Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
16 August 2012 at 13:00 UTC

Note: The following is the output of transcribing from an audio recording of the DNS Security and Stability Analysis Working Group (DSSA WG) teleconference on 16 August 2012 at 13:00 UTC. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. The audio is also available at: http://audio.icann.org/gnso/gnso-dssa-20120816-en.mp3
on page
http://gnso.icann.org/en/calendar/#aug

Attendees on the call:

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

ccNSO Members
. Rick Koeller, .ca (CIRA)
. Wim Degezelle, (CENTR)

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

ICANN Staff:
. Julie Hedlund
. Patrick Jones
. Bart Boswinkel
. Nathalie Peregrine

Apologies:
. Andre Thompson (At-Large)
. Mark Kosters
. Don Blumenthal - – (RySG)

Coordinator: Please go ahead.

Nathalie Peregrine: Thank you very much for that.

Good morning. Good afternoon. Good evening. This is the DSSA call on the 16th of August, 2012. On the call today we have Mikey O'Connor, Cheryl Langdon-Orr, Olivier Crépin-Leblond, Rick Koeller, George Asare-Sakyi, Julie Hammer, Rosella Mattioli, and (Unintelligible).

We have apologies from Don Blumenthal, Mark Kosters, and Andre Thompson.

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

I'd like to remind you all to please state your names before speaking for transcription purposes.

Thank you very much, and over to you Mikey.

Mikey O'Connor: Thanks Nathalie. Welcome to the call.

First up, the agenda actually has some work work on it today. We'll take a final look at the way forward -- that's the slide that's on the screen -- and then we'll start working on this gaps and overlaps stuff, which is sort of the featured event between now and Toronto.

Is there anything that people would like to add to the agenda?

Okay.

How about updates to people's Statements of Interest? Anything there?

All right.

With that, we'll dive right in. What you see on your screen is sort of the semi-final, maybe final, possibly final, perhaps final version of the plans between now through sort of Toronto and on. This is pretty much reflective of what we talked about last week, but it may have gotten tweaked one more time on the Ops call. I'm not sure.

Anyway, the main activities for us as a working group are to work on that gaps and overlaps stuff, and identifying the risk scenarios - or the risk scenario and the skills that we want to assemble to work on that for the assessment that we undertake after Toronto.

And so I just sort of wanted to put this in front of you one last time and at least for awhile will consider this plan. There is a - there is still a bit of scurrying about going on under the - behind the scenes. We're going to meet with Bill Graham in a week or so on the Ops call, so this may change again. We don't know, but at least for now this is the plan.

So with that, I kind of want change gears and start - where is that little rascal? I know you're in there some - there you are. I want to work on this gaps and overlaps stuff.

Is that type big enough for people to see? Hopefully it is. If not, sing out and I'll make it bigger.

This is sort of the rough sketch of what we have been talking about in terms of what we're doing. And as far as I'm concerned, we're starting today to do this work. And I think that this decision, the one about shall we do a survey or shall we do some desk research? I think that one's sort of been made by acclimation that the first thing we should do is some desk research. And then

go out to the people we've identified for some confirmation of the conclusions that we've arrived at, rather than going out with a survey. There was absolutely no appetite for doing a survey.

So where I'm at right now is to start brainstorming a bit through some of these items here. And as usually, Julie Hammer is ahead of me, so I want to show you some stuff that she sent me which I thought was really good, just to get your creative juices flowing and then we'll start expanding on what Julie sent. So hang on a minute while I get that up on the screen.

What Julie did was pull out some of the slides from the pictures deck that she thought were relevant to this conversation. And so, she just assembled, but then at the end she built a new one. So let me just remind you of the slides that we had in the - have in the report. This is one of them that's a newer version of this one, which is the third slide in the deck.

This is a pretty old model. This is a model that I built back in the 2001/2002 timeframe for a multi-campus - a 50-campus university here in Minnesota. And I was mostly using it in the context of defining our scope vis-à-vis the SSRRT. But, it does have a whole lot of detail, whereas this one is less detailed and gets at these ideas that we were talking about.

