you...

Rosella Mattioli: Yes.

Mikey O'Connor: ...okay with that too?

Rosella Mattioli: I'm in. Yes.

Mikey O'Connor: Wow. It's interesting.

Jacques Latour: Jacques here.

Mikey O'Connor: Yes Jacques go ahead.

Jacques Latour: I'd like to - can we go through the predisposing condition in the scenario because I'm still having issues around that?

Mikey O'Connor: Sure let's see this is - we're back to Joerg's and get these all on the screen. So the predisposing conditions that positively impact risk, let me get those up to the top, are the resiliency and redundancy ones which Joerg has very high.

So that means it reduces risk a lot because implication is that it is very - that it's applicable very broadly.

And the diverse distributed system architecture and deployment which is a moderate reduction of risk because many of the organizations that provide the DNS have that. So take it away Jacques. Do you have a comment about those that you wanted to add?

Jacques Latour: Oh just but they could get it now.

Mikey O'Connor: Yes I mean I what I did is I split it into two piles of predisposing conditions. The ones that are - that reduce risks and the ones that increase risk and maybe even positively impact it.

I'm actually going to put that as a note in my little - not that way.

(Warren Komali): And this is (Warren). I've got a question once we're done.

Mikey O'Connor: Sure. Hang on just a minute.

Dang it. Okay (Warren) go ahead.

(Warren Komali): So I still don't entirely understand what we do with the - that would result in adverse impacts. Because it - we say we presume that all would happen but in many cases that's not necessarily true.

Like identity theft doesn't happen if the zone doesn't resolve partly or something like that or, you know, if the zone has - is unavailable.

And then also the numbers on the side of that I still don't get so...

Mikey O'Connor: Yes we...

(Warren Komali): ...And I'm...

Mikey O'Connor: This is left over from the prior conversation. I think this might have been - it may be that we want to revisit this now.

But what we basically said in the lead up to Costa Rica was that we were really struggling with an exploding permutations tree.

And so we solved the permutations problem by saying we really only have a couple of threat events. The zone is either not available or it is incorrect.

And then we took the adverse impacts right out of the methodology and we probably need to revise that into two, at least two versions, one being the version for when the zone's not available and one being the version when the...

(Warren Komali): Okay.

Mikey O'Connor: ...zone is an accurate. That's a good catch (Warren).

(Warren Komali): Yes I think they should be able to be grouped nicely like that...

Mikey O'Connor: Yes.

(Warren Komali): ...hopefully.

Mikey O'Connor: Let me take a go at that.

(Warren Komali): And I guess while I'm holding the talking stick what are we supposed to do with these ones were sort of written in? Who do we ship them to?

Mikey O'Connor: I would - another good catch. Hold that one while I type...

I was going to mention that to the whole group. And that is that - let me show you something else that I did and see if this makes sense to you.

(Warren Komali): I mean I wrote two of them last night but thought that they were kind of crappy and was embarrassed so I just mailed them to you a minute or two ago, waste everyone's time with the whole (unintelligible).

Mikey O'Connor: With me as your co-chair you're worried about crappy or embarrassing stuff.

(Warren Komali): Oh you haven't seen them yet? Hold your judgment until you...

Mikey O'Connor: Okay I just want to point out the low standard that I set. So here's what I did on our wiki.

(Warren Komali): Oh a wiki.

Mikey O'Connor: A wiki, yes. This is our little DSSA wiki. And I built a little section which is probably a little too hard to read (unintelligible). That's better.

What I was thinking is that we probably want to take this through stages. So I'm holding the pen on the template. And I've got a list of to-dos for Version 5.

And I think the next stage is the ones that you all are submitting. And unless it drives you crazy what I'd like to do is post them to the wiki.

And the only drawback to that is then the whole world gets to see them which heightens, it makes the embarrassment factor even worse.

But I think the nice thing about that is that then what we have is a big, at the beginning we have a big pile of risk scenarios that are essentially individual efforts that are being continuously refined by the working group.

And the individuals would sort of remain the editors until they graduate at which point they move into this pile where the risk scenario is one that's been hammered on enough by the working group that we're all in agreement that it's at least close enough that we can all support it.

And then I'm going to also start building a worksheet that summarizes these so that we can see all the risk scenarios on one page.

And essentially doing that we get to start comparing scores and ironing out some of the inconsistencies between them.

And my thought was that I would start doing that with our individual ones. And simply, you know, change their status in that worksheet.

So what that implies is that a couple of things. These sort of go through stages. And in the earliest stage you're sort of accountable for your own crappy work.

But I think that I would find it hard to imagine a bad job of a risk scenario. So I'm wondering if having the spotlight shined on you that brightly is going to - I

would worry if this spotlight is going to make you not you collectively but especially you (Warren) not want to submit a risk scenario because you're embarrassed. I wouldn't want to do that. I don't want to make it uncomfortable or an unsafe place for you.

