ICANN Costa Rica Meeting
Joint DNS Security and Stability Analysis WG- TRANSCRIPTION
Thursday 15th March 2012 at 11:00 local time

Woman: We're ready for the recording.

Mikey O'Connor: It's going. Cool. Let's see. In this routine, Nathalie, you want to call the roll from the bridge and then we'll do a roll inside the room?

Nathalie Peregrine: Hi there Mikey. The recordings will be (stopped) on (unintelligible) bridge. And we have as yet no remote (unintelligible).

Mikey O'Connor: Pardon me. The last part got garbled. No remote. Oh, okay. Well that makes sense.

Nathalie Peregrine: No remote.

Mikey O'Connor: Okie dokie. Well, this is neat. We're face to face. Well let's take a minute and do a face-to-face roll call, which we never get to do on the phone starting with - nope I haven't mumbled yet but I'm going to hit that marker. And we'll start with Cheryl.

Cheryl Langdon-Orr: Hi. I'm Cheryl Langdon-Orr.

Keith Drasek: Keith Drasek from VeriSign.

Garth Bruen: Garth Bruen, At Large. Just observing.

Russ Mundy: Russ Mundy, SSAC.

Jim Galvin: Jim Galvin, SSAC.

Edmon Chung: Edmon Chung, ISOC Hong Kong ALAC.

Greg Aaron: Greg Aaron, GNSO.

(Arishi): (Arishi).

Don Blumenthal: Don Blumenthal, Public Interest Registry, (Registry Takeover) Group.

Jorg Schweiger: Jorg Schweiger, (unintelligible), the co-Chair for the ccNSO.

Mark Kosters: Mark Kosters, (ARIN).

Mikey O'Connor: And co-Chair for the NRO.

Mark Kosters: And co-Chair from the NRO.

Mikey O'Connor: You know, we just, you know, kick the ball and drag Mark. There's no respect in this group. I'm Mikey O'Connor. I'm the co-Chair from the GNSO and a member of the ISP constituency as of yesterday.

Oh, no, here you go.

Julie Hedlund: Julie Hedlund, ICANN staff.

Olivier Crepin-Leblond: Olivier Crepin-Leblond, ALAC Chair and co-Chair from the ALAC.

Gabriella Schittek: Gabriella Schittek, ccNSO.

Kristina Nordstrom: Kristina Nordstrom, ccNSO.

((Crosstalk))

Man: …NRO.

(John Latool): (John Latool), (CIRA) (unintelligible).

Diego Espinoza: Diego Espinoza from (.cr) (unintelligible) and ccNSO.

Katrina Sataki: Katrina Sataki, (unintelligible), ccNSO.

Mikey O'Connor: And the wall people are welcome to just jump up to a mic and introduce yourselves as well. I knew this was going to happen. There's way...

Woman: Do you have a roving mic?

Mikey O'Connor: Yeah. Do we have a roving mic?

Woman: I'll get it.

Mikey O'Connor: Ah, we've got one. Cool. That'll be better.

Man: Okay.

Mikey O'Connor: Jim can kick off the wall people while the roving mic is roving.

Jim Baskin: Jim Baskin from Verizon, not to be confused with VeriSign.

Mikey O'Connor: There's a lot of people in (unintelligible).

(Marey): (Marey) from (.iu).

(Justin Esmond): (Justin Esmond), (.nl).

Mikey O'Connor: Oh. So yes, Suzanne, why don't you go ahead and kick…

((Crosstalk))

Mikey O'Connor: Yeah.

Suzanne Walsh: Yeah.

Mikey O'Connor: Yeah. Absolutely.

Suzanne Walsh: Okay. I didn't know you wanted observers to introduce themselves also.

Mikey O'Connor: Yeah. Absolutely.

Suzanne Walsh: Suzanne Walsh, observer.

Mikey O'Connor: You bet.

((Crosstalk))

(John Mennis): Hi. My name is (John Mennis) from (unintelligible).

Marcie O'Connor: Marcie O'Connor. I'm married to Mike. I just know you wanted everyone to know that.

Mikey O'Connor: You know, there's no accounting for bad judgment. What can I say? Poor Marcie made a terrible mistake about 30 years ago and she's been suffering for it ever since.

((Crosstalk))

(Rick Keller): (Rick Keller), .ca.

(Harry Brown): (Harry Brown), .ca.

Man: (Unintelligible), (SAP).

(Marco): (Unintelligible) (Marco) from (unintelligible).

Mikey O'Connor: I think we're good.

((Crosstalk))

Mikey O'Connor: Yeah.

Woman: No seats here.

((Crosstalk))

Mikey O'Connor: There's seats. Come on in.

Woman: (Unintelligible).

Mikey O'Connor: Come on in.

((Crosstalk))

Mikey O'Connor: Yeah.

Woman: (Unintelligible).

Mikey O'Connor: (Rove away). Good deal. Okay. I think what we'll do is maybe we'll go for a while and then let more folks filter in and then go around and pick up the new folks on the fly.

Welcome all. It is so cool to be able to see people's faces in the DSSA. This is very unusual for us. We've spent an awful lot of time together on the phone.

Woman: (Unintelligible).

Mikey O'Connor: Yeah. That's probably right. That would be a not so pretty thing. So it's neat to be able to do this together. And it does get a bit hysterical but this is a - in the management lingo, this would be called a peak functioning team. We've done an awful lot of work really fast.

And so this is sort of a party if nothing else for us to get to work together face to face. So for those of you who are observing, if it gets a little out of control, that's typical. And enjoy the ride as Cheryl says.

So the agenda today is pretty simple but I think it's going to be pretty entertaining. We built a slide deck to update the community and I thought what we would do is go through the slide deck fairly slowly and let the people who updated their respective constituencies sort of chime in whenever there's feedback from your constituency on that slide.

And it shouldn't just be feedback from the sessions because the sessions for the most part were really short but feedback in general. So this is a chance for all of us to feedback into this process whatever we've heard in the hallways, observations that people had.

Observers are welcome to contribute. That's the whole point of doing something like this is to get a little bit more variety in the conversation. So for

the duration of this meeting consider yourselves deputy adjunct junior members of the DSSA and don't be shy about joining the conversations.

So with that, if I can figure out how to - of course I'm running all of the goodies at the same time. And I have to learn a slightly different mode of operation. Now this ought to work.

((Crosstalk))

Mikey O'Connor: No. I got two. I got mine and I got that one. The trouble is that one's so far away I can't see the mouse, so, Jim.

Jim Galvin: (Unintelligible)

Mikey O'Connor: Yeah. But if I do that I hose up the Adobe. Trust me on that. Been there done that.

Man: (Unintelligible).

Mikey O'Connor: Yeah. This is as good as it gets. So if - I think it's okay. I'm looking in the Adobe room. Adobe folks, if there's anything that's - well but we have nobody on the call - we're all live here. So you can...

Woman: My turn to do it. The issue is that because it's recording Julie Hedlund and a whole lot of other people are listening to it through the Adobe room. So they may not be dialed into an audio bridge but...

Mikey O'Connor: But they're on the - they're on the call.

