Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
05 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 05 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-20120406-en.mp3
Presentation will be posted shortly on:
http://gnso.icann.org/calendar/#apr

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)
. Rick Koeller, .ca (CIRA)
. Wim Degezelle, CENTR
. Luis Diego Espinoza,.cr
. Katrina Sataki, .lv
. Takayasu Matsuura, .jp

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

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

SSAC Members

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

Experts

ICANN Staff:
Julie Hedlund
Glen de St Géry
Bart Boswinkel
Nathalie Peregrine

Apologies:
Rafik Dammak – (NCSG)
Don Blumenthal – (RySG)

Coordinator: Thank you. The recordings have started. Please go ahead.

Nathalie Peregrine: Thank you very much, (Sam). Good morning, good afternoon, good evening. This is the DSSA call on the 5th of April, 2012. On the call today we have Mikey O'Connor, Warren Kumari, Cheryl Langdon-Orr, Andre Thompson, George Asare Sakyi, Jim Galvin, Olivier Crépin-LeBlond, Takayasu Matsuura, Jacques Latour, Rick Koeller, Julie Hammer, Jörg Schweiger and Katrina Sataki. And Rosella Mattioli has just joined on the Adobe.

From staff we have Bart Boswinkel, Julie Hedlund and myself, Nathalie Peregrine. And we have apologies from Don Blumenthal and Rafik Dammak.

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 thanks all for joining. We'll take our traditional moment to see if anybody has a change, an update to their statement of interest that they want to share with us.

Okay I think I've done mine. Nathalie, have I done mine on this?

Cheryl Langdon-Orr: Yes you have.

Mikey O'Connor: Okay, well we don't need to go through that for the fifth time. Olivier, go ahead.

Olivier Crépin-LeBlond: Thank you, Mikey. It's Olivier here for the transcript record. Since we have a newcomer, Julie Hammer, who has not yet taken part in a GNSO working group or even cross community working group she will have to fill in a statement of interest. But this is just for the record that she will do that. Well I trust that she will do that.

Julie Hammer: Yeah, certainly I will.

Mikey O'Connor: Oh great. Well welcome to the gang, Julie. We also have Warren Kumari on the call who's from the SSAC. And he also has the opportunity to. Any others?

Warren Kumari: Hi, yeah, this is Warren. I will get to one of those soon.

Mikey O'Connor: Yeah, they're a delight, nice little - and, Nathalie, maybe you could send the link...

Cheryl Langdon-Orr: GNSO one will do...

Mikey O'Connor: ...gizmo to them so that they can use that to fill it out. Okay onto the agenda. There are really two things that - well there are three things. Two are sort of review introduction items. One is to the compound sentence gizmo that got sent to the list earlier this week and the other is to the very extreme ultra first draft of the report outline.

And then the last item which I'm going to just preview now so that you can be thinking about it during the call today is that this is sort of the time when I think we can sort of break into multiple parts and let folks go off and write first draft of parts of stuff.

And so as we go through this if the, you know, if some piece of this appeals to you as something that you'd like to write about or write an initial paragraph about I think the size of the writing effort that you should keep in your mind is a paragraph or two but not much more than that.

So if you see something that goes by that you want to write a paragraph about just sort of mentally note that. And then at the end maybe what we'll do is just let people pound their requests to write paragraphs into the chat so that we can sort of self-document what people volunteer for really quickly.

So with that sort of preview let's dive right into the first big piece of work that's the - what I call the compound sentence way of writing risk scenarios. I was completely enchanted with that idea when Rick brought it up at the meeting in Costa Rica. And so I developed this. But I have to do all the usual disclaimers which is that this is ultra, mega, super draft and can change in any way that people feel is appropriate.

But the thing that appeals to me about it is that it sort of smashes this giant complicated methodology down into one page which I think is really helpful for us and for people who are looking at what we're doing. So I just want to give you an extremely quick tour and then show you how flexible this is because it's something that we can clearly quite easily modify because it's a very simple spreadsheet; there's not really a lot going on here.

But what you see on the screen, hopefully big enough that you can read it, is the compound sentence where the way I think of this anyway is that we sort of read down this page and fill in the components of the risk scenario in the green spaces on the spreadsheet.

