Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
24 November 2011 at 14:00 UTC

Note: The following is the output of transcribing from an audio recording of the DNS Security and Stability Analysis Working Group (DSSA WG) teleconference on 24 November 2011 at 14:00 UTC. . Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. The audio is also available at:
http://audio.icann.org/gnso/gnso/dssa-20111124-en.mp3
On page: http://gnso.icann.org/calendar/#nov (transcripts and recordings are found on the calendar page)

Attendees on the call:

At Large Members
- Cheryl Langdon-Orr (ALAC)
- Olivier Crépin-Leblond (ALAC) (co-chair)

ccNSO Members
- Takayasu Matsuura, .jp
- Luis Diego Espinoza,.cr
- Ondrej Filip, .cz
- Katrina Sataki, .lv

NRO Members
- Carlos Martinez (LACNIC)

GNSO Members
- Mikey O'Connor – (CBUC) (co-chair)
- Rossella Mattioli – (NCSG)

ICANN Staff:
Bart Boswinkel
Nathalie Peregrine

Coordinator: We're now recording.

Nathalie Peregrine: Thank you, (Ricardo). Good morning, good afternoon, good evening. This is the DSSA call on the 24th of November. On the call today, we have Rosella Mattioli, Takayasu Matsuura, Luis Espinoza, Olivier Crepin-LeBlond, Mikey O'Connor, Cheryl Langdon-Orr and Ondrej Filip.

From staff, we have Bart Boswinkel and myself, Nathalie Peregrine. We also have apologies from John Levine, Jim Galvin, Scott McCormick, Greg Aaron, Nishal Goburdhan, Don Blumenthal and Rafik Dammak. I would like to remind you all to please state your name before speaking for transcription purposes. Thank you and now over to you.

Mikey O'Connor: Thanks, Nathalie, as always. Nathalie does this incredible job on setting up this really complicated Adobe Connect room. And as usual, it's perfect, thanks.

Oh, I guess we ought to do the SOI thing, especially since Cheryl just got off of the SOI call. So we'll take a moment and just see if anybody's statement of interest needs to be changed. Okay, you'll note that the agenda is identical to last week's agenda, but I'm happy to report that I think we're getting there.

And so while this is a slightly smaller group than normal because of the U.S. holiday, the Co-Chairs really wanted to run through a couple of things with you just to get a check on how this is progressing. And presuming that you give us the thumbs up, we'll probably repeat this just next week to get the eyes of the whole group on it. But I think we're going to be able to keep moving ahead, which is our big goal with all of this.

And Cheryl, I'm going to do this without sharing my desktop this time. Some time I'd like to experiment with you and there are some settings in the chat room, in the Adobe room, that I've changed and if we have time at the end of the call - this call may be a little bit short - I might want to just try an experiment to see what it does to the bandwidth - pardon me?

Cheryl Langdon-Orr: I'm happy to play.

Mikey O'Connor: Okay, new toys, you know, toys are good. Okay, so the first thing that I want to look at is this new version of the spreadsheet that's - this isn't the live one, so I can't demonstrate it live. But I think the trade-off is - in terms of bandwidth - is worth it.

So what you see in front of you is essentially the same spreadsheet that I sent to the list a few days ago, with a few changes. And - so from last week to this week - let me step through the changes from last week to this week. Last week, we basically just had you assessing priority.

And this week, what we've said is give us your opinion on the likelihood the impact of a threat and the effectiveness of the current control efforts. Thanks to all of you for contributing ideas on that. And as you can see, the way that the scoring is now set up, it's set up to drive extreme variation in the responses.

So in the first row is an example of a very low priority piece of work for us, badly chosen, because it's probably not. Physical threats actually tends to show up higher in our lists, so forget that. But you can see that if the likelihood is low, the impact is low and the effectiveness of control efforts is good.

Then - let's see if I can squeeze in - I can't quite - let me just - I'm going to make it a little bit more of an eye chart. I'll just go down a notch in terms of size, it makes it harder to see, but can you all read that, or is it...

Cheryl Langdon-Orr: Yeah, it looks like my normal screen.