Woman: ...and they are asking the volume be turned up.

Mikey O'Connor: Ah. Any way we can get a little more volume on the bridge? No maestro. Try and see - well, we'll keep our fingers crossed and I think we'll take that as a message that certain of us will not mumble.

So on with the show. I want to sort of start with a continuation of the conversation we really started in the last meeting, which was with the - in the public session of the Board DNS Security and Stability Working Group chaired by Bill Graham. Is Bill here? Dang, he's not. Oh well.

So I - this is a sketchy version of our charter. And as you can see, we're charted by the five ACs and SOs that comprise our constituent parts. And our charter says actual level of frequency and severity of threats to the DNS. Well that phrase, threats to the DNS, bears some exploding and some unpacking. And so we'll do that on the next slide.

Then we're supposed to take a look at current efforts and activities to mitigate those threats. Take a look at gaps and maybe even go so far as to suggest some additional mitigation to those. So let's unpack the word threats.

We use the words that were now coming from our chosen methodology. We'll get to the methodology stuff in a minute. But don't confuse threat events, which is what happens, with the impacts of those events, which may resolve, or the vulnerabilities that lead to those events that gives bad actors a way to cause the threat event.

Don't confuse it with pre-disposing conditions. In other words, if you put your nuclear reactor right next to a tsunami zone, that's pre-disposing condition and exposes you to threats and perhaps makes your vulnerabilities worse.

Then there's the notion of controls and mitigation, which is actually called out in our charter and we're carrying that forward pretty much unchanged. Those generally reduce the likelihood unless they're badly implemented in which case that's an issue.

And finally the sources of the threats and those fall into sort of two categories. There's non-adversarial sources of threat like tsunami or a big weather system or something like that. And the other is an adversarial source of threat, which would be anonymous or, you know, somebody that's doing it with intent and it's usually people. So that's just unpacking what was handed to us as sort of a big word into some smaller words that we can then do some analysis around.

I'm - I want to stop here and see if anybody unpacked this with anybody during the course of the week. And if so, whether there was any reaction to this idea and also to give the folks who've just heard it for the very first time a chance to say this is a good thing, this is crazy, this is bureaucratic nonsense, et cetera, et cetera. Suzanne, go ahead.

Suzanne Walsh: These terms seem to be very consistent with other regimes of terms or some of these I've seen before. And I think that's a really good thing because it allows people to hook what you're doing here into what they already know and see where you're doing something different. So I think this is actually really good.

Mikey O'Connor: It's great to hear that. These words actually come from the methodology and the definitions do too. And we sort of picked a methodology with that idea in mind is that we wanted to leave work behind that could be plugged in to subsequent work. And so that's great to hear. Any other reaction either like Suzanne's, you know, thumbs up, good idea. Getting some thumbs up. Any thumbs down? We'd really like to hear those if anybody's got a concern about this.

I don't mean in the negative bomb throwing sense but in the have you thought about sense. Because constructive criticism because quite frankly at least through your co-Chair Mikey this is the first time this has ever been

done by me. So I'm sort of feeling like I'm flying an airplane and building it at the same time. And, you know, so I'm looking for feedback. Okay.

On to what we've been doing. And I will note to my co-Chairs that being the guy that held the master copy of the deck, I fixed the mistake on this slide whereas I tripped all the rest of the stuff by leaving the wrong city at the top. Sorry about that. Singapore, God.

You know, a couple of times it just sort of - for a minute. I'm sorry. But we have done three really big chunks of work in the last interim. Given our charter, depending on how far down we go and that's a conversation we'll have in a minute into the details.

We - the DSSA may be handling some extremely confidential information. This is information that cannot get out into the world because it would essentially provide a roadmap for the bad guys to conduct attacks. And so while we need it, we also need to protect it. And so we spent a lot of time coming up with what we think is a pretty good first try.

And for those of you like Suzanne and some of the others who are working on other projects, we would cheerfully offer this up. It's out on the Wiki. It's out, you know, it's out everywhere but a lot of our - we've got so much stuff that we've produced that it's hard to navigate.

So if anybody wants any of this, please just ping me and I'll send you the links to the right versions of things. And again, we'd love to hear people's reactions.

If people who are new would be interested in a quick tour of that protocol, okay, let me just jump a little bit out of order here. Nice thing about this kind of meeting is that we have enough time to sort of take detours.

So this is a picture of it. I'm going to make it a little bit bigger. That's really hard to see. Bear with me while I run my mouse from 40 feet away. We had a fairly hysterical meeting just before Dakar where I shrank the slides down because tiny - that's better.

So this is the standard consultant's two-dimensional matrix. Do I believe in God or do I not believe in God? Is there a God or is there not a God? In this case the floor boxes are starting from the lower left - it's hard to read. I apologize for that.

Type 1 is the most sensitive data. It's sensitive and it's attributed to the source of the data. So if my friend Keith from VeriSign handed me some really secret stuff from VeriSign, that falls in that corner. That's the information we will absolutely want to make sure does not make it to the list, doesn't get published to the worldwide Internet, et cetera, et cetera.

And so that black box that's immediately to the right of it says confidential information should never pass through this path. That's the exposure of the - you know, that's the path we're trying to prevent with this.

That information stays in a subgroup that is bound by confidentiality. I believe it's in there - language about all that. There's a text behind this that's about five pages long that explodes this.

The next kind of information it's still sensitive going vertically to the upper left corner. It's still sensitive but it's no longer attributed. And this is sort of the, you know, mentally think about it as this is where the information gets scrubbed, it gets sanitized, it, you know, you look at it not just to make sure that it's going back to the source but also to make sure that we're not giving the bad guys good ideas.

And the boundary out of that is the right turn that the arrow makes where it crosses that vertical boundary into the not sensitive public zone. And a really

important concept there is that no information crosses that boundary unless it's approved by the provider of the information.

So if Keith puts information in, Keith gets to be the gatekeeper to make sure that the sanitized version does not harm his organization. So that's the sort of final check before we release to the public.

Then the - on the right side is information that's the sanitized stuff. And the fourth type is just information that's already out in the world. It's not sensitive. It's attributed to the source. This is information that Keith and VeriSign have already published to the net and we're just drawing it into our analysis.

So that's the sort of short version of what is actually a somewhat more elaborate process. But if people in other working groups are dealing with the confidential information problem and you want a sort of starting point for how to handle it, we're happy to share. I'm sure that I and any of us would be more than happy to walk you through it and help you with it and so on and so forth.

Okay. Back to the - any thoughts about this? Any reactions from the group while I navigate back to where I was? Okay. Yeah, I got to shrink. I won't go too far. Be careful Mikey. This is like Alice in Wonderland and the eating the mushrooms, you know. Don't go too far.

((Crosstalk))

Mikey O'Connor: This is a - this is a working group that doesn't stay within the bounds of propriety. I'm sorry.

Woman: (Unintelligible).

Mikey O'Connor: Yeah.

((Crosstalk))

Woman: Unlike all the other - unlike all the other (words you say).