And so each green space - if you click on it you see just to the right a little pair of up and down arrows. And if you click those arrows you get the choices that we have at this moment in time. But again this is where the all-draft

statement comes in because, you know, these may change, we may add some, we may delete some, we may modify them. But this is where the choice can be made.

And one of the things that you may find is that a choice that you want to put into a green blank isn't there and that's fine, you can type anything you want in the blank. And, you know, unlike the last versions of these things the spreadsheet will not prohibit you from doing that - validation on these it's just - it's just providing you options.

And so I'm not sure that I want to take you through all of the slots because that could take quite a bit of time. But I want to show you sort of the connection between the slots and where those choices are made.

If you look down on the bottom what you see is a series of tabs. And let me go all the way to the left and start. I hope that the version of the spreadsheet that I sent you all starts with this page of instruction which I also hope is going to get better, a lot better by the time we publish it if we decide that this is something that's worthy of pursuit.

Then as you walk to the right the first tab is the one that I was showing you before. That's this adversarial risk scenario tab. And there is a matching one for non-adversarial risks. Oops, let me make that bigger so you can - because it turns out that in the methodology there are some changes between the way adversarial risks are handled and the way non-adversarial risks are handled.

And I'll show you. If you look at our - a non-adversarial threat source what you see is that they only have a range of effect, you know, and so it's the sort of thing that says if we had a non-adversarial threat let's say from an earthquake. And earthquakes have a range of effect. They probably don't affect all DNS providers.

Whereas if we go to an adversarial threat the way the methodology thinks of them is that adversarial threats have three things; they have capability, in other words they have some level of resources, expertise and opportunity. They also have a level of intent. And they have amount of targeting. So that's why there are two tabs is because the methodology really thinks about adversarial and non-adversarial risk scenarios differently.

And in the instructions I'm saying let's just document one risk scenario per spreadsheet. It's possible to document two but I think it's going to get really confusing if we do that. So even though you could document two risk scenarios with one spreadsheet I think you just pick whether to use the adversarial one or the non adversarial one and go ahead and just do one at a time.

Okay so then those are really the two tabs that you need to fill out. However let's continue walking to the right across the bottom of these tabs just for a minute so that you can see how the information is rolled forward to that front page.

Basically the rest of the tabs correspond to the rest of the tables in the methodology. And all these table names and table numbers like Table D3, adversary capability, and so on come from the NIST 800-30 methodology.

And in most cases I've very lightly edited them to reflect our circumstances. But I may not have edited them well or correctly so that's what I mean about this being a very draft document.

It seems to me that there are sort of three dimensions of draft-ness. One is that we need to start creating risk scenarios. Another is that we need to correct errors or omissions that I've made in this spreadsheet. And then the third is tailoring and refining the words that we're using.

You know, so for example this is the list of threat sources that we've - make that bigger - that we made up quite some time ago. You'll find that a lot of this starts to sound familiar and it's because I've pulled forward a lot of the work that we already did - previous mind maps and stapled it in here.

And so one of the things that's a sort of a writing opportunity is that we probably need a paragraph to describe each one of these so that, you know, we have a narrative that flows in the report in the section that's called threat sources. So if you want to start thinking about things you could write one of the things that you could write is a paragraph about any of these things.

There's one addition to this one and that's the very first one which I listed from the SSRT report. Which, by the way, the SSRT report was published the day that we met in Costa Rica. And the deadline for comments is Friday of this week.

So if any of you missed the publication of that and want to comment it's published on their page in the wiki. And we don't have a lot of time. I'm going to publish as an - or comment as an individual because there just isn't enough time to run comments back through you all for approval. But I found a bunch of things in that report that I thought were interesting and this was one of them so I stapled it in here.

So, you know, there's lots to talk about in each of these tabs. And I think the way to do this is to go ahead and try and build a risk scenario or two. Each of us should do this. Because I think as we build one we're going to find things that are broken here either in terms of our lists or in terms of the definitions or the actual model itself.

And so I would really encourage everybody to try and build at least one risk scenario between now and the next call and publish it to the list some time before the meeting with any comments that you've got because that'll be a huge resource for us to start modifying.