Mikey O'Connor: Okay. So you can see sort of what's going on is that if your opinion is that things are not a big threat and the mitigation is good, then the score is very low. And if the threat is very likely, the impact is very high and the control efforts is bad, then we get a gigantic score. And then the last row is just an example of something in the middle.

I put in that big, bold note above all of that just now because this particular spreadsheet is really just designed to help us focus on what we're going to work on. I want to take you through the methodology a bit in a minute, and I think that the point that Luis is raising is the value of risk thing - is going to become clearer as we get into the methodology. But Luis, if you look down at the row that says weights, you'll see that a low score gets ten points for a likelihood an impact - maybe I'll go up one notch.

Now that you've seen those scores off on the side I think I'm going to come back up so that you - it's hard for even me to see this, so it's got to be impossible for you. But you can see down here at the bottom where it says weights - so what's going on is the low score is getting ten points in the likelihood column and then the three scores are being multiplied. That's how the arithmetic is being done here.

And Cheryl's raising the point, then you can risk assess using the weights. And that's where I put this sort of grouchy note up on the top, because as you'll see in a minute, when we dig into the NIST methodology, this doesn't - this is not terrible, but it's not really aligned with the methodology very well. And so what I don't want to have is a situation where the summary of this spreadsheet gets out in the wild and people start thinking that this is the result of our analysis.

This is really just being used to pick what we work on. And so I put that big disclaimer in there so that people wouldn't be confused about that. Yeah, as Cheryl was saying, this is just a filter, a tool, exactly.

To quote Cheryl's - I should really quote the exact thing that Cheryl posted in the chat. Hell no, this is just a filter tool, there we go. And so it's exactly right, maybe I'll steal those words when I revise this, because I, you know, what we're going to find is that the methodology that we're sort of zeroing in on has all these things in it but it organizes them slightly differently.

Now the other thing that I stole out of the methodology - and again, these are awfully small, so I think I'm going to go up one more notch - oh, oh, so that we can read these. These are out of - well, two of them are out of the NIST methodology, the National Institute of Standards and Technology is a U.S. government outfit that's - I don't know where they are housed. They might be in the Commerce Department.

And then as you can see on the right, there is the Mikey column, because I couldn't find that definition in the NIST methodology. But since I wrote these into the spreadsheet, I have - (Patrick) has pointed me at a much better document that describes the methodology and these definitions will undoubtedly become clear. So again, this is just the first cut to kind of give you a sense of what's going on in the tool.

And I don't want to belabor the language, because I think we're going to replace this with newer language from a newer document that I found. So I - that sort of concludes my tour of the document. I'll sort of shrink back down a little bit so you can see it all.

Cheryl Langdon-Orr: Mikey, it's Cheryl here.

Mikey O'Connor: Go ahead, Cheryl.

Cheryl Langdon-Orr: The only bit - and it might only be me reading the Mikey column and the review of the Mikey column will pick it up anyway - but I just don't want to lose the likelihoods in those final assessments. Let me use an example. We all know that if we use raw chicken on a surface and then prepare food that is, for example, a salad on that same raw surface, bad things can happen.

And that, in this particular system, would be running, you know, high risk, et cetera, et cetera.

Mikey O'Connor: Right.

Cheryl Langdon-Orr: But the actual - and the mechanisms are in place providing they are operated, they everything is okay. But you're still going to have this sort of likelihood issue of how likely is it for those mitigation mechanisms to be always or occasionally or rarely used. So there's sort of a - almost a swing or a seesaw swing somewhere in this system where sometimes really bad things are very unlikely to happen, but when they do, oopsie, and therefore they don't get tested often.

But, you know, you've still got to have that critical control in place, or simply be willing to risk them. And sometimes that's a decision, you just go, yeah, well it's going to happen and occasionally we'll have to deal with it. Or there's things that are really, really, really likely to happen and they're really, really bad and they're likely to happen a lot and you have to go all out and put those mitigations systems in.

In this case, you know, train people not to cut sandwiches on, you know, bloody boards. But when a sandwich is cut on a bloody board, oh dear, the results are really, really nasty. So there's that whole likelihood and risk balance that needs to be picked up as well.

Mikey O'Connor: So I have a question for you.

Cheryl Langdon-Orr: Yep.

