Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
17 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 17 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-20111117-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
• Katrina Sataki, .lv
• Luis Diego Espinoza,.cr
• Ondrej Filip, .cz
• Jacques Latour, .ca

GNSO Members
• Mikey O'Connor – (CBUC) (co-chair)
• Rossella Mattioli – (NCSG) – on adobe connect
• Don Blumenthal – (RySG)
•Scott McCormick (IPC)

ICANN Staff:
Patrick Jones
Julie Hedlund
Glen de St Gery
Bart Boswinkel
Nathalie Peregrine

Apologies:
Rafik Dammak, GNSO
Rick Wilhelm, Network Solutions

Jim Galvin (SSAC) Forest Rosen GNSO
Carlos Martinez (LACNIC)
Greg Aaron – (RySG)
Joerg Schweiger.de (co chair)
Mohamed El Bashir (At-Large)
Nishal Goburdhan (NRO)
Mark Kosters (co chair) (NRO)
Keith Drazek – (RySG)
John Levine – (At-Large)
Otmar Lendl, .at
Patrick Vande Walle – (At-Large)
Chris Wright, .au
George Asare-Sakyi – (NCSG)
Adam Palmer – (CBUC)
Andrew de la Haye (NRO Member) - for the next 4 weeks
David Conrad (SSAC)
Andre Thompson (At-Large)
Wim Degezelle, CENTR
Edmon Chung (ALAC)
Arturo Servin (LACNIC)
Sean Copeland, .vi

Man: ...me okay?

Mikey O'Connor: Yes, I can hear you fine. Are you using your PC microphone?

Man: A hundred percent, yes.

Mikey O'Connor: Oh, this is turning out just fine. Well, Nathalie gets a gold star for pulling together all this stuff, so we should all bow to Nathalie because she got this running and it's working perfect.

Nathalie Peregrine: The (Caldor) informs me that the recordings have started, so I'll do a quick roll call, then. Good morning, good afternoon, good evening. This is the (desit) call on the 17th of November.

On the call today we have Rosella Mattioli, Cheryl Langdon-Orr, Mikey O'Connor, Scott McCormick, Katrina Sataki, Matsuura Takayasu and Jacques Latour.

From staff we have Glen DeSaintgery, Patrick Jones, Bart Boswinkel, Julie Hedlund and myself, Nathalie Peregrine.

We also have apologies from Rick Wilhelm and Rafik Dammak. I would like to remind you all to please state your name before speaking for transcription purposes.

And please also remember to mute your phone or PC microphone when not speaking in order to avoid any background noise. Thank you very much and over to you, Mikey.

Mikey O'Connor: Thanks, Nathalie. Don Blumenthal just typed into the chat that he's here, too, so, well, we've got a whole bunch of people coming in.

Welcome, all, to this call. Our first item, as usual, is to just take a moment to see if anybody needs to tell us about a change to their Statement of Interest. Okay.

We have pretty much the same agenda we had last time. And so I think we'll just dive right in. I'm going to share my screen because I have the results of the poll and it came so late that I haven't sent this file to the list yet, but I will momentarily.

Oh, there it comes. And let me give you a guided tour of what this means. The - what you see on your screen is the eight or nine folks who filled out their questionnaire. Thank you to you all.

And then listed underneath are the number of votes that they gave for each of those threats. It turns out that doing it by ranking and doing it by votes

amounts to the same thing and I found it easier to understand the texture by actually looking at the number of votes.

So that's what you have on your screen. Let me give you the quick summary interpretation. If you look to the right side of the screen, there are sort of two kinds of analysis.

The first one is I simply added up the number of votes and ranked the threats based on the votes across the whole group. And so the way to read that is that Row 11, DDoS is ranked number one and Row 15 is ranked ninth, so the others are sort of in rank order according to that.

So one approach to this is, you know, there's our answer. But then you also need to look at the far right...

Nathalie Peregrine: Mikey, I'm sorry to interrupt you. This is Nathalie. I think we're having problems seeing what you're sharing on Adobe.