Just walking you the rest of the way through the tabs. This was D7, adversarial threat sources. This is D8, the exact same idea except non-adversarial. And you can see the different scale sitting out there, the range of effect scale.

In the methodology table E5 is the threat events. And what we've concluded in prior work is that we really only have two. But we also had a pretty lively discussion in Costa Rica about the DNS SEC. We had DNS SEC where security is compromised as its own - we started with three and we kind of collapsed two. But we also had a pretty lively discussion last week about whether that was really the right idea.

And then the thing that I added is that there may also be a confidentiality leg to this discussion. So we've got some work to do here. And I went ahead and put it in in its unfinished state but - work our way through this; we're not done on this one.

Then get into a pretty big table; the list of vulnerabilities. And this part of the list you're going to recognize because this part of the list came forward from the work that we did leading up to the - no the thing in Africa - bah, just lost the name of it...

Cheryl Langdon-Orr: Dakar.

Mikey O'Connor: Dakar, yeah, thanks Cheryl. And I stole something from the methodology which is these two chunks of vulnerabilities and stapled them in as well. This is another little departure that your spreadsheet builder just went ahead and did on his own. So this by no means approved or acceptable to the rest of you; this is just something I stapled in.

But I find this a very interesting list to think about. Again with the exception of one, which is this one, these - the rest of these are just straight out of the

methodology. And I thought they were pretty darn good so I stuck them in there.

But, you know, this is draft - draft, draft, draft so this all gets to be changed if you want. And as you go through building risk scenarios you may find things that are just very uncomfortable that we need to hear about and talk about. But again I think that the best way to learn that is to go ahead and try and use this tool to build some risk scenarios to see how well it works for us.

The next one is the same idea except that this is the predisposing conditions. And this is entirely my creation; this is not out of the methodology at all so this is really draft. And you really need to take a look at this.

And what I tried to do when I wrote these is write them in a non - in a way that they could either be advantages or disadvantages to the security environment.

So for example the legal standing and relative use of ICANN could be a bad thing or it could be a good thing in terms of the risk scenario that you're building. And so remind me to circle back to the front page and explain how I accommodate that on the front page.

But again all of these are mine and need to be vetted pretty carefully before we go ahead and publish this to the world except to the extent that we do it in drafts through the list.

And then this last one - oh no I guess there's two. This is from a different methodology. One of the things that you see when you look at vulnerabilities is that methodology - the 800-30 methodology has this tiny little line, vulnerabilities arising from missing or ineffective security controls - it's this tiny little thing.

But that tiny little thing is a trapdoor into a whole another methodology which is a companion to the 800-30 that's 800-59 I believe. I keep meaning to send a link to that to the group.

Anyway so I went to 800-59 and they have a whole taxonomy of controls. And those - there are actually two of them; there's one that's the list of controls, that's 800-59 and then there's 800-59(a) which is the audit document. That says if you're auditing yourself to see whether these controls are in place here's the way you do that.

The combined documents are 250 pages long. So on last week's call we were talking about the difference between going fast and going deep. And my comment was that there is no bottom to the going deep and this is why. It's amazing how deep we could go in terms of some of these views.

This list that's on this page here is the very top level of hierarchy in 800-59. And I just stapled them in. And one of the things that I want to do next iteration of this - and I'm just going to pound this in so that I don't forget - is that operational controls are generally things done by people; technical control - and this is another phrase out of the methodology that struck me and I just forgot to type it in here - these are things done by computers.

So access controls talk about, you know, the access gizmos in a computer program that allows people to log on and, you know, the matching of that stuff, who has access, what are the levels of security, etcetera whereas operational stuff is more human being oriented.

And then finally the adverse impacts page is the way we've handled this - this is one that we tentatively think is done. What we've said is that we're going to treat this as the worst case and these are the words that we use to describe that.

I added a concept that I liked out of the methodology that I haven't built into this spreadsheet yet in a good way. But it's the notion that for our analysis we'll treat this as a high-water idea where we'll essentially only look at the worst case; we will not look at those cases where the impacts are less than dire. And in fact we may want to use this high-water concept throughout and we can circle back to that too.