Mikey O'Connor: When I was interviewed by the Board of Regions for the University of Minnesota for a very sensitive job, they asked if I experimented with drugs and my answer was, "Wouldn't exactly call it experimentation." Okay.

Second thing we did - you think this is unusual.

Man: If I can save my co-Chair and ask him to go on because I think he's just incriminating himself at the moment.

Mikey O'Connor: In public on the worldwide Internet. Hey. It was a long time ago and I have no recollection. See why the room clapped when Marcie got introduced. She has to put up with this every day. Okay.

The second big thing we did, and it was a big thing, was this selection of a methodology. Because we ran into a lot of trouble and we saw a preview of that in a way in the preceding meeting where the Board DNS Security Group was struggling a bit with terminologies and boundaries and all that kind of stuff.

And one of the helpful things to do in that situation is to select a methodology that sort of pre-defines boundaries for you. And so we looked at about two dozen, 24 or 25 methodologies and wound up pretty informally selecting the NIST 800-30 standard, which is pretty well known.

And that's - we consider that a big deliverable just in and of itself because simply selecting the methodology as Suzanne pointed out leaves a way for this working to be plugged into the work of others and be passed on to subsequent groups. We're going to circle back to that in a minute.

And then the last thing is that we, you know, we dug into the detailed analysis. We actually went a little too detailed at first. And that towards the end of this we'll circle back to that question, which is how detailed to go in this pass and how fast to go in this pass.

And I've got a sense of an emerging consensus from the community that I want to try out on us just to make sure that the sense is right. And if it is great and if it's not we need to talk about that. So anyway that's the very high level view of what's going on.

Diving in just a little bit more to the NIST 800-30 stuff, I've previewed most of this. The highlights are that this methodology is out in the community and is available at no cost. There are a lot of methodologies that you have to pay for some of which are quite expensive.

And A, we were in a hurry; B, we didn't have a budget; C, we like open source here. So to the extent that we could find something that was already out at open source, we liked that. And so the NIST methodology sort of hit that criterion.

We also found a bunch of dead methodologies that were fine but they weren't being supported anymore. And what is going on behind me? It's like - are there invisible people walking in and out?

Woman: No.

Man: No. (Unintelligible).

Mikey O'Connor: I hate that when...

Man: The door is locked so we could not get out.

Mikey O'Connor: Let me hit the unlock button. And then, you know, the last point is sort of this reusability idea, which is that, you know, people within other parts of ICANN might be able to use that and that would be useful.

There's an eye chart. We don't want to talk about eye chart except to say that there is - this is a very substantial methodology and there's a lot of pages like that in here and that was really useful. And I've already sort of previewed the benefits so I'll skip this.

This is a 45, 50,000 meter view of where we are and the distance in time between the where we are now and where we're going is a variable and we're going to circle back to that question in a minute. But we're really right now digging into the real analysis of the threats vulnerabilities, et cetera.

And now we get to that sort of magic question. So we've been at this as a team for about 43 weeks. That's the precise number because every week we get a weekly status report and I count them because I love to count. And there's 43 of them.

One way to think of that is 43 weeks. Another way to think about it is that we've really met for 43 hours because we meet for an hour a week and we've covered an awful lot of ground for meeting for 43 hours even though its taken a long elapse time.

And one of the things I've been previewing with people with money in their budgets is the possibility that we might be able to move the ball a lot forward by meeting as a group in person a couple of days before the next ICANN meeting, something like that.

I'm not sure we're going to need it but I have been sort of laying foam on the runway that we might. And so far I've been getting answers sort of along the lines of if you can give me a decent justification we can probably find the money to do that if you need.

But the puzzler and the real choice and the thing that I've been socializing this week as have the other co-Chairs is given that we have a finite set of resources, pick any two of three and there are only two, that's clever. I like that. Mikey, that was good.

I took off one and that's why there's only two but then I didn't notice. Oh, go ahead (chief). Sorry. You should be in my sight line. I know - what can I say?

Olivier Crepin-Leblond: Thanks Mikey, it's Olivier for the transcript. Forty-three weeks, 43 hours but you do have to bear in mind that we loved it so much to be co-Chairs that we also had an hour as well so it's actually 86 hours that we spent together.

Mikey O'Connor: I stand corrected. And I apologize for that because that's absolutely right. There's a leadership team that meets an additional time a week and does double the email load because we have a pretty busy email list too.

The leadership group focuses on process stuff for the most part. And then we bring those ideas back to the main group for verification but we try to keep the SSA focused on content as much as we can because we know that people get a little impatient with process. And so we try to segregate that. So Olivier is exactly right. It's at least double and perhaps triple the 43 hour that was - right on. Thanks Olivier.

The choice that we're at right now is how fast or how deep do we go. We think tentatively that we could probably get through this whole methodology in one pass by Prague but we would do a very rough cut pass. And basically we would be able to identify the very rough outlines of all of that stuff, vulnerabilities, blah, blah, blah. We'll get to that in a minute.

But we wouldn't go very deep. We certainly wouldn't be able to do an extensive analysis. Probably wouldn't be able to go through the confidential

information layer in this pass. Or we could go deep and get into the confidential information and it would probably best guess take us two to three years to get that done, which probably needs to be done sometime.

The question is whether that should be our approach. And I had a lot of conversations where the initial reaction was your charter is to go find those details, go deep. And then I would start talking along these lines.

We've got a team that's been at it for almost a year. We're starting to already see attrition. We're going to burn people out. We - and probably the worst thing is that we might get two years in to a three year project and discover that there was something fundamentally wrong with our approach and have throw away work that, you know, we've had a bit of throw away work up until now but it's only been a month's worth or six week's worth.

We had two weeks - two years worth, that would be a big problem. And so at least in my conversations with people around - I've been lobbying pretty hard for let's go through this pretty quickly once, identify whether the methodology actually works right and identify areas that clearly need more work, deliver by Prague or at least deliver the preliminary document by Prague and then see where we go from here.

And generally the people I've talked to who've started out saying go deep circled around and said oh yeah, that's not a bad idea but, you know, I want to stop at this point and see where - for others who've been socializing this, you know. Our co-Chairs, staff, observers, you know, I think this is - we're actually going to go in the decision making mode here for a minute. This is no longer update mode.

I'd like to come out of this meeting with sort of a sense that we've got a path forward. And then if it is that path, you know, we'll go right to work on putting the pieces together to execute on that. So I'll stop now.

Mark Kosters: So I'll volunteer to go first. This is Mark Kosters. I like to go for speed just because there's a lot more things that we'll circle around with at some point. But I'd like this to be a determinately ending process as opposed to indeterminate.

Russ Mundy: Russ Mundy. I think Mark has a very good point to get through it once, get it out the door. Having done different or similar kinds of things in another life, one of the real risks you run with that is at the end of it from a realistic point of view you don't necessarily know a lot more than you did at the beginning. Okay.

And I think as long as the committee is aware that that is a possibility - I mean I'm not saying that will be the outcome but it's a possible outcome. I think that's the right way to go to get something out quicker because that in itself if that is one of the outcomes says okay, we need to figure out how to do a long hard deep, you know, like much more energetic kind of thing.