Mikey O'Connor: Oh.

Nathalie Peregrine: I think quite a few participants are getting a dark screen, as am I.

Mikey O'Connor: Oh, that's interesting. Let me see what's happening here. Zoom. What do you see now?

Woman: Give him a shiny new toy and he makes it dark for the rest of us.

Mikey O'Connor: I'm sorry.

Nathalie Peregrine: There we go, we see the threat screen.

Mikey O'Connor: Yes, okay, so I was wondering why it popped up so nicely on my screen. Something changed just a little bit in the way Adobe behaves. Now can you see it okay?

Nathalie Peregrine: Yes, it's perfect now.

Mikey O'Connor: Oh, good. Sorry about that. Well, I'm not going to repeat that, I think it's fairly straightforward. Those are your votes and the ranking and then the last thing on the far right is a ranking by standard deviation, which means a ranking by dispersion in our views.

And what that means is that the largest dispersion, the largest, if you will, differences of opinion, come in Row 9, Physical Events. Some people feel that that's very important and some people feel that it's not important at all.

And so what we've got is a fairly clear result in some areas. For example, Row 15, Email Server Hopping, we are very much in agreement that that's a pretty low priority threat. It ranks very low and it's also our highest level of agreement, if you will, in the far right column.

But we do have some conversations to have and I think what we'll do today is focus on some of the threats where we have a fairly high level of differences of opinion so that we can take a moment to sort of understand why people felt the way they felt and see if we can persuade each other one way or the other.

The problem with just using the number of votes or the average is that that's not a very good basis for consensus. That's essentially majority rules and what would be nice is to understand a little bit more about where we differ and see if we can move ourselves in one direction or the other on that.

So with that I'm going to just throw it open for a minute to the group for reactions to see what you think of this, see if there are any surprises for you, etcetera, etcetera. Any immediate reactions to this before we dig in a little bit?

Don't all speak at once. I am interested in a conversation. Let's dig into some of the high dispersion ones. So let's talk about the Natural Disaster Physical Event Threat for awhile and hear some opinions on why people feel strongly either way because I think that we can't leave it this diverse. We need to educate each other, inform each other, etcetera. So (Olivier), go ahead.

(Olivier): Thank you very much, Mikey. (Olivier) for the transcript. I think it relates down to the individual experience of each person. Those people that have experienced a natural disaster do find it very disruptive. Those people that have not, have seen it on TV and might not find it as disruptive as it actually is. Thank you.

Mikey O'Connor: Oh, that's an interesting observation. Yes, that could well be. Other thoughts on that? How do we go about resolving that? Do we have any of the folks who ranked it as a pretty low priority on the call? I'm looking for Greg, no. Joerg, no. (Olivier), you ranked this pretty low. Are you essentially agreeing that maybe it could get a few more votes in your view?

(Olivier): Thank you, Mikey, (Olivier) for the transcript. Well, the question was really, I think it's kind of related to my comment which I made on the list. Agree - admittedly, it was the comment on the Chair's list, which was that the significance and the likeliness, I think, was it?

Mikey O'Connor: Yes, you had the word impact.

(Olivier): The impact.

Mikey O'Connor: Yes, impact and likelihood I think were the two.

(Olivier): Yes. And so the likelihood of a natural disaster is rather low, the impact is rather high. So how do you then relate this to everything else? So the way that I saw it as, what was the likelihood of a natural disaster compared to the likelihood of something else like, you know, I don't know, Denial of Service attacks and so on? And there certainly are a lot more Denial of Service Attacks around than natural disasters.

Mikey O'Connor: Ah, this is a flaw in my methodology. Oh, that's a good one. Okay, so I'm going to just briefly take a detour into the methods discussion and then we'll come back to this.

One of the things that I did over the week was I broke apart a couple of the methodologies that we've identified as possible ways to do our analysis. And in both of those methodologies the question of likelihood and impact come up.