Mikey O'Connor: We have likelihood of the risk, of the threat...

Cheryl Langdon-Orr: But not likelihood of the ability for the mitigation to be successful or used or whatever.

Mikey O'Connor: Yes, all right. So you're suggesting another column which says effectiveness of the controls, and then another column that's something on the lines of the likelihood that they are in place and consistently used.

Cheryl Langdon-Orr: Yep, I mean, you're not going to run - back to my chicken - Cheryl, for the transcript record. You're not going to run a standard that you would expect in a food service handling situation in a, you know, normal house.

Mikey O'Connor: Right.

Cheryl Langdon-Orr: And so in households, there you go, people get sick.

Mikey O'Connor: What a surprise. So the way that this is written now, we have the effectiveness but we don't have the likelihood dimension.

Cheryl Langdon-Orr: Yeah, just if it's possible. I mean, I'm...

((Crosstalk))

Mikey O'Connor: I think it is. No, no, the reason I - one of the reasons that I don't want to belabor this particular sheet is because it's only to be used to pick our focus. But when we get to the methods, which I'd like to push this along to in a minute, let's keep our eyes out for that. Because I think that what you're describing is something that is an enhancement to the methodology that we need not - we need to remember to stick in, which is easy to do.

And I think it's a really good one because you're right, you know, perfectly effective controls in a restaurant situation don't happen at home and people get sick. Well, the same thing could happen, perfectly effective controls in a very large organization are a lot less likely in a very small one, and...

Cheryl Langdon-Orr: They might actually be impractical or impossible.

Mikey O'Connor: Yeah, exactly. So I've typed it into the chat because you were busy describing it, and I will take that as a note to...

Cheryl Langdon-Orr: Thank you, kind sir.

Mikey O'Connor: ...add that as, at least mentally, as a column to this and let's keep our eyes on the methodology as that evolves. So that was a good one. Anybody else got any thoughts about that?

I don't think I'm going to change this sheet, because I just want a quick and dirty assessment. And I don't want to get stuck on this sheet because what's happening is this sheet is starting to turn into something that's competing with the methods, and the methods actually do a much better job than my lame, stupid spreadsheet. And so with your permission, Cheryl, I think I’m going to let people take a first cut just so we can pick our focus effort and then, you know, for sure we'll remember the issue that you've raised, because I think it's a really, really good one.

Anything else? I'm kind of anxious to get to the methodology because I think that this is going to help us a lot. Okay, well we can always come back to this, but let me show you something and get your reaction.

This is a document that is 85 pages long, and I plan to read every single word to you during the rest of the call, because I know that you'd be really interested in every single word in this document. And what the heck, I haven't got a whole lot of material, but maybe I'll skip that. I'm way back in the appendices of that document and I just want to run through a few of them with you.

Maybe before I do that, let me just update you. The Co-Chairs have been working pretty hard on this sort of unexpected extra project that we've encountered, which is to try and pick a methodology by which to evaluate threats and vulnerabilities. And I think it was on last week's general DSSA call that somebody mentioned that there was a comparison tool that compared a lot of methodologies out there.

And I'm not going to overwhelm your bandwidth, Cheryl, by sharing my screen, but I did go and run through that evaluation tool and found it pretty out of date. Many of the links are broken, many of the methods that are listed in there that were listed as free or open source are now behind pay walls. And so I got grumpy.

I didn't go through the whole - it evaluates about 20 methodologies and I didn't go through them all. But I found it fairly unhelpful and, you know, since our charter is not really to pick a methodology, our charter is just to evaluate threats. It's not even to evaluate vulnerabilities.

We've already expanded a little bit. I started pressuring the Co-Chairs a little bit on our call on Monday to sort of push through this. And the NIST methodology is out, it's open source, it's, I think, pretty good.

It's pretty well aligned with the work that we've done so far. And so I'm pushing just a little bit, and I'm perfectly willing to have people push back and say no, let's keep working this issue, but I think that the NIST methodology is good enough for what we need to do. And I want to give you a pretty detailed tour of some of the components that I've found and then get your reaction to that.