But then the list is just straight out of the methodology and is really just tended to remind us that the unavailability or lack of integrity and perhaps loss of confidentiality of the DNS is a pretty dire thing; it has a lot of effect.

So there's a very quick tour of the spreadsheet. And I'll head back and do one last thing. Remember how I said the predisposing conditions are written ambiguously?

Cheryl Langdon-Orr: Yeah, you need to take us back to the front.

Mikey O'Connor: Pardon me, Cheryl?

Cheryl Langdon-Orr: Yeah, you were going to take us back to the front page on that.

Mikey O'Connor: Yeah and so here we are. So let's take this legal standing ambiguous statement. It's got - we have to give it a score as to pervasiveness. Basically I think that - oh it doesn't wrap well, I'm sorry about that. I'll fix that the next time around.

But then what you get to do is choose the sign of it. So if this is a negative problem or issue - so this increases risk - then remind us of that by putting that choice in there. Okay this is a risk increaser.

If on the other hand - and let's take another one - this is one that came up - Jim Galvin came up with this. Talk about resiliency and redundancy in the

architecture. This actually reduces risk so let's just remind ourselves that this is positive; this is a good thing.

Then what that does is instead of adding a 10 to the multiplying that goes on in the far side it makes it 1/10th if it's really widespread. So that's my first try lame approach to handling ambiguous thing. And if that drives you crazy we can fix that too.

That - I apologize for the long rant. I want to stop and get reactions to this. I'm hoping that that's not stunned silence, oh my God there's no way I can use this but rather huzzah, great job, Mikey, let me go try it and see what I learn. That's...

Cheryl Langdon-Orr: Cheryl here, Mikey, because I don't want to have you in stunned silence.

Mikey O'Connor: Go ahead, Cheryl.

Cheryl Langdon-Orr: And you're right, I have found no way that I can put my hand up off the Android advice so there you go...

Mikey O'Connor: Yeah, I couldn't find one either.

Cheryl Langdon-Orr: Cheryl for the transcript record. Can I take you back to the high water approach?

Mikey O'Connor: Yeah, yeah.

Cheryl Langdon-Orr: Just wondering - and I'm not saying - I think, you know, that we need some sort of benched mark to try and make this (slightly) manageable both on the - I was going to say cheap and cheerful but it's neither of those things - the faster approach and the deeper dive approach.

I'm just a little bit unsure - and it might be that we just need to approach this introduction at this pass through our processes. But if we only look at high water, worst possible scenarios, is that doing justice to our mandate where what we're supposed to be doing is making some ascertainment of what are the actual threats not just what are the actual worst possible scenario threats.

Mikey O'Connor: Yeah. I get that. And I'm not that committed to this idea it was just something that appealed to me as I read it. So I'm going to start...

Cheryl Langdon-Orr: Well what I think - if I may, Mikey, Cheryl again in response to your - I'm not pushing back on it for this stage of our approach. I think it's a good management tool for this stage of our approach.

But we probably need to make it really, really clear that is at this stage of our management - of the project approach. Because to do too many layers simultaneously simply wouldn't get the work product out in a timely manner that the community needs.

Mikey O'Connor: Well and another way to handle this would be simply to write the scenarios this time around and not try to evaluate them at all. So for example - because I think just writing these...

((Crosstalk))

Cheryl Langdon-Orr: And socialize the scenarios or list the scenarios, sorry.

Mikey O'Connor: Well, you know, let's say that each of us came up with a scenario so we've got, I don't know, 20 people on the call. We come up with essentially 20 answers to this column. And we leave the evaluation of this column to the detailed phase. That's where folks who write compound sentences like Jacques may have something to say about this; not that his hand is up.

But, you know, one way to handle this high water mark thing is simply to say we're going to try to sort these scenarios into some sort of priority sequence and try to pick several of them to pursue in the next phase when we go deep and essentially sidestep the high water issue altogether. That's another option that we can pursue.

But I certainly agree that we need to make it clear. And I'm not even sure that - I mean, for example let's say we wrote a risk scenario - I'm going to just pick stuff at random - where rogue elements exploited a DDoS vulnerability with some predisposing conditions that there, you know, there was a positive one and a negative one. And they exploited an access control vulnerability and took down the root. I mean, please do not consider this anything but just random selection.