And so maybe the best way to handle this is to acknowledge that the next time we do this survey we need to accommodate those two dimensions. And in fact, both of the methodologies that I tore apart do that.

And so that's, I think, a really, really good - I think what I would say is that's a good critique of this approach to doing this. And I'm going to file that away as a to-do. The next time I do this, set this poll up, I'll set it up with at least two and maybe several cells per threat so that people can at least put in likelihood and impact.

And there may be one more, I can't remember, from some of the methodologies I saw. So that's a really good observation, (Olivier). And that might, in one single stroke, explain that dispersion.

Any other observations on that particular row? Okay, let's take a look at the next row, which is Row 10, which talks about Fragmentation of the Root and

purely by voting we ranked it pretty low. We ranked it 8th of our 9 threats, but that was our second most diverse series of answers.

And again, I'd like to hear, much like (Olivier) commented on the last one, why some of us have pretty low, you know, (Olivier), Mikey have pretty low numbers on that and others, Katrina, Greg Aaron, Joerg, Rafik, have pretty high numbers.

Again, is that because of likelihood? And does (Olivier)'s issue sort of explain that diversity as well? I have to admit that in some cases I just didn't know. And so things I didn't know much about I tended to rank lower than things I did know about, so part of it may be knowledge as well. I tend - having worked with Greg Aaron on other projects like this, I tend to follow his lead a lot of times and I was surprised at how high he ranked this.

And so I wish he were on the call so he could explain a little bit more. And I guess the question to the group is, is this so invalid that rather than trying to make a decision from this one, should I redo it and send a new version out and let people do at least two numbers per cell here? (Olivier), go ahead. Oh, (Olivier) just blipped in and out.

(Olivier): Thank you, Mikey. Yes, it's just because someone keeps on clicking the mics and saying, "Yes, please give the mic to this gentleman." So then I revert back to the everyone having a mic thing.

Mikey O'Connor: Okay.

(Olivier): Somebody has to keep their fingers off their mouse. No pun intended on that one. With regards to the fragmentation of the root, I can explain my reason for ranking it low. Maybe others could explain their reason if they've ranked it low or high.

My reason for ranking it low is primarily due to the recurrent theme of immediate death of the 'net predicted through Fragmentation of the Root, alternate route, etcetera.

And having been around for awhile, we've seen so many alternative routes come up and crash and have seen none of that, no alternate routes actually gaining any significant traction. So it could just be being cynical about it and

thinking, "Yes, yes, we've heard it all before," type thing, at least for me, that's my reason, thank you.

Mikey O'Connor: I'm going to try and channel Greg Aaron, which is a bad idea, because Greg Aaron is way smarter about this stuff than me, but I think that he's probably less concerned about the alternate routes and more concerned about things like the U.S. government doing something really stupid in terms of legislation or the kind of blocking that was going on, say in Egypt during the turmoil there.

I think that's the kind of issue that this may have spoken to Greg about. And we have seen some examples of that fairly recently. Yes, that's true, Row 8 is - it's true, (Olivier) in that if you look at Greg's answer he ranked that extremely high.

He gave that one eight votes. So, you know, it may be that he's conflating these two things. And Patrick is agreeing in terms of Protect IP and now this new one, I forgot the name of it.

It's, yes, SOPA or whatever. So I would be - I would be open to discussion as to sort of where we go from here. Let's see, oh, Don's got his hand up. Go ahead, Don. Oh, you may be muted at this point, still can't hear you, Don.

Jacques Latour: Hello?

Mikey O'Connor: There we go, I hear somebody.

Jacques Latour: Can you hear me?

Mikey O'Connor: Jacques, hang on a minute, I'm sort of waiting for Don to chime in. Don, are you on? Well, you probably can't - well, you can do, yes, way to go, Don, you're typing. Are you on a phone or you on your computer speaker? We'll let Don - we're ironing out kinks of a new approach here, so bear with us, folks. While Don is typing, Jacques, why don't you go ahead, because I could hear you?