Mikey O'Connor: Cheryl.

Cheryl Langdon-Orr: Yeah. Cheryl Langdon-Orr. Okay. Agree. And I - and, you know, I'm all for it but let me be clear in interest. I was one of the three CCs, which was (shared), chartered this. But I understand absolutely why we wanted what we wanted to get done to be done.

However, I want to challenge the group and say why can't we have it both ways. Let's do what we're planning on a proper quick but detailed enough run through for Prague. And at that point recognizing that some humans actually have a life outside of ICANN, okay. Then commit those who have the stomach or stupidity to go on with the job to go on with the job.

What I see as a huge danger is whoever is tasked with getting what we're charted to do done done is then going to have to start (unintelligible) and I don't want that risk. Whole education, whole lot of other stuff. Right.

We've got a whole lot of infrastructure, intelligence and knowledge, which we've managed well in position. So I would like to have my cake and eat it too.

Mikey O'Connor: Typical. So I put a slide up that's - well let me just - let me just respond to Cheryl. We actually had a slide in sort of the backup deck that said - and I use the bad underneath slide to use it that sort of hints at that.

And what I hear you saying is do the first pass and then find some places to go deep. Try and hold the group together. At least go back to our chartering ACs and SOs and get permission to do that. And maybe that's the way forward and I agree wit that. Now Jim, go ahead.

Jim Galvin: So Jim Galvin. I'm more inclined for speed rather than depth because I feel like if we can, you know, get something out then we have the opportunity to get some public comment. I mean we can call it a draft and take a step back and get some comments from folks on making sure we've got all the high risk things laid out and then we can dig in deep in a second round and do it that way.

And I'll also pass on that you've got Don all the way over here on your right with his hand up.

Mikey O'Connor: Online is better than in person. It's easier to see the check, you know. That's another problem is I often crack up my team members. And then there's a pause while everybody giggles. It's fine. You're behaving perfectly normally for this group.

Don Blumenthal: To be honest I was joking but that's another - I was going to say something along the lines that Jim did. I don't think it has to be a complete either/or. It can - Cheryl just get through and then we really do have the opportunity to dig in when we see it's really necessary.

Mikey O'Connor: Anybody else? Olivier, go ahead.

Olivier Crepin-Leblond: Yes Mikey. Olivier Crepin-Leblond. May I just suggest the report might be called interim report and that will open the door to us continuing?

Mikey O'Connor: Yeah. I kind of like Stage 1 because we're sort of done with something when we're done with that first pass. And I think that we deserve to be able to call it that. So but words are really important. So let's pick a good one that sort of declares all the good things that we've done but also leaves the ability to continue on.

Man: Alpha.

Mikey O'Connor: Yeah. Alpha test. Beta test. At least beta test. Maybe customer pre-release. I don't know. Anything else? Does this seem - yeah, what I'm hearing is that we're sort of on the right track, you know. Okay. I'll get off of that one.

The real problem is that I want to do this on my screen because I'm seeing this. And when I click on the Adobe Connect room, nothing happened. Okay. Ooh, back up. Back up. There's where we were. I think we've got a decision out of that one. That's great.

Here's summary - remember what we said was that we have started doing real work. And this is the summary of the real work. I'm going to read these in reverse order. I think the biggest piece of real work that we did was we identified three threat events.

And you may say wow, that's not very many. But what about this? What about a left handed (DDOS) attack by a Martian that's landed on a flagpole in Arizona? Isn't that a threat event? And the answer is that's a threat event that's, you know, it's an attack fact but it's not a threat event.

The threat event is a zone is not resolved, a zone is incorrect or a zone is insecure. And then there's a lot of things that go into creating that threat event.

And when we started using the words in that narrow sense, it allowed us to get our list quite short because what we realized is that we were packing too many clauses into those sentences. And in fact in putting all those clauses together, we were creating a task that probably could never finish.

In fact we sort of started to extrapolate that just getting through one part of the task was going to take us three years and realized that we were heading into trouble with that.

So those are our three threat events. A zone - and note we're careful not to specify which zone. And the reason we don't specify which zone is another trap to fall into because if we say the route doesn't resolve, we've conflated two variables.

And so we say A zone doesn't resolve and then we address that which one question in the level of impact, which is right above it there, which says that in the worst case -- let's say it's the route zone -- there would be broad harm, consequence, impact worldwide if the route went away.

But in all cases with all zones not matter how big or small or how widely used or how many domains, whatever scale you choose to pick, if you're using that zone as your domain and your customers need that zone to resolve in order to do business with you or reach your Web site or deliver your messages or whatever the use is, if that zone that you're in doesn't resolve, the impact is profound. Go ahead.

Russ Mundy: I have a little bit of a problem with the second two as being two separate things. I have a really hard time differentiating between them. And it seems

that in terms of the end product that, you know, when - we want people to read it and understand it and have it make sense.

And so if we've got in the list of threat events three things but two look the same, we either need to come up with better naming, better description or better way to put forth their differences in their short one line bullet or there's really only two things. At least that's how I think it'll be perceived.

Mikey O'Connor: I think it's you're perceiving it that way because that's a correct perception. How about that? You know, when we talked about this we said, you know, zone security is really a subset of incorrect. But we were so interested in it we decided to promote it to the top level of our hierarchy. And so when you see that in just an instant briefing like that, that says that that was maybe a mistake.

Russ Mundy: So some set of the people in this room know that I've been a big DNS SEC geek for a lot of years. But if they've seen some of my presentations, they'll hear me say the date in the zone is the most important thing; even more important than the DNS SEC and the DNS SEC protection problem.

And the meaning of the term security is hugely hard to understand because it can have such a wide meaning to so many different kinds of people. If you're in a DNS SEC session probably most of the people are talking about the DSN SEC aspects of security.

If you're in, you know, a ccTLD session, you're probably talking about more of the processing and the content, the physical and so forth. And to try to differentiate security from the information is correct when security is such a broadly inconsistently used word, I think frankly is a mistake.

Mikey O'Connor: So we could go a couple of different - oh, I'm so glad you raised your hand since you're the one who came up with this idea. You can dig yourself out of this one.

((Crosstalk))

Jim Galvin: It's still consensus of the group that however it came out but no, I think the action here is just that Russ' point is taken, you know, quite - and he's right, you know. We need to be very careful about terminology. I mean we learned that obviously before as we spread apart threat events not to be confused with - and we had that long list of things. I think it's very important whatever we decide we want these things to be.

And in fact we were sitting here trying to chat and I was trying to tell him what I thought those things were and he's, you know, just telling me I still don't like it Jim. And so it's fine. We need to put - we need to think harder about what we mean by those things and come up with different terms and we should take that back as an action to the group to revisit that and do that differently. I think that's exactly right.

Mikey O'Connor: Yeah. I mean I think it's a fabulous comment and I think it gets right to the - a nicely substantive issue that we do need to take back. Thanks Russ. Do you have a follow-up on that?

Russ Mundy: Well, in terms of what terms might be good, I'm not certain. But I think using the word security is probably bad.

Okay, some other phrasing would be better because security just is so widely and broadly overloaded in so many contexts.