I mean, you could basically write a risk scenario with that column and not fill in this column at all for the first pass. And in fact it might be that we can't fill in this column because we need to go find out what their capability is. See where I'm going with that, Cheryl? Does that maybe make more sense than trying to confuse things with that high water idea at this stage of the game?

There is lots of puzzles here. I'm not saying that this is puzzle-free zone, that's for sure. So you can ponder that. Let me swing over to Jacques who's an experienced compound sentence writer and see what Jacques got to say.

Jacques Latour: Hi, Jacques here. I like the spreadsheet. The only thing I'm not sure about is the predisposing conditions. How we would use that or my question is do we really need that section or...

((Crosstalk))

Mikey O'Connor: ...you know, I'm being a slave to the methodology...

Cheryl Langdon-Orr: Yes, straight out of the meth.

Mikey O'Connor: Yeah. And so I think that we're all going to sort of have to learn what that's about as we go. So I tell you what, let me take an action item to dig out - one of the things that I already mentally have as an action item that I didn't pursue because I wanted to make sure that this was roughly okay before I did.

But the methodology has definitions for all these terms like vulnerabilities and predisposing conditions and so on. Let me take an action item to for sure dig out the definition of a predisposing condition from the methodology, Jacques, and push it out to the list. I'll try...

((Crosstalk))

Cheryl Langdon-Orr: ...on the glossary anyway so you may as well.

Mikey O'Connor: Yeah, right. And it's just that it's a big job and I wanted to make sure that I wasn't so far off the track that people were saying no, no, no this is completely crazy in which case I didn't want to do all that work and have it get thrown away.

But if people are comfortable enough that this isn't crazy I'll go ahead and do definitions for that. And I'll push the predisposing conditions one out to the list, Jacques, so that you can see what you think.

Jacques Latour: Okay. Jacques here. So I think everybody should do like top five that - scenarios that they think are relevant to them and then we can merge all of it together.

Mikey O'Connor: Yeah, yeah.

Rick Koeller: Yeah, Rick speaking. So, Jacques, you're saying do the statement only...

Jacques Latour: Yeah.

Rick Koeller: ...as first pass.

Jacques Latour: But the top five...

Rick Koeller: Yeah.

Mikey O'Connor: Yeah and there's a place down here at the bottom. I just scrolled down to the bottom. One option that people have is if you've got statements already, which many of us probably do, go ahead and staple those statements in there as the starting point.

Because I think that in some cases it may be easier to start with the statement and then roll back up into these details. In other cases it may be easier to go through the details like I did and then write a statement. You see what I mean? I don't think there's any sequence to that.

I think that the goal is that at the end we probably ought to have both because the statement is going to be really handy for the report. People aren't going to want to wade through these sort of extremely weird compound sentences. But I think the compound sentences are going to be really helpful for us as the basis for the analysis that we do.

So, you know, I agree, top five by next week would be fantastic and maybe either form is fine for the assignment. Because I think that gets us a way forward in terms of having something that then we can look for common themes, we can look for, you know, there are several that everybody agrees is the big threat. I think that's...

((Crosstalk))

Cheryl Langdon-Orr: Mikey?

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

Cheryl Langdon-Orr: Thanks. I'm just sort of having flashback moments of us - of us going down - and I like the compound sentence-building method; I think this is a good thing. But was it D3 - I really ought to have remembered better but I'm not now. We were playing with the tables where we were almost doing this for actual risk analysis where we were going down and establishing the actual occurrence, lack of thereof and had it been reported by a good source or, you know, or a third or fourth party type one.

Where are we going to be tying that kind of a methodology back into this or are we just not going to do that part anymore? Is this replacement or is it...

((Crosstalk))

Mikey O'Connor: No this is the same methodology.

Cheryl Langdon-Orr: Yeah, I know but are they two different tools we're now using?

Mikey O'Connor: I don't think so. I think that where we were...

Cheryl Langdon-Orr: Okay.