Because if it's good enough, I think we'll go ahead and use it and leave a formal security risk analysis, risk management methodology project to somebody else who's got that in their charter. Because we really don't have that in our charter and doing a full-blown selection on methodology could take us months and I'm conscious of the time, and so that's just a little bit of background. And if you feel like I'm pushing too hard, feel free to push back.

But with that, the NIST methodology, I think I took us through the high level of this last week. This document - I didn't have this document then, or I might have taken you through it then, but (Patrick) pointed me to it. NIST starts with threats and it says - and it's got all these nice tables that say well, here are sort of representative examples of threats which, you know, aligns pretty well with the taxonomy that we have - the structure that we've already built.

And I'd be inclined to do a little bit of minor editing to get our list aligned with this list, because I think then we get points in the wider world because our list is aligned with a generally recognized structure. And again, we don't need to resolve all this today, I just want to give you some hints as to things I'm thinking about.

So in the NIST world, there are really - I think just those four, let me just look forward here, yeah. This is the whole list. Let me shrink it just a little bit, see if you can read it. Is that readable still?

Cheryl Langdon-Orr: Yep.

Mikey O'Connor: Okay, so that's one, you know, that's sort of the threats layer. Not terribly different than the list that we came up with, and I, you know, I think - I haven't checked this, but I think almost all of the threats that we've identified fit in this taxonomy somewhere. And this one might even give us some ideas of ones that we've forgotten about, so that seemed like a useful discussion.

Then what the NIST methodology does is it talks about adversaries. You know, a threat is nothing until an adversary comes along and embodies that threat. And so what NIST tends to do is say okay, the first priority is how capable are the adversary?

Are they Mikey, in which case their capability is very low. The adversary has limited resources, expertise, intelligence, capability to walk and chew gum at the same time, all the way up to a very sophisticated threat that, you know, has lots of resources, lots of capabilities and so on. That seemed like an interesting conversation for us to have in a structured way.

Another dimension is this dimension of adversary intent, another interesting distinction. And you can see, Cheryl, why I'm quite keen on your idea of splitting the controls discussion, because what this methodology does is it splits some other things in really interesting ways that I think are useful discussions for us to have. And so your split seems like a really interesting and useful addition, and I'm not sure what we're going to find when we get down to vulnerability control stuff, whether they have already made that distinction or not, we'll find that out in a minute when we get there.

So anyway, there's adversary intent and then there's targeting. Again, another interesting distinction that - you know, is it a very targeted attack or is it sort of at the very other end of a super scattershot thing. So if we thought about something like DDoS, suppose that the DDoS attack was just targeted at a critical resource, that would be one extreme.

If the DDoS attack was basically targeting everything and it was just bringing down the Internet in general, that would be a different kind of thing. So again, I thought that was a really useful and interesting distinction. And then they point out that some threat sources are non-adversarial. So, for example, a...

Cheryl Langdon-Orr: Yep, good.

Mikey O'Connor: A storm or a natural disaster or something like that is not an adversarial threat but it's, you know, we still need to think about the effects of that. And so there's a different assessment scale for those kinds of threats. And let's see, I think this is just - some of these are just suggested tables.

So then we get to threat events, and I need to take another pause. In the NIST methodology - let me zoom in on this, it's a little easier to read that way

- that's a little too much, let me come back one, there we go. We are skipping this - not consciously, we didn't know about this.

But in the NIST world, what they do is they say start at the very highest level, the organizational level, and essentially do an analysis. Then go down a level in the organization and conduct the analysis again with different people, essentially the middle management tier. And then go to the bottom level, which is the front line people, and conduct the analysis a third time.

I think one of the things we may want to do when we write our report is leave behind a list of things that we didn't do that might be a pretty good idea. I don't want to go back and re-charter us, and that's what this would require. But I think it's not a bad idea for an ongoing threat management process to use.

And what we can do is we can say, well we did it the first time and we found a bunch of things that if we had it to do over again, we would do. But I'm - personally, I haven't checked this out with my Co-Chairs - I'm not personally keen on the idea of actually trying to step back and recruit three different groups of people to go talk to and so on. But that's one that I'd be interested in your reactions to.

Because what we could do is we could interview people at these three different levels and essentially conduct the full-blown thing. It's just that, again, I'm conscious of time and I'm not sure that we have that much time. And so that's one to think about.