Mikey O'Connor: It's sort of like threats. And you know...

Russ Mundy: Yes.

Mikey O'Connor: ...it's sort of like what we ran into.

Russ Mundy: Right. Yes.

Mikey O'Connor: You know, we get that big time.

Are there any good - just to pause at this point, are there any good explosions that - you know, taxonomies of that word security that are out there that we could steal?

Russ Mundy: Well, I don't have any that - off the top of my head, but one of the - the big concern was I see that phrase.

Mikey O'Connor: Yes.

Russ Mundy: And you want a nice, you know, concise sort of phrase. But it doesn't convey a meaning to even a security person because a person that's not deeply in security would say, "Okay. Gee, I heard this. I heard that. I don't know what it means." A person that is deeply engrossed in security would say, "Well," - you know, enumerate off 10 or 20 different things that it might be.

So they can't really differentiate from the one above it, and I think that's the important thing. If we're going to have three, they need to be differentiatable in a very straightforward way.

Mikey O'Connor: Now I'll take a queue. I've got Joerg, and (Jacque), and (Ray). There we go. Okay, so Joerg go ahead.

Joerg Schweiger: So Joerg Schweiger. If we really do want to go into technology right now, I would suggest something like aren't we really talking about data integrity? Would that be summarizing all of your issues? Like security and incorrectness?

And on the other hand, if the zone doesn't resolve, well we're talking about zone and data availability, so we've basically got those two things; availability on one hand side and integrity on the other one.

Mikey O'Connor: Go ahead (Jacque). Unless - yes, we'll just go through the queue and then can come back...

(Jacque): Well, I just had a small question. Let's say by mistake I put my private people, my (KSK) on Twitter. My zone is still resolvable. It's still correct. But then there's a third thing which is it's compromised by security. So there might be three just from my point of view. So...

Mikey O'Connor: Yes. That's a good one.

Go ahead.

(Ray Callas): So...

Mikey O'Connor: I'm sorry, we do have to do the transcript.

(Ray Callas): So, (Ray Callas) from DotCA. One of the things I'm observing here is you're struggling with how you're framing or trying to communicate a list. A practice that I've established in my organization is an IF/THEN statement. An IF - like a risk is something bad may happen. Something good may not happen. The threat event is the IF, but you're missing the THEN. The consequence. And by combining them both in a structured sort of language and format, you can more accurately convey whatever risk you're trying to identify.

There are other models in - you know, in an IF/THEN statement, but by using consistent sort of structure, the leader always understands what you're trying to say.

Mikey O'Connor: Thanks a lot for that. We've gotten - and let me just show you the THEN's which are on the next page.

So then all these terrible things happen. And the reason that we're being so cautious about not putting those together is because of the permeation of the problem.

Yes, exactly.

And one of the things we realized is that as we were combining, we generated something that didn't scale and we wound up with a list that was too tall to evaluate.

And so what we're trying to do is do them in columns and then thread through essentially compound statements which is IF/THEN - if this actor does this thing to this vulnerability, then this bad thing happens and this is the impact. So you wind up with like these long statements which if you conflated them all, you wind up with millions of permutations.

And so towards the end of this, we're going to have this interesting threading together of compound sentences - problems to solve. But for now, we're trying to keep it in silos and you immediately run into this exact problem, which is it's easier in a way to define those compound sentences. But as soon as you do, you don't scale.

And for those of you who have done these before, you know how tricky this is.

Anybody else want to chime in? We certainly got the message and appreciate the message a lot.

Man: Let me just say Mikey, I think that the subsetting underneath of the main bullet might be the answer.

Mikey O'Connor: Yes.

Man: You know, so there's two main items and then...

((Crosstalk))

Mikey O'Connor: ...on the list.

Man: ...and then (unintelligible) - there's a (unintelligible).

Mikey O'Connor: So maybe what we do is we kind of lapse the two and then subsets under each because we may have a - you know, we may have a subset under the first one as well, yes. Yes, that sounds good. Okay. That's terrific.

And by the way, those of you who are now new to the group, you're now official deputy members. This is what we do every week. And this is sort of the way we do it every week. You know, we don't do it with a PowerPoint deck, which is a pretty inflexible thing. We have these elaborate mind maps that we maintain.

So, I'll show them one - I'll show them mine.

Oh in fact, I've got a slide. Wait a minute. I'll do it right now because - and don't leave the room Cheryl. Hold on a minute.

No. No. Wait a minute. You can't leave yet. You can leave in a minute, but you can't leave now. I've got to find it - this slide that's so - there it is. All right. And the reason Cheryl can't leave is because she's got the design credit on this.

Cheryl Langdon-Orr: (Unintelligible).

Mikey O'Connor: So - oh it's too bad it's not a mind map on this one. But when we're working...

Cheryl Langdon-Orr: That's what it looks like.

Mikey O'Connor: We're really beating the heck out of the Adobe Connect environment, because what you're seeing is there's a shared document that's on my screen at home that we're - and now you can see it.

Cheryl Langdon-Orr: (Unintelligible).

Mikey O'Connor: That is being updated in real time. Then we've got a chat going that's pretty lively. We've got polling sometimes going on. We've got definitions along the bottom. We have the list of persistence. So this is a pretty active/interactive lively conversation that's going on and I think that the online tools are the only way we could've gotten this work done. There's no other way we could've gotten this far this fast. So it's pretty neat.

And you can tell that there's a fair of us (unintelligible).

Okay. I think we were on this one. Yes. And I think we've kind of beaten this one up. Anything else on this slide before we move on to the next one?

That was a great discussion, so I don't want to leave it prematurely.

Okay, we'll call that done.

The one that I previewed was - well what happens. And these are straight out of the methodology. These aren't words that we invented at all. The methodology actually has a very detailed hierarchy of the nature of impact. And we're probably just going to steal it. We're probably not going to do a whole lot of work on that because getting - you know, if we do our sort of rough cut thing, we're just going to say there's the list.

And then when we thread the compound sentences together, there will be certain ones of these that will tend to rise and float into those sentences.

So I'm not going to go very deep into this and don't want to defend it a lot, but if there's something that makes you crazy about this list, sort of like our list made Russ a little bit crazy on the last one, that's important and we'd really like to hear about that. So I'll give you a minute to sort of look at that, conjugate about it, see whether you know it makes you nuts.

If it doesn't, we'll keep going. But these are very broad and they really aren't generic at this point because it really isn't in - it doesn't really modify our charter a whole lot if we go very deep into this, because we all know that bad things will happen, and here's sort of a taxonomy of those.

So - oh, sorry. I'm missing somebody.

Man: (Unintelligible).

Man: I (unintelligible)...

Mikey O'Connor: Oh, you're going crazy again. That's excellent.

Man: But the one that really caught my eye is harm to individuals. And I think that's intended to be point at, at least in this context. The users of the zone. And it would seem if we're taking the liberty of tailoring the words out of the...

Mikey O'Connor: Yes. We certainly are.

Man: ...(unintelligible), I think it would probably be better to say something like that. Harm to individual users of a zone, if we're talking about the zone as sort of the atomic thing...