Mikey O'Connor: ...when we were going down the rabbit hole was we were on this line; we were looking at non-adversarial threat...

Cheryl Langdon-Orr: That line we were...

((Crosstalk))

Cheryl Langdon-Orr: As we were going down the rabbit hole we were very definitely looking to the expertise at least within this workgroup to say has this occurred? Has it occurred rarely? Have we - is it just the possibility, you know, have we been

told it's going to happen and (unintelligible) any evidence for it, that type of section.

Mikey O'Connor: Right.

Cheryl Langdon-Orr: And I was, as you know, quite comforted by that exercise. Now I think that's a deep dive exercise but I'm just wondering if we use this compound sentence-building approach whether that's more appropriate for this level of - the top view analysis. And we let them know in this set of reporting that we might be using the more traditional approach to the tool - to the method used by a - I hasten - I don't want to use the term real analysis but more quantitatively based data set going into the analysis I guess at a later date.

Mikey O'Connor: Let me show you where - I need to highlight a gigantic error that I made in that deep analysis that we did. We were looking at privileged users making a mistake. And where we - where I went wrong is that I used the wrong scale. We combined that with - we combined privileged users with a threat event...

Cheryl Langdon-Orr: That's the actual likelihood of a threat event.

Mikey O'Connor: Well and then we had the likelihood - so we had - let's see if I can get all of these on the same screen. Yeah. Remember that we had - before we smashed these down to two we had a bunch of different threat events; we had a big zone, little zone, root zone...

Cheryl Langdon-Orr: Yeah.

Mikey O'Connor: So we were basically picking this one plus this one and evaluating this one. And where we ran into trouble is that we evaluated every single permutation of...

Cheryl Langdon-Orr: Yes, that's where we were getting into deep doo-doo.

Mikey O'Connor: Yeah. And we - at the same time that we were doing that we were also missing this one which is the range of the effect of...

Cheryl Langdon-Orr: Yeah.

Mikey O'Connor: So I think that what we were doing was a mistake in the - in the application of the methodology. I don't - I think that - the nice thing about this is that it - I'm hoping will structure...

((Crosstalk))

Cheryl Langdon-Orr: ...you see this method - mechanism - this tool as meeting the same analysis needs and outcomes as what we were circling the rabbit hole with.

Mikey O'Connor: Yes. But I'm also hopeful that by doing these compound sentences we will dodge the every permutation bullet.

Cheryl Langdon-Orr: Sure, okay.

Mikey O'Connor: Because, you know...

Cheryl Langdon-Orr: In which case I'm coming down firmly on the side of perhaps for our own purposes, you know, maybe just doing the first column to begin with but I think we actually have to do the couplet for the reporting.

Mikey O'Connor: Yeah, I think eventually, you know, especially when we go into the deep analysis we have to evaluate these. And we...

Cheryl Langdon-Orr: What I'm saying is I think we should at least do a degree of this evaluation in the first exercise.

Mikey O'Connor: And treat it...

((Crosstalk))

Cheryl Langdon-Orr: And just warn that there's a whole lot more to do...

Mikey O'Connor: Right.

Cheryl Langdon-Orr: ...and a lot more depth to go into. And, you know, the corresponding - this 59 and everything else needs to be looked at as well. But I don't think - I don't think we'd be doing our mission justice if we only did the first part now.

Mikey O'Connor: And so what we could do - and I think you said this earlier is we could say the evaluation of the second column is simply the opinion of the DSSA in...

((Crosstalk))

Cheryl Langdon-Orr: ...in depth analysis that it will be carried out in the...

Mikey O'Connor: Right.

Cheryl Langdon-Orr: ...blah, blah, blah.

Mikey O'Connor: So our preliminary view is and then try to...

Cheryl Langdon-Orr: Yeah.

Mikey O'Connor: ...evaluate all those too.

Cheryl Langdon-Orr: It's a bit like, you know, a dip stick test versus the, you know, GC/MS analysis on something.

Mikey O'Connor: I'll bet two-thirds of the people on this call didn't know what you were talking about...

((Crosstalk))

Cheryl Langdon-Orr: Yeah but you did.

Mikey O'Connor: I sure did. Jacques, you want to dive in? You're the team that knows how to do these better than the rest of us.