So then they just have a bunch of adversarial threat events. Now, you know, this is a subdividing of threats. We combine - we have a mix of these in our list.

And I have to learn - I am sort of like the college professor that’s one chapter ahead of the class. I need to read this methodology more carefully. I don’t quite understand the distinction between these two kinds of things quite yet. So I need to get better at that.

But they do have a pretty good list of things from both adversarial and then as we go on down the list, you know, I mean it's quite a substantial list of things. You can see it goes on and on and on which I find I actually quite like because it makes me...

Cheryl Langdon-Orr: It gets into the weeds.

Mikey O'Connor: It gets into the weeds. But the nice thing is we could poll for example and say which of this huge list of things do we care about and thin it out and know that we haven't missed anything.

The nice thing about this is that I feel a lot more comfortable that if we went through our - if we went through this list we could come back to the community with a pretty good case that says well we sure looked at a lot of them. We may have missed a few. But we looked at a bunch of things cause, you know, we're still in adversarial threats here.

And then finally we get to non-adversarial threats. And, you know, this is, you know, earthquake, fire, flood, you know, two flavors of flood, two flavors of hurricane, accidental things from users and so on and so forth.

And I think that if we could go through these lists and find the ones that really are likely to have a big impact on the DNS we would have done a good thing for the community. But we wouldn't have to weed through a bunch of stuff that as you say is pretty detailed. But I am a weeds detail kind of guy.

So anyway, you know, you can then see that - where things...

Cheryl Langdon-Orr: (Unintelligible) Table E4.

Mikey O'Connor: Pardon me?

Cheryl Langdon-Orr: I'm getting excited at Table E4, Mikey. Just so you know now we're getting...

Mikey O'Connor: Okay.

Cheryl Langdon-Orr: To relevance.

Mikey O'Connor: Yeah. Yeah.

Cheryl Langdon-Orr: I'm getting excited with relevance opportunities here.

Mikey O'Connor: Yeah, exactly. Well see that's the thing that I like about this methodology is that it feels like they've - they're thinking pretty much the way we are and...

Cheryl Langdon-Orr: Yeah.

Mikey O'Connor: Unlike some of the methodologies I've read which don't feel like that at all, like the OCTAVE one. I went in to a - I...

Cheryl Langdon-Orr: I...

Mikey O'Connor: Analyzed that pretty carefully and...

Cheryl Langdon-Orr: Because it...

Mikey O'Connor: Just...

Cheryl Langdon-Orr: (Unintelligible).

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: I'm excited.

Mikey O'Connor: Okay. Let me push the pace because as you can tell there's a lot of material. What I thought I would do is introduce you - this to you on the call and then send the link to this 85-page document so that you can all have it.

Cheryl Langdon-Orr: Oh please do. Yes. Okay, pop quiz next week following.

Mikey O'Connor: Yeah, pop quiz. There will be a test.

So now we're into vulnerabilities. And again here's the Tier 1, 2, 3 thing. They always start with that.

But then they talk about the severity of a vulnerability. Fine, I get that. But this is the - this is where we start to get back to the control stuff that you're interested in, Cheryl.

This isn't the issue that you raised. But they do start to slice the control issue fairly - in fairly interesting ways in this part of the methodology.

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: So then there's this taxonomy of predisposing conditions. And I have to admit that I don't quite get what this one is yet. But I will be smarter in a week cause I haven't really had a chance to read through the whole methodology myself yet.

But you can see that again there are interesting lists of things for us to consider once I figure out what they mean. And again they're pretty detailed.

Here's another pervasiveness one, you know, to - and so I think that what this starts to look like to me is a series of worksheets kind of like the very sketchy one that I've sort of walked us through at the beginning of the call. And they put this in a sequence that there's a very long description of how to do this. So it's not like we're having to invent this methodology.

Here's the likelihood scale, again Tier 1, 2, 3. And, you know, there are the adversarial and the non-adversarial. You know?

And again this is the ones that are, you know, now we're - the bottom of the page shows one that's - for those of you who are listening to this transcript maybe I should say the names of the tables so you can follow along. This is Table T4.

It talks about if, you know, the difference between the likelihood of the threat event and the likelihood that that event would result in a bad thing, an adverse impact.