Jacques Latour: Okay. You can hear me okay?

Mikey O'Connor: Yes, I can hear you fine.

Jacques Latour: When we do this kind of work at CIRA, we look at the threat, the impact of a threat, very high, high, moderate, low. We assess that based on that criteria. We assess it on the probability of the risk happening, very low, high, you know, very high.

And then we build a matrix of, you know, impact versus probability, (which is work) on what the risk is based on, you know, this is high impact, but low probability, meaning it's less important than something that's very high impact and very high probability.

Mikey O'Connor: You know, I think that this has been incredibly valuable and as the fellow that created the spreadsheet, I'm really keen on the idea of if you all are willing to put up with doing this again, essentially presenting you the same series of choices but instead of one choice putting two into each cell.

And I'm not sure - I'm not sure that it makes sense to put them in pairs. See, what this methodology does is it forces you to compare each thing to the other.

Another approach would be to just take the list of threats and give you two cells for each threat and say, you know, what's the impact and what's the probability and fill out the matrix that way.

What are people's reactions to that? Does that drive you crazy? Is - because it would be easy to do; I could turn out a new spreadsheet today and push it out to the list and we could take another run at it.

One of the nice things about that is that that drops really well into both of the methodologies that I've reviewed and so it wouldn't be wasted work; it would probably be a first try. We would undoubtedly have to circle back and iterate a bit but it would I think be a really good first step.

Olivier is saying he's okay. Rosella is saying it's okay. Jacques, go ahead.

Jacques Latour: Well I have a (complete) spreadsheet that I can give you that are risk - we have a risk management office. We can give you a template and you can start from there. Because I think it builds all the (unintelligible).

Mikey O'Connor: Oh that would be lovely. I'd do that in a heartbeat. Yes please.

((Crosstalk))

Mikey O'Connor: That would be great. Okay I think let's do that. I think this was a nice exercise. It confirmed that we're all fairly concerned about DDoS attacks. It taught us that we need to split this question in two. I think we learned a lot about some other things. Go ahead, Cheryl.

Cheryl Langdon-Orr: Thank you, Mikey. Cheryl for the transcript record. I also I just wanted to point out something I put in chat and that is with any of the methodologies there's the human factor. For example I tend to rank things at - in terms of threats at the likelihood of the risk of them being a meaningful threat.

That may not however translate to - even though it's a critical issue - that the critical issue is at so far when tested in reality managed well and hasn't had a bad outcome. And that's where things like natural disasters would be ranked very highly by me and so far so good they've all been managed really, really well.

But should they not be managed really, really well it is a critical control point which needs - it's worth looking at. So we need to find something that's sort of effective in that or limits our choices on we are not only ranking threats, for example, above or below each other but in their effect as, you know, as well as in their risk or not in effect and only on their risk. So there's other tweaking to do and now...

((Crosstalk))

Mikey O'Connor: Yes and that too plays right into the methodology discussion. So I think that it would be useful for us to change gears for just a minute and switch over to methods. I'm going to take Jacques up on his template. But I want to share with you what I learned as I decomposed a couple of the methodologies where - I mean, some of the methodologies are proprietary but some aren't. And those that weren't I found pretty interesting.

So let me mumble for a minute in honor of Cheryl. See if this time I can get it on the screen. So can you see that okay? Well it's pretty small but, I mean, you can see my screen, correct? Okay, thanks Cheryl.

I took a look at two of the methodologies that we identified before. Let me clean this up a little bit, make it a little bit bigger. And I'm going to very quickly take you on a tour through this. I will post this as always to the wiki so that you can review it at your leisure.

The two that I took a look at are the - a methodology that's fairly old from the National Institute of Standards here in the USA. And another one called OCTAVE which comes from the big systems research center at Carnegie Melon University. So me just show you at very high speed what I learned. And let me make this a little bigger.