Mikey O'Connor: Right.

Man: ...in the report.

Mikey O'Connor: That's cool. I'll add it in brackets so that we can beat it up later on a call just in case. But...

Warren Kumari: So - Warren Kumari, Google. So I'm not entirely sure in what cases there wouldn't be harm to users of the zone if there's any sort of harm. And it - do you mean individual users or do you mean consumers of the zone? Or - I mean if nobody's using it, nobody gets harmed.

Mikey O'Connor: Bear with me for just a minute. This'll be my chance to show you one of the mind maps. Because, I mind mapped the whole methodology, and so I can explode this terminology, and so I can show you the mind map thing at the same time that I show you what the methods actually say about this.

And this is what we typically do is when we get into a discussion about this and we say, "Well, what do we mean by this term?" So let me just drag the mind map on the screen. It's kind of small. Let's make it bigger so you can read it.

So there's the top of the tree. Here's the task we're in, conduct risk assessment. And we're in the part that - this is awfully small. I apologize for that.

So this is - where are we? No, this isn't it.

One of the things that we've done is - here we're getting to impact. Yes, here we go. I found it.

So you see this table. Examples of adverse impacts. See those words? Those are the same ones. This is how we're stealing it. So then in the

methodology, let's explode the harm to individuals one and there's their list. Let me make it big enough so you can read it. Hang on a minute.

There we go.

So here are examples of harms to individuals that the methodology is calling out. And so it's not really users of the zone necessarily. It's people who in that zone may suffer these kinds of harms. And, those could be - yes. And in that zone's got Russ - he's got the words - you're right. I mean, that's why we're thinking a first pass through this is really helpful, because then those kinds of quizzical looks towards the sky can come out and we can tune this up.

So I saw - did your hand go up Jim for a minute?

No, okay.

So let us take your modification on advisement and we'll beat this up and we'll see.

But this is the way that we use the mind maps, and this is also the way we use the methodology. This is why methodology is so helpful to us because it gives us a touchstone to come back to.

Now that said, one of the really important things to say about this methodology is this is a methodology that's designed for a single organization. And in this project, we're bumping up against the edges of using a methodology that's designed for a single entity to address multiple entities.

And a bunch of us have had lots of conversation about that in a lot of different contexts, and we're going to puzzle through that as we go.

Anyway, that's sort of a little digression into covering a bunch of stuff; methods, mind maps, et cetera.

Some of these mind maps are unbelievably gigantic and they're pretty bewildering, but at the same time they're really helpful when you get - when you want to quickly get to the details of something - try to find that in a Word document. I bet you can't.

Okay, so there we are back at the top level of that hierarchy. And we'll leave that in for now, and we'll circle back around and cogitate about that.

Anything else? I mean this - again, this is precisely why we're here people. It's - we're not here to listen to Mikey give a talk that you can get anytime you want. You know, what we're here to do is have this kind of conversation.

Go ahead.

Russ Mundy: It's Russ again. At the risk of being a pest...

Mikey O'Connor: No. No. Excellent.

Russ Mundy: I look at this list and say, "This list seems to be very ISP, registry, registrar-centric.

Mikey O'Connor: It's IT-centric because this is an IT methodology. It's not even...

Russ Mundy: Right. No, but I'm - but just to look at the words that are up there and - you know, that's - if I were again trying to think - I'm at the end, I see an output and I see that list.

Mikey O'Connor: Yes.

Russ Mundy: And that was probably the first thing that keyed me. Where are the users?

Mikey O'Connor: Right.

Russ Mundy: That's why I had to search to say, "Okay. Harm to individuals."

You know, we exist because there are users of the Internet. You know, this organization - every one of our individual organizations probably, at least to an extent, exists because there are users of the Internet. And it looks to me like the user - the user aspect of this is way under emphasized.

Mikey O'Connor: And I think that what we can do is we could take that - because those detailed ones are pretty good examples of the harms. So maybe the thing to do is pull some of those examples up so that people can go, "Oh, that's what you mean by this list."

Russ Mundy: Yes. (EG)'s.

Mikey O'Connor: (EG), yes.

Jim?

Jim Galvin: So, Jim Galvin. I confess I - just at this point I don't remember where it is in all of this, but I mean we've obviously had many conversations about users and impacts and effects on them. It feels to me like that's covered somewhere. It's just not in this particular section, so I just want to point that out. We don't have to resolve that issue right now, so your note there is fine. I just want to remind ourselves on the record here that I think this is covered.

I think the issue that Russ is probably getting to most is that we've included some things for completeness because they came out of the methodology that we're using, but they may not all be appropriate and we may want to revisit that and maybe revisit a little bit of the structure that we're coming out with here. So that's all. Thanks.

Mikey O'Connor: Well - and to a certain extent it gets back to the preceding slide, which is this taxonomy that if you're in that zone, if you're - you know, your impact is going to be profound even if your zone is tiny little zone. You know, and that's that huge conversation that we've had over the last month.

And then the question is, "Well, what are those impacts?" And I think that what I'm hearing is we should get more illustrative in describing those so that people can get a sense of what those profound impacts would be. And that's I think great feedback.

Cool. Anything else?

All right, so this the way forward slide. This is sort of the questions that remain to be answered in the methodology in big chunks. One of the things that's interesting about using a methodology is you try to get inside the heads of the people who wrote it and you go, "Now, why did you ask that question first?"

And we've decided to sort of resequence it just a little bit because the methodology starts with the threat sources, and we discovered that that's not helpful because we immediately get into the problem of, "Well, when this threat starts we get this, and this, and this," and we started getting these huge compound sentences right off the bat.

And so we're still in the process of tailoring the sequence of the methodology to be one that works for the task that we're working on. And so I've - the reason I say that is because this sounds very orderly and put together, because it's in order and stuff like that. But, it's not really. We are still working our way through a first pass of a methodology.

And so if people have insights on which questions to ask first I'm sort of looking at a new recruit to the working group because you know, your gang has been through this a lot before. You know, if you were to look at this list

given all the work that you've done at (Cirri), is this the sequence you do the work?

I mean, we're thinking we're going next, but I would like thoughts from people in the room. Because now that we have this very rough cut view of what the threat events are, we're going to dig into vulnerabilities. We have a gigantic - a gigantic mind map of vulnerabilities that we built before we realized that we needed to structure this work a little bit more. It is simply mind boggling.

Man: (Unintelligible).

Mikey O'Connor: Oh, okay. Okay. Hang on.

Woman: (Unintelligible).

Mikey O'Connor: Okay, hold on a minute. There'll be a short pause while Mikey rummages on his machine to pull this mind map up. But you know, it's probably good for the rest of us to remember what we did, because we did a lot of stuff. I mean, we spent - we did a bunch of work in Singapore in a face-to-face meeting like this with flip charts and all that kind of stuff, et cetera.

So here it comes. It's probably going to be a tradeoff between text size - so let me start making it a little bigger because this looks innocently simple.

That was a really good diabolical laugh Cheryl.

Cheryl Langdon-Orr: (Unintelligible).