Jacques Latour: Oh I just - something just occurred to me. The charter is to look at the current threats on the Internet and assess them. So and then...

((Crosstalk))

Cheryl Langdon-Orr: Yeah, we're after a measure of actual threats not...

Jacques Latour: Yeah, so - and what we're working on right now is (unintelligible) threats. Let's say somebody does a huge DDoS and takes the whole internet down and what would happen. But in reality I think what we need to do is based on our experience to look at existing threat that we've seen and run them through the model and do an impact assessment on those.

And if everything is low priority then there are - the report is going to say that there are no immediate threats that we've seen that are of high impact or maybe some are high impact or whatever. But it's like a - we should look in our backyard, see what happens, put that on the scenarios that are relevant to this and then we measure the current threat as being either extremely high or low.

Mikey O'Connor: I think that's a great idea. You know, I think the...

Cheryl Langdon-Orr: Measure the degree of rubbish before we look at the detail toxicity.

Mo: Yeah, yeah. And I will caution people that I think that the technical threats - the technical vulnerabilities yield a fairly low level of threat to the DNS. The scenarios that I'm going to tend to write are up in the management layer.

And I think that one of the interesting political choices that this group gets to make is whether to tackle some of the interventions from outside the process like SOPA legislation, like the ITU, etcetera.

Because I actually think that the threats to the DNS that are more profound are the ones that aren't in the technical pile. I think we do a pretty good job of handling technical threats right now. But I think the best way to do it is like you say, Jacques, it's lets push out our top five, back them into the model...

Cheryl Langdon-Orr: Run it through.

Mikey O'Connor: Run it through, see what comes out. And try and do that pretty fast, you know, set a pretty brisk pace on this so that we can really quickly get a sense of what that landscape looks like. And then carry on from there. I think that's exactly the way we ought to do it.

So maybe that's the assignment for this week. I mean, that's I think a pretty darn big assignment actually is for each of us to take the time this week not - I think I'm going to pass on the report outline because that's basically documenting what we're doing. We'll certainly...

Cheryl Langdon-Orr: Get back to that.

Mikey O'Connor: Yeah, we'll get there. But I think in terms of priority, in terms of what we should be focusing on right now let's focus on what Jacques and Cheryl are describing. Let's take this thing through the model ourselves, learn a lot from that experience. I bet we will learn a boatload from that experience. And hit it again next week.

So with that assignment in mind do people have questions about what you saw in the spreadsheet that I can either fix or answer right now? I mean, as I drove you through this today were there things in there that you felt you couldn't work with that I should try to either explain or fix before we drop off the call and get on with the work?

Cheryl Langdon-Orr: Mikey, Cheryl here.

Mikey O'Connor: Go ahead.

Cheryl Langdon-Orr: In some earlier efforts of doing this type of analysis we've come up with really clear numerical or ranking values which when a particular pivot point in the contributing layer that makes that number at the end of the line is changed it changes the whole lot really easily. Are we going to end up - I rather liked that approach. Are we going to get - end up with that same sort of level; there's now five, change this and it'll suddenly become seven type tool at the end of it or…

((Crosstalk))

Mikey O'Connor: I forgot a column...

Cheryl Langdon-Orr: ...open to more interpretation than maybe I'm comfortable with.

Mikey O'Connor: The way that the - we are continuing to use - at least at this stage of the game - numeric values.

Cheryl Langdon-Orr: And maybe it's just because there were empty fields I wasn't seen this accumulated...

Mikey O'Connor: Right. And the reason is simply because I couldn't figure out how to do the arithmetic so thank you for reminding me, Cheryl.

Cheryl Langdon-Orr: Ah, it's a watch this space is it?

Mikey O'Connor: Well it's a fill it in by hand.

Cheryl Langdon-Orr: Right, okay.

Mikey O'Connor: So I will...

Cheryl Langdon-Orr: Can I suggest then we don't ditch the other mechanisms we were using totally; sort of keep those in our toolkit somewhere? Because I think what we don't want to make here especially at this first approach is something that looks too onerous for the organization to take up and continue to do itself in whatever form it decides to do that in.