So in the NIST world they break their methodology into two big pieces; risk assessment and risk mitigation. And this is the methodology that - you remember that graphic that I built for our conversation with the folks in Dakar - this is the methodology that I built that little graphic around.

And what we are really working on is these two. But then Cheryl, your point is right here; it's sort of next in the process this whole business of control points and planned controls.

Then we get to likelihood, a theme that we've heard in the first half of this call, and impact. So this conversation seems to be playing fairly nicely into this methodology.

You know, once - and the methodology is I think detailed enough that we can sort of do it on our own; I don't think we need big fancy experts to help us do this. The write-up that's in the URL is pretty clear. And I think that we can figure out how to do this.

And the - sort of the endpoints again plays right into the point that Cheryl made which is okay if we stick with the natural disaster one, you know, what are the critical control points and what are the issues that happen if those aren't addressed?

The part of the methodology that I think is outside of our scope is the what do you do about this. You know, we - in our charter we have a gentle point that says that we can go out and take a look at these controls and if we find gaps we can make recommendations about what to do.

But the focus of our charter really falls up in this series of steps. So just take a quick pause on that and we'll go back to this in a minute.

The OCTAVE methodology I was less taken with. Basically what the OCTAVE methodology does is it's focused on assets, it's focused on systems or servers or devices or processes. And it doesn't match very well with the work that we've done so far. And it also didn't feel as comfortable to me.

Because essentially what it does is it takes us through a whole series of interview steps which we haven't done. You know, this is presuming that we are working for a company or an organization and we have a senior management team that we can go interview, etcetera.

Oh Cheryl's got her hand up, sorry. Go ahead, Cheryl.

Cheryl Langdon-Orr: Thanks Mikey. Cheryl for the record. And I was just about to jump in rampant agreement with you before you tried to sell OCTAVE any further. The OCTAVE style of stuff is probably something that we'd be suggesting done when you need to do the fine tuning in that whole risk profile for actual mitigation.

It's the difference between generically recognizing the risks - let me use an example here - of building and construction industry side versus the actual

site assessment which is site-specific. So, you know, it still has a place in space but not necessarily one that we need at this threat identification and vulnerability identification stage.

Mikey O'Connor: That really cheers me up, Cheryl, because you know a whole million pounds more than me about this stuff. And I'm glad to hear that my intuition is right. For those of you who are actually doing this kind of thing day to day and know what you're doing, unlike yours truly, do you agree with this?

Because if you do then my inclination is to, you know, unless there's another methodology that people are really fired up about my inclination is to say okay let's take a pause. It's pretty easy to go back and turn this process into a work plan for us to do our analysis.

And I could dig in to that and have something ready certainly for the ops call. And if the leadership group is comfortable with it then we'd jump right into this on our next call.

But I'd like to hear other folks who are familiar with other methodology. I know, Patrick, you're familiar with ISO 27000 series stuff. Do you see any huge conflict with using the this NIST kind of approach if it turns out that somewhere down the line 27000 series is where we need to go - or Cheryl or anybody else for that matter. I mean, you know, you all are a lot smarter about this than me.

Patrick Jones: Hey, Mikey, it's Patrick. So what I think might be useful is before we think about jumping to NIST there is a really useful risk management method comparison tool that (Lisa) has posted on there. I'll try to send the link in the chat and if I can't from here I'll send it to the list. It might be good to spend a little bit of time (unintelligible) to look at the comparison before you settle on one.

Mikey O'Connor: Okay I'm game. You know, one of the problems that I had with some of the - well especially the ISO ones is that in order to compare them I had to buy them. And they're pretty expensive. You know, some of them cost like $500 US which is - it's a little steep for being a volunteer-type guy on a project like this. You know, if they were 50 bucks I probably would have gone ahead and bought them but...

Patrick Jones: I don't think you need to do that step when a group has already done a comparison.

Mikey O'Connor: Yes.

Patrick Jones: So looking at a NIST's comparison tool, you know, you don't need to buy the standards that are - when they've already done the work.