Mikey O'Connor: So you say, "Well..." - and by the way folks, as I've gone through this I think we've got a few major categories at the very highest level that we have to flesh this out with. But we said, "Well, there are operational issues, there are infrastructure vulnerabilities, and business and technical process vulnerabilities within those." We've got all the stuff that was in (SEC 47) in

terms of registry failure, and then we've got a whole pile of stuff that sits under managerial choices.

And you go, "Well, it's not too bad." Now let's see if I can explode the whole thing.

Yes, there we go. Now in order to get this on screen - no, it's still too big. We have to make it smaller than that. so we'll make it that size. And you think, "Oh, that's good." Oh, but that's only one branch. Hold on. That's not the Explode All button.

I'm learning a new tool. I used a different mind mapping tool.

There we go. So we have a list. So for those of you who are looking for lists, have we got something for you, and that list ain't done by far. So we've got a parsing, crunching, thinking thing to do, and that's what we think we're going to do next is go to work on this because we think that's the next tastiest conversation.

Are you nodding in agreement that this is a good place to start?

(Ray Callas): (Unintelligible).

Mikey O'Connor: Yes, okay.

(Ray Callas): Just a question of...

Mikey O'Connor: Go ahead and grab a mic. I don't where the roaming one is, but why don't you just sit at the table. That'll be easy.

(Ray Callas): It's (Ray Callas) from (Cirri) again. This - just a question is have you contemplated a numerical scoring algorithm at all?

Mikey O'Connor: Yes. We have.

(Ray Callas): You did? Okay, good. Good. Yes, because that's critical.

Mikey O'Connor: Yes.

(Ray Callas): Mathematically, you can then start to rank.

Mikey O'Connor: Okay, right. So that makes sense. Yes, the methodology has a scoring system in it, it's just zero through five. You know, you sting them together and you get weights and all that good stuff, and that's the thought.

The error that we made was in doing the scoring as a group because you know, you pick one item from a giant list like this with 30 people on the phone, then you have a lovely conversation - it is lovely. I mean, I'm not kidding. That is not sarcastic at all. It's just like this. It's really good conversation. Very rich, but only evaluate one and there's 150 yet to go.

And so we're - that's part of the how fast, how deep, and we're not going to go this deep in the first pass. We're going to do a lot of clumping and stuff like that.

But you know, the question that I'm really puzzling on right now is I don't think there's any necessary first step, but this seems like a fruitful first step and so this is sort of where we're heading first.

Man: (Unintelligible).

Mikey O'Connor: The roving mic is getting fired up and - there we go.

Man: We had two engineers trying to make it work for about ten minutes, and (unintelligible) - there you go.

Man: Miracle.

Man: Found (unintelligible) about one and a half second. I love my support staff.

Mikey O'Connor: We're not going to go too deep into that one.

So (Ray)?

(Ray Callas): So yes, (unintelligible).

You may find because of the very, very many (unintelligible).

Mikey O'Connor: Right. And my thought is I think at this stage that we'll traverse a pretty deep data set like this and maybe just eyeball it and say, "Okay, that's a couple of layers in the branch." This one is still full of snakes and dragons, and this one isn't.

And so in terms of the next pass, here are our favorite branches to go down because they seem to contain the tastiest, nastiest thing.

And I think that one of the things that occurs to me is when you're a member of the group, he says...

Man: (Unintelligible).

Mikey O'Connor: Yes, don't you think? Yes.

Woman: (Unintelligible).

Mikey O'Connor: Yes. I think induction by drafting is fine, yes.

Woman: (Unintelligible).

Mikey O'Connor: I think those of us who have done these before to the extent that it's not confidential information - if there are things that pretty closely mimic this analysis that you've already gone several cycles through, that would move the ball forward for us a lot because this is not necessarily the best group to actually evaluate these things. We're not close enough to it. I'm certainly not versed enough in it.

And so, we might want to go look for those who have gone ahead that we can steal from, and I mean - and I'm looking at you and some of the others in the room who've gone through these before as the source of this.

Why don't leave (Ray) with the mic? I imagine he might be back with more.

Okay. So we'll get rid of the stupid mind map, and I think that what we're saying is vulnerabilities first is fine. It's not perfect, but it's good enough. We do good enough here. We don't do perfect here.

And then the rest of this page is the compound sentence that says when you thread these together - you know, a thread event through a vulnerability through an actor that's trying to exploit it that's in these previous (building) conditions with this situation about controls. What are the high risk scenarios that fall out of that?

That's really our target is to find the high risk ones in this first pass in a very rough cut way. Pass that structure on to people so that then we can dive down a layer or two and quickly get something out to the community for a reaction like the conversation that we've been having, which is extremely important.

And if that feels okay, then good deal. It's kind of a validation of what we've been doing. I'm kind of getting nods. That's good.

It's a quarter after the hour. We have the room until 1:00 if we wanted to kill ourselves we could do another big chunk of work, or we could not do the next big chunk of work, or I could do a very high level - I think I want to do a five minute version of the next chunk where I'll just talk at you.

And once we've gone through that, if there are reactions and we want to go deeper, maybe those who want to go a little deeper into this can stay and the rest can leave, blah-blah-blah.

But given that the vulnerabilities next step made it through the essential - the review cycle if you will, I want to get - what the heck? Oh, I see. Linked together. (Unintelligible).

This is hurting this old brain with this one.

At home, I have all these monitors and it's just like, you know, a space ship. This isn't nearly as spacious so to speak.

Here it is.

Man: (Unintelligible).

Mikey O'Connor: All right, so what I did for this next deck is I took the vulnerabilities part of methodology. One of the things about the (NIS) methodology is that it's extremely dense. And even I who have read it a bunch of times now keep finding more stuff in it.

So what I thought I would do in this deck is just very quickly take you through one page of a 90 page methodology that describes vulnerabilities and just do some sort of level setting on terminology.

So I'm just taking sentences from the methodology and highlighting things. So they say in the - and this is straight out of the methodology, and I think we

will want to for sure, if not today on our next call or the next few calls, we're going to want to change these words to fit our circumstance better.

But there are the words of the definition of what the methodology thinks of as a vulnerability. And I'm not - you know since we're all here in the room I'm not going to read those to you. I highlighted the interesting bits to say - and here it's - you know, back to the point I made earlier Russ, this is information system methodology.

And this is the kind of thing you need to tweak because this isn't exactly that kind of critter. It's close, but it's not quite, and you need to constantly remember that. And so your point there was right on target.

So the - you know, there's a definition that - you know, a threat source can come in. This is sort of the very expanded version of a compound sentence that we were talking about, (Ray) and me. And you can see how those sentences sort of get threaded together. That vulnerabilities are usually tied to some sort of control situation that may or may not have been applied, and that amplifies the vulnerability when they haven't.

On the other hand, it mitigates the vulnerability when they have, and that's why you have to thread these together, and I'm getting a nod on that from (Ray), so it feels like we're on the right track.

Then the next thing it says is - but wait folks - and this is why I wanted to highlight this today because this gets to the non-information system stuff. It gets into the governance and the risk management strategies and communications, and all that kind of good stuff, which hopefully is going to come out of the (SSRRT) conversation too.