And to perhaps act as a best practice model for the component parts like ccTLD operators, etcetera, etcetera.

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: And I think what was attractive, if I stick on a ccTLD hat for a moment, what was really attractive about that earlier tool was this, you know, plug a new issue or something actually has occurred and therefore it shifts in its actual risk ranking. It made that lovely click, click into a new level.

And I thought that was rather attractive because you didn't then as an ongoing maintenance issue have to go through and redo this as a huge effort but rather, you know, pull out one little transformer piece and pop in a new one and the thing just readjusted with a new level of risk or lack thereof.

Mikey O'Connor: Yeah I'm going to take an action item that says fix the arithmetic because again I got to this stage of the spreadsheet and I was sitting in this cloud forest in Costa Rica sipping a beer...

Cheryl Langdon-Orr: This is just tragic the fact that you were doing these instead of looking at some of the most beautiful rainforest in the world.

Mikey O'Connor: Oh I was doing the same - I was doing that at the exact same time. Let's see if I - no I can't, I have a great photograph of the top of my laptop and then a rainforest behind it and hummingbirds landing on a feeder. So it was not a great sacrifice that I made.

But when I got to this I simply couldn't figure out the arithmetic part because - and I decided to just leave it empty. So for this particular iteration leave it alone; don't try and fill it in by hand. Arithmetic will follow.

And another thing that will follow is as long as the format of these spreadsheets is always the same, in other words as long as you don't change where cells are, it's easy to roll these up into a giant list of 20 or 30 each with numeric values in columns.

Cheryl Langdon-Orr: Okay.

Mikey O'Connor: That could...

((Crosstalk))

Cheryl Langdon-Orr: Yeah, okay.

Mikey O'Connor: Yeah and so I've got a fix the arithmetic summarize action that I'll work on this week. Because it's not hard I just ran out of gas in the rainforest.

Cheryl Langdon-Orr: You were being carbon-neutral, I appreciate that.

Mikey O'Connor: Oh God. I think - yeah that was very well stroked. That one's right on the tape. I'm not even going to try and come back on that.

Anything else? Are people comfortable and confident that they know what they are to do? Go out, take a - make five copies of this spreadsheet that I sent to the list or however many you need for your top five scenarios. And either start at the top and work down the way I've been doing or start at the bottom and work up with your top five.

And push them back to the list by - I don't know, let's say Tuesday just to...

((Crosstalk))

Cheryl Langdon-Orr: ...less than five for those slackers amongst us won't you?

Mikey O'Connor: Yeah, I'm not going to come up with five. Some of us...

((Crosstalk))

Cheryl Langdon-Orr: ...make come up with five...

((Crosstalk))

Mikey O'Connor: Yeah, I don't know if I could come up with five. Mostly because I'm not that close to the security - the actual...

Cheryl Langdon-Orr: Exactly right.

Mikey O'Connor: ...operational security. So don't feel like you have to come up with five. And I'll send this note out to the list that sort of summarizes this assignment as well.

Cheryl Langdon-Orr: Okay. And will you be doing a quick poll to see how many of us pick the same ones?

Mikey O'Connor: Well I think then what we do is we look at them and see if there are themes.

Cheryl Langdon-Orr: Which I'm assuming there probably will be.

Mikey O'Connor: I would think so.

((Crosstalk))

Mikey O'Connor: You know, I think that it's likely that DDoS is going to be on just everybody's list, certainly be on mine. And we'll see about the others.

Cheryl Langdon-Orr: Okay.

Mikey O'Connor: So that's the story for the day. Two minutes to go, any final questions before we wrap up? Otherwise I'll call it quits and we'll go off and start writing scenarios. Okay that's it. Thanks, gang. Stay tuned for scenarios galore next week. Nathalie, I think you can cut off the recording. And have a terrific day, folks.

Jacques Latour: All right, thank you.

Rick Koeller: Thank you.

Cheryl Langdon-Orr: Bye.

Jim Galvin: Thanks, Mikey. Bye.

Man: Bye-bye.

((Crosstalk))

Cheryl Langdon-Orr: Bye everybody.

Mikey O'Connor: Glen, are you still on the...

END