Mikey O'Connor: Yes, that would be fantastic. And that's something that's just out in the wild in the public view or do we need to buy...

Patrick Jones: Yes.

Mikey O'Connor: ...the comparison?

((Crosstalk))

Mikey O'Connor: That would be great.

Patrick Jones: It - just as an example you could put in their system the NIST 830 that you used and ISO 2701 and do a compare and it has a table that shows where they're the same.

Mikey O'Connor: Oh.

Patrick Jones: So that is helpful.

Mikey O'Connor: Yes that would be extremely helpful. Yes, let's do that for sure. That's another no-brainer. I love that when the no-brainers come. And I think that one of the things that - it was helpful for me to do this decomposition of the NIST one was that then when Olivier and Cheryl raised their points I could say, ah, yes. That speaks pretty clearly to the sorts of things that are on this page.

So I'm feeling confident that we're going in the right direction. Let's see Don has a chat. Let's see and then Luis is agreeing with Don. Oh I see it's a different - so Don says I don't see a conflict but I don't know that we need to be as formalistic as ISO; pieces can work together. And Luis is agreeing with that. And Patrick is too. And Luis is amplifying one of my favorite concepts, the KISS, concept; keep it simple stupid.

And Jacques is saying I think all core risk management frameworks do the same thing; they assess risk, threats and opportunities against probability and impact. Katrina is agreeing. So I think we're all kind of homing in on the notion that we should do a little comparing, do something that's straightforward and simple.

Good deal, I'm feeling like we've advanced the cause. But I'm not sure that we need anymore today. It seems like our next - our next step is to get that comparison - oh and Rosella posted it to the - is that the same one, Rosella, is the one that Patrick was talking about?

Rosella Mattioli: Yes.

Patrick Jones: The link.

Mikey O'Connor: Perfect, all right. So we've got the link, we have our homework assignments. I think we've done a good job for today. I don't think we need to belabor this anymore. Patrick? Oh Patrick just saying thanks. Anybody in disagreement

with taking 20 minutes off from our hard work schedule and getting on with our lives?

Cheryl Langdon-Orr: At 20 to 2:00 in the morning you really want me to answer that?

Mikey O'Connor: Oh my God, oh my God, I didn't realize it was that late. Never mind, sorry.

((Crosstalk))

Cheryl Langdon-Orr: You should because you shifted the time.

Mikey O'Connor: I didn't...

((Crosstalk))

Mikey O'Connor: Gisella did it. I'm going to point at Gisella. Oh okay so let's give Cheryl a few winks and I'll see you all in a week. Thanks, I think this was a fabulous conversation. I think we're really moving the ball.

Cheryl Langdon-Orr: Fantastic.

Mikey O'Connor: I'm all done.

Cheryl Langdon-Orr: Mikey, I might just mention on an (administrivia) of the AC room until you started to share your large data screens I could run the AC room fully on 3G. Once you started to - and getting very good audio in and out not a problem.

Once you started to share your screen with us I was starting to get some packet loss so I did have to shift to, you know, a hardwire connection into the router. But that's not an insurmountably difficult thing to get over. I think that the test of using the room it also worked well.

Mikey O'Connor: Oh but that's really helpful because I was assuming - I see that change in bandwidth consumption on my end. And I was assuming it was just happening to me; I didn't realize it was happening to everybody.

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: Okay well that's easy to fix.

((Crosstalk))

Cheryl Langdon-Orr: On a 3G connection it did.

Mikey O'Connor: Yes. No I can easily change a lot of these into PDFs and that'll knock that one in the head. Sometimes we are going to have to do stuff on the screen but the two things we did today I didn't need to share my screen I could have done those both as PDF files so that's good to know. Thanks, Cheryl.

Okay I think that's it. Nathalie, I think we can end the recording and again three cheers for all the great work you did getting this Adobe room working. I think we proved that this is a great technology that is going to work going forward. Way to go for getting it running.

Cheryl Langdon-Orr: Brilliant.

END