(Warren Komali): Oh no, no I'm perfectly fine having three things posted with my name on them. I just wanted to make sure I wasn't going to be wasting other people's time by sending (them) something.

Mikey O'Connor: I don't think so.

(Warren Komali): Okay.

Mikey O'Connor: You know...

(Warren Komali): My first one's probably acceptable to post. My second one turned into more of a joke because I - it was (unintelligible).

((Crosstalk))

Mikey O'Connor: I think maybe a couple of joke ones in here wouldn't be such a bad idea you know?

(Warren Komali): Great.

Mikey O'Connor: We working groups all tend to take ourselves awfully seriously. And sometimes the occasional, you know, we could have eggs on the cover and a couple of joke scenarios that we'd leave it up to the reader to figure out which ones were the jokes and that might not be a bad thing.

How do other people feel about that structure that I'm describing? Are you all okay pushing your risk scenarios right out into the light of day or would you rather not?

Cheryl's okay. She's in with a checkmark. I think it's - and so then to save - I then debate whether to post these to the list and then I scrape them off the list and post them to the wiki. Or if you want you could send them to me and then I can post them to the wiki and send a link to the list.

And I thought that given that some of us are on limited bandwidth at times, you know, all of us have limited bandwidth at some time.

But it might be better if you sent me the risk scenarios and then I'll post them to the wiki and send links to the list.

Mark is that a checkmark on that idea or is that a checkmark on the previous one? Of course you can't speak. Oh you can type previous, okay.

Rosella go ahead. Oh you may be muted. maybe that there was a lot of line. Nathalie did Rosella's line get muted during that...

Rosella Mattioli: (Unintelligible).

Mikey O'Connor: Oh there she is, Okay never mind.

Rosella Mattioli: Can you hear me now?

Mikey O'Connor: Yes. Now I can hear you.

Rosella Mattioli: Oh yes Rosella for the transcript. Yes I just want to pointed out as Jacques was saying on the chat that maybe some scenarios should not go public.

Because we are talking about vulnerabilities and okay we don't have the same scenarios like there was a scenario but yes somebody could read it.

So maybe we should create like (access) only DSSA members part of the wiki.

Mikey O'Connor: That is a really interesting question. For those of you who maybe didn't hear Rosella because she - her line is not too loud Jacques raised in the chat maybe some scenarios should not go public.

And Jacques I might circle back to you and Rosella and say is there a way to write this scenario so that it could go public for this phase and then indicate that the deep analysis of the scenario might require confidential information so that we could capture the idea in very broad strokes and then indicate that this particular scenario may require a nonpublic part of its analysis?

You got any thoughts on that one Jacques because you're thinking - I bet you're thinking...

Jacques Latour: Well.

Mikey O'Connor: ...of the scenario and I'm just wondering if you think about that particular scenario could you cast it in a way they could be public at this phase?

Jacques Latour: You have to summarize the scenario at a high level. And you kind of dilute the value, the exercise to some level, right?

So I'm planning to have a team meeting later on today with all my DNS people to figure out all the worst-case scenario here.

And they're going to be pretty detailed so I'm not sure I want to put that out. Rosella something we've got to figure out.

Mikey O'Connor: I think that the for this phase at least for a first try I'm not terribly committed to this and it would certainly be easy to keep some scenarios out of the public eye, you know, from a technical and project standpoint.

But I'm sort of in - I would rather have all the scenarios be out there in public and an indication that some of these we may have to assess in a different way in the future.

So this is a perfect opportunity Jacques when you do your meeting this afternoon see which scenarios fall out and then maybe as part of that meeting see if there's a way to describe that scenario that could be made public.

And if there is, you know, if there is no way to describe it that tells us a lot and may get to exercise our confidential information model a little sooner than I was thinking.

So let's let you be the test case on that and see what you learn. And why don't you kind of give us a report either via the list or if not via the list certainly next call as to how that came out because I think it's really important to understand and learn.

And then if it turns out that there’s some scenarios that simply cannot be revealed that's fine. We can certainly operationally accommodate those.

It'll be interesting to see how that turns out. Is that a reasonable course forward for you Jacques?

Oh it's 9 o'clock.

Jacques Latour: Yes.

((Crosstalk))

Jacques Latour: I'll try to summarize.

Mikey O'Connor: Okay I just realized it's the top of the hour and we're losing people. Dang, guess that's - I guess that's going to be it. I do try to stay within hour. So that's it.

Talk about an ungraceful end to a meeting. I'm really sorry, but there you go.

Anyway carry-on and we'll - I'll put some stuff out to the list. And thanks for being here. And Nathalie I think we can wrap up the recording and call it a day.

Nathalie Peregrine: Okay thank you. We will now conclude the recordings. Thank you.

Man: Okay thanks Mike.

END