Because as we get into the higher levels, that starts to get outside the scope of our remnant, but I'm sort of declaring some of this inside the scope because I think if we only stay at the sort of technical layer, we miss the

opportunity to identify threat sources, intentional or not, in things like governmental actions.

You know, a (SOPA) bill in the United State presents a threat to the integrity and security and stability of the DNS. And I think that we may as volunteer members of multi-stakeholder body, be better positioned to raise that issue than almost anybody else in ICANN. I think it's very dangerous for example, for the staff to raise that. That's pretty dangerous even for the SSAC too.

But you know, this is just Mikey and his gang. They can pretty much say anything they want. And I think that there's some very important things that need to be said here.

And I'm getting a smile out of Wendy on that, so that's good. I like that.

Continuing on in this vein, there are other places to find vulnerabilities. And again, this - these aren't just technical vulnerabilities. These could be business processes, relationships with other entities, and this is again where we're going to have to work on some of this because this is presuming that we are a single entity having external relationships with other entities. And that's not quite computing for me. We have to (unintelligible) through that a little bit.

And then there's the security architecture stuff. And it's interesting to sort of think about DNS in the architecture kind of way.

I'm seeing I'm losing key people, so I'm going to push along here. In fact, we're getting into the weeds.

I think I'm going to stop. It's 22 after the hour. Everybody's really exhausted. It's tough to do much on Thursday because we're so tired.

But you know, I'll just turn the slides and let you know that there's a lot of good thought that's already been done for us in the methodology. And then to the scale thing (Ray), this is a good example.

The methodology has a scale for every single dimension in the 1 through 10 kind of thing, and this is an example of one for the vulnerability assessment.

So again, we even have pre-built scales that we can tailor. We don't have to start from scratch on that.

So at least I'm feeling pretty comfortable with the selection and the methodology and the place that it gives us to stand. And I think that even if we just did one pass through at tailoring, and a very high level pass through all of these buckets and cranked it into some tables, you know, we would've moved the ball forward quite a bit. And certainly, will have identified some places to go lots deeper.

I think there's one more slide. Yes, there's one - here's another - there's another scale for pervasiveness. The first one was severity. You know, there's no controls. It's just totally wide open all the way to, you know, you're totally tied down. And then the other is how pervasive is this vulnerability across the organization or organizations, depending on how you're doing this.

Well, that's the end of that deck. It's 23 after and we'll stop there and we'll have conversation until the bottom of the hour and wrap it up. Any reactions to all this? Anybody got any big stuff?

Russ, you want to...

Russ Mundy: I have to admit I've not looked carefully at this methodology. I have heard about it and have used something similar.

And one of the most challenging parts when you use one of these things is to get your mind wrapped around the fairly - as big a picture of it as you can see how the pieces fit together and understand what the specific terms - because the terms are incredibly important what they mean, how they assign.

So from a process and a mechanism and a way to go about it, I think it's good. Because I was in the meeting and I (think I see your point). And I think it's been huge progress and I - personally, I want to do more, but I'm going to have to try to carve some time out just to understand the specifics to be able to make a more useful contribution.

Mikey O'Connor: Well, anything and anywhere is helpful. You know, to any extent would be great. Thanks Russ.

Anybody else?

Going once.

Go ahead, (Don).

(Don): I've got one final question. How'd that Minnesota interview turn out?

Mikey O'Connor: Well, you know, Julie and I were talking about that not long ago there. And we were thinking that maybe we'd end the meeting in Minnesota. For You's who haven't ever heard that before, don't ya think? Do you want to join me on this here Julie?

Julie Hedlund: No.

Mikey O'Connor: No. She doesn't seem to want to. Well, we focused on a number of things in Minnesota. One, we do fishing in our boats. We eat toast on the boat there, you know.

How long you want me to go?

Okay gang, thanks a lot. Have a great trip home - oh wait. Wait. Wait.

Man: (Unintelligible).

Mikey O'Connor: No, that's fine. We're not out of time. We have plenty of time.

Woman: (Unintelligible).

Man: (Unintelligible).

Woman: (Unintelligible).

Man: So (unintelligible). I've got a question about you're going to make this sort of one organization methodology? You mentioned (unintelligible) but I don't understand what you're going to do to make this one organization methodology work on the Internet, right?

We're dealing with infrastructure that is - so it's not going to stay this pervasive. It's a cross-organizational boundary where you can't talk to the people on the other end of that connection. And it's the second part of that that I'm worried about.

Mikey O'Connor: That's a lovely question, and here's a first cut answer at it. Because I ran into a similar problem on a much smaller scale, but I've thought about this a bit.

Once upon a time I was doing a project for a 60 campus university coming up with a security strategy for them. And interestingly enough - I'm turning this mic so I can face you.

Man: (Unintelligible).

Mikey O'Connor: Or, I'll move down there so I don't have to - interestingly enough, Presidents of universities get a little cranky when you march into their office and say, "This is the way you're going to do stuff," because they're an independently cranky bunch. That was only 60. And what you're raising is the issue that what we're talking about here is hundreds of thousands - you know, if you take it all the way out to the edge, it's - pick a number. It's a very large number.

And I think that the strategic answer to that is that because we're at the core of a conversation, we're not the authority, we're not the cops you know, but we are a place where a lot of very interconnected people meet and exchange ideas and make policy and so on.

That in our report, and I'm previewing something for the rest of the task force because I haven't thought this through yet; that when we roll out our report, we need to be very clear about the difference between what happens in the core - what happens inside of ICANN and what happens at the edge.

And I think there are some really useful things that can happen at the core. I think we can develop models. I think we can develop examples. We can develop approaches to solving problems. But, we cannot do the security analysis - for example, for a ccTLD. We don't have the authority.

But what we can do is develop a bunch of tools and resources and helpers and stuff like that to help people at the edge actually deliver some of this stuff. And so it's that relationship boundary and that roles...

You know when I was talking in the earlier meeting about roles, responsibilities, accountabilities, I think that's important to define at least in the rough cut as a preliminary thing and then say to the community, "What do you think? Have we put too many things in the central basket? Should we put more things in there? Where are the really touchy ones?" And I think that's

part of our deliverable. That's part of our mission. Does that come at what you're talking about?

Because, I think it's incredibly important. It's really important. And I don't think that ICANN historically has done a very good job of making that clear and we get in trouble sometimes as a result of that.

So there's a rant. Now I have consumed all the time. It's - five, four, three, two, one. It is now the bottom of the hour. We're closed. I thank you all for coming and we'll see you in two weeks. I'm announcing that I'm not going to be on the calls next week, so I don't think we'll have any calls next week because I'm spending ten days here in Costa Rica (unintelligible).

Man: Awesome.

Mikey O'Connor: Thanks a lot. See you soon.

Woman: Thank you.

Mikey O'Connor: Nathalie if you're still with us, we're closed and thank you as always for your fabulous help, and I sure hope that they come up with a travel budget so you can come see this circus in person sometime. Thanks again.

Nathalie Peregrine: I'll vote for that. Thank you. Bye-bye.

END