Cheryl Langdon-Orr: It is my chicken.

Mikey O'Connor: It is your chicken. But it's not quite - it's not the issue that you're talking about. You know? I think what you're raising is maybe another scale like...

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: These...

Cheryl Langdon-Orr: Yes. That's...

Mikey O'Connor: Because...

Cheryl Langdon-Orr: Yeah, further on. But the fact that this is identifying the chicken is the problem and leaving the crap on the board is the issue.

Mikey O'Connor: Yes, exactly.

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: So then there's an overall, you know, again I don't want to go into it in a lot of detail on this cause I'd be making things up that I don't know much about yet. But you can - this is sort of reading along.

These are the harms. This is the impacts things. And they have operations, assets, individuals.

And we might have to modify this a little bit because now we are getting - until we get down to the harm to the nation - and remember this is a federal government document -- we would - we may have to do some work on this harms to align it with the circumstance that we're in where we're really dealing with a worldwide resource.

And we're dealing with a bunch of different organizations. Again this is where the kind of organizational view starts to creep in because our mission is not to evaluate this for ICANN. This is - our mission is to evaluate it for the world and the respective organizations that participate in that. So we've got a little work to do here.

Oh (Luis) is having trouble. Every - is everybody else able to see what I'm seeing or does everybody...

Woman: It's there.

Mikey O'Connor: Have a blank screen? Tell you what. Let me re-share it. Before - (Luis), before you go off let me just re-share this document and see if that brings your screen back. Maybe it will. That would save you all the thrash of having to - did that bring it back for you, (Luis)?

Black. No. I think you may have to reconnect now.

Cheryl Langdon-Orr: Yeah. It only - it goes through black as it's loading.

Mikey O'Connor: Oh. Are you on a fairly slow connection, (Luis), because if you are I could - instead of paging incrementally I could page one chunk at a time? That would not force your screen to refresh so much. That might be a good thing to do.

Too many toys at home, aha. (Luis) may have - well let's - let me try paging down a page at a time instead of incremental.

Cheryl Langdon-Orr: I'm only watching a few movies.

Mikey O'Connor: Yeah. Well I have all of my kids at home. And I admonished them that they had to stay off the internet while this call was on so. Anyway let me keep going forward.

Another one that they've got is the impact. I mean you can see that there are all these - it seems to me that this is a series of choices that a group of people make in a sequence.

And I think we're the group of people. And I think what we do is we just sort of bash through these in whatever order they tell us to do it in. And at the end what we wind up with is this very elaborate version of a spreadsheet that's like the one that I showed you a minute ago with much more detail in terms of which threats, etcetera, etcetera.

So let me stop -- I think that's enough of an introduction to this and besides it's probably driving (Luis) crazy to see his screen go black all the time -- and step back and get your reactions to this. Does this seem like the right direction to go?

I mean I apologize for not being more articulate about how this actually works. But I really just started reading this document a couple of days ago.

And I don't want to wait months to get through a selection of a methodology. And so if this seems close enough at least on first reading I'd like to get that sense from you.

And if in fact this bothers you or you have concerns about it I really want to hear about that because if it's got something that's very bad that we want to avoid then I'll keep looking for other methodologies. But if this seems close enough then I might pause and spend the next week sort of learning this methodology and coming back to you with a better summary of it than the unbelievable detail that I put on the screen today.

So thoughts, reactions? Olivier, go ahead.

Olivier Crepin-LeBlond: Thanks very much, Mikey. Just a couple of questions on this or comments actually.

First I think the methodology is absolutely fantastic. It looks as though it's very deep and it certainly seems to be very thorough.

The concern I have is the amount of time that such a methodology might take for each one of the threats, etcetera, that we're assessing and whether this really isn't in some way the blueprint for a tool to be used and just think it has all the flavor of an actual tool that they would be designing. And I'd - I'm just concerned doing it by hand how long that would take.

I might be wrong. It might be due to my total ignorance on this specific tool. But I just wonder. Thank you.

Mikey O'Connor: You've raised two really good points. So I'm going to name them so that I don't forget.

The first is the process by which we would evaluate threats. And the way that I in my ignorance have been steering us I think is wrong. And I'll come back to that in a minute. And the second is the question of tools.

So let me go back to the first one. What I've been steering us towards is a threat by a threat analysis. And what this tool is presuming is that you evaluate all of them at the same time.

And so what you do is you take that giant list of threats that we've got and mash it up against the list that they've got, make sure that we haven't missed any. And then you evaluate them all at once sort of the way that that spreadsheet that I built does it. And we'd say okay these threats are the ones that we're very concerned about, these vulnerabilities are the ones that are likely to have big impacts. So instead of doing it one threat at a time which is the way I've been steering us we would do it across the whole landscape at the same time.

Does that make sense to you? Did I describe that well enough that it makes sense because I think that shortens the amount of time a lot?

I think if we go threat by threat you're right, we'd probably be at this for a really long time. And that's a point that I was going to make but forgot. So...

Olivier Crepin-LeBlond: Okay.

Mikey O'Connor: Does that - I mean I'm very uncomfortable with my ability to describe all this stuff because I'm pretty new to this methodology. And so if I've done a bad job of describing it please say so and I'll try again.

And then the second thing is that I'm pretty good at bashing out Excel-spreadsheet-based tools in a hurry. You know? If we were to say okay we're going to take, you know, let's just take the one that's on the screen right here. This is Table I-2. And we're going to take all of our, you know, we're going to take something. I don't know what the list would be but we're going to apply this scale to it. It's pretty easy for me to bash out a spreadsheet that we could use to do that in an afternoon.

And if we were to build this tool sort of a chunk at a time like that I'm pretty confident I could stay ahead of the group on that. If you asked me to do the whole tool at once I'd probably have to pull a few all-nighters to get it done. But I think I could even do that.

So I think at the end what we might have is something that would be pretty useful for ICANN in general. And I'm perfectly happy to sort of build those and let you all sort of help me, you know, refine them till they're right.

And the other thing is that you're right, this is a tool. And one of the things that I'm trying to find is whether anybody's already built this because it seems to me that it would be so obvious that somebody built a whole series of spreadsheets and worksheets. And it may already be out there. So I'm also sort of thinking about pursuing that. But those are both really important points.

So did I - what's your reaction to all that ramble, Olivier?

Olivier Crepin-LeBlond: Thanks, Mikey. Olivier for the transcript. As I've just written in the chat the - any tools in the public domain, we're not sure, who knows, hopefully, maybe. I just wondered if it might not just be available for a fee somewhere. I'm sure someone sells tools that follow this methodology. But if you're able...

Mikey O'Connor: Well...

Olivier Crepin-LeBlond: To put together a spreadsheet that does that then I would certainly be - I'd concur that it would be very helpful for - not only for this working group but also for ICANN.

Mikey O'Connor: Yeah. I think - one of the...

Olivier Crepin-LeBlond: It would be great.

Mikey O'Connor: One of the advantages to building our own is that then we could publish it on our email list and we could publish it out on our wiki and it would be something that's out in the world.

I really jump back when we have to use a proprietary methodology because suddenly we can't share it, you know, we can't use it in our usual open...

Olivier Crepin-LeBlond: Yeah.

Mikey O'Connor: And transparent way. And so I'm pretty reluctant to do that.

But one of the things that you haven't seen in this document because I didn't take you through the first part is that this document is very recent. This was published in September of this year. And it's draft. And you'll see that when you get it. It's - every page higher in the document has draft stamped all over it.

And it may just be that it's so new that the tools haven't been built yet. But I know people at NIST back when I ran the quality function at the University of Minnesota and I was involved in the quality management part. And I'm going to try and reach out to some of those folks and see if there is a tool that backs this up cause if there is one that would also be in the public domain and we could use that. And it would save a lot of work.

Cheryl, go ahead.

Cheryl Langdon-Orr: I - thanks, Mikey. Cheryl for the transcript record. I know you've picked up on a whole lot of points so I don't - there's a whole lot I don't need to say, not the least of which is it's always dangerous when you start looking at particular threats in isolation or just in the vectors that they exist in as opposed to more like a full-blown disaster exercise cause quite often what happens is some of the simplest things actually become some of the more catastrophic when it's actually tested. So I don't need to go through that.

I know you're talking this as a tool. But I'm excited about it as a well-established system that we can customize into a purpose-built tool for our needs because we're not looking at national security here. We're looking at something slightly more (unintelligible) that.

Mikey O'Connor: Right.

Cheryl Langdon-Orr: And we are working with a - an internet that's particularly good under normal circumstances at finding workarounds. And a lot of these things, the concept of workaround just isn't going to be in it.

So it may need to be customized a bit. But I like where it's heading. And I think if we can just hunt out the bits that are going to be right for our work it would be a very good basis indeed. Thanks, Mikey.

Mikey O'Connor: Thanks, Cheryl. I think that's - that customizing notion I think is very important.

The thing I like to do is take an existing thing, either an existing system or an existing methodology, and cut out the irrelevant bits and enhance the bits where it sort of misses the mark and, you know, leave that behind.

I think that would be a pretty significant deliverable of this working group that, you know, we could leave behind for subsequent either working groups or, you know, the - there's this possibility that there's some sort of ongoing risk management function. I think we could leave a pretty good body of work behind for those sorts of people that's tailored really to - it - I don't think it needs a lot of tailoring to fit us pretty well. But, you know, clearly this business of everything referring to the nation needs to get changed and stuff like that.

And, you know, I think that if we were to sort of take this in sort of a series of waves where we'd go through - the methodology does lay out a series of steps that we go through. And I think if we walked our way through these steps we could build the tool as we went and at the end have a pretty good work plan, a pretty good series of tools to record the information and a pretty credible first-round assessment of the situation. So I was pretty keen when I saw this one.

Cheryl Langdon-Orr: (Unintelligible) Cheryl for the record. I just wondered whether or not we might also have the opportunity of taking whatever gets tweaked out of this by the group and asking some, you know, actual real-world people to apply it.

Mikey O'Connor: Yeah. Well I - one of the nice things about building our own is that we can then publish it out in the world and do just that, encourage people to use the same tool on their own. You know, for example it, you know, that's not in our - well a lot of this isn't in our charter; it's just a byproduct of the work that we have to do.

But this might be a very useful tool for especially a smaller organization, a smaller registrar, a smaller registry that doesn't have access to, you know, the - I mean I'm sure that all the big accounting firms have tools like this and, you know, for a substantial fee will come in and do this kind of assessment. But for a smaller organization that doesn't have that kind of resources available this might turn into a useful framework for them to apply to themselves.

Okay. Well I didn't hear any violent howls of protest so I think what I'll do is I'll keep reading. I have a nice holiday week coming up. And I'll send this out to the list, the link.

And we're not going to send the document. It's pretty long. So I don't want to send it by email. But the link is out there. And we'll learn together.

And that's sort of what I had for today. Oh and it's four minutes to the hour. So...

Cheryl Langdon-Orr: Yes. That's (unintelligible).

Mikey O'Connor: SP800-31-Rev1-ipd, that's the one. Rosella's got the link in the chat. Way to go, Rosella.

Cheryl Langdon-Orr: Thanks, Rosella.

Mikey O'Connor: Yeah. That's the NIST site. Yeah. That's it. That's the document.

So you guys can get a head start. I'll immediately publish the link to the list too. And we'll carry on.

Cheryl Langdon-Orr: Thanks, Mikey.

Mikey O'Connor: Yeah, great. Sounds like we're perking along.

Have a great day. And I'll see you in a week. Now I'm going to go eat turkey. And we're - and Olivier's going to go get his best friend married off so we've got a lot going on here.

Cheryl Langdon-Orr: You two all enjoy your day. And thanks to everyone else as well actually. I thought we got a long way on today's call. I'm - I don't often end these calls smiling seeing as it's 2:00 am. But...

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: I am smiling, Mikey. Mikey, you've made me smile.

Mikey O'Connor: Oh well that's great. That's a good goal to have.

Cheryl Langdon-Orr: Happy Thanksgiving, my dear.

Mikey O'Connor: Okay. See you all. Take care.

Man: Okay. Bye-bye.

((Crosstalk))

Man: Goodbye.

Woman: (Unintelligible) you may now stop the recording. Thank you.

END