The difference between what goes on at the core versus the edge. The edge being organizational focus, and the core being sort of an ecosystem focus, and the glue being the regional or segments, or something that essentially provides a mechanism to communicate between the core and the edge.

So then what Julie did, which I thought was really neat, was put those two pictures side-by-side. And she started clumping by color the pieces of what could become a model.

And so Julie, do you want to walk us through this and tell us the tale, or do you want me to stumble along? I'm sort of hoping that you'd walk us through...

Julie Hammer: I'm happy to.

Essentially where I've started thinking was that we have a diagram with some useful ideas and some (hitting), and then had this much more data table. And it occurred to me that really they were describing one in the same thing in terms of functions.

And I started thinking, "Well, it would be really useful if they were better aligned." Because at the moment I pulled out the headings from each one, from the diagram and the table, and some of the headings aligned quite well. But, there are some headings in the diagram that don't exist in the table. And one in the table that doesn't exist in the diagram.

So I just sort of said to Mikey, you know, these functions would actually form a really good basis for having a conversation about (unintelligible) and overlaps to actually describe gaps and overlaps in terms of functions. But if we try and depict it on a diagram or a table, it would be much easier if they were really well aligned.

Back to you Mikey.

Mikey O'Connor: Thanks Julie.

So I wrote back and said of course, "Yay! What a great idea." And then promptly got stuffed off into stupid (fracks) and lawsuit stuff and didn't do anything about it. But it seemed to me that this might be a good starting point for the conversation about the stuff that we're doing here.

And so unless people just violently object, I think what I'd like to do is spend the rest of the call sort of combining these two things. Because it dawned on me that one of the problems with that hexagonal picture is that it's very pretty, but it's very cumbersome to modify.

And so I think that what we might want to do is really work kind of in text outline mode for awhile because it's really easy to change things around. And then when we are comfortable with the clumps that we've put together, we can always turn it back into pretty stuff again.

And so, what I was thinking we could do - let me just see how this works. (Unintelligible) things paste well into - oh, I'm going to - for those of you who use FreeMind, let me show you a trick, which is that if you go through a text editor - in my case, this little text wrangler, and then past things into FreeMind, you'll find that they past a lot better.

So there's the diagram and here's the table.

I find that if you paste right out of at least Microsoft products, you'll wind up with a hash if you go straight. But if you strip all the formatting off it works out pretty well.

And now if we were to combine - let's do a new table and - so there's one that was - this is one of the ones that was in the table but not in the diagram. And these diagram ones - that's not what I intended. Take two.

There we go.

Now let's compare - so the diagram had more stuff, so these were sort of all in a clump. Risk planning, risk assessment, and monitoring are kind of the classic risk management frameworks. So let's pull this one down, put these in that one like that, and we have education, training, and awareness.

And the way, you know, Julie was highlighting this is by showing it in a color that doesn't show up on the other side. However if we go a little deeper into this - I thought I had - no, I guess not. Not really.

Oh, here we go. I knew it was in there somewhere.

So we've got - all right, so that's okay.

Let's go back to - oops. Hang on a minute.

Here's my mumbling Cheryl.

Standards, tools, and techniques. We had three tech practices/op practices, technology management. And actually I put them there, but I'm going to debate that in the - and then - (unintelligible) that response going in there, or at least closely related.

Julie Hammer: Yes, Mikey, Julie here. Julie Hammer that is.

I guess by putting in the same color, I wasn't trying to say that they were identical, just that they were closely related. So yes, they're not necessarily a 1:1 or a 1:3 exact match. So they're just functions that are in the same vein.

Mikey O'Connor: Yes. And so maybe what we do is we kind of put a new title on them. And then -- oops -- make them peers for now.

I still like this hierarchy, because these are sort of the trio in the classic risk management framework.

Now security management is a new term. Let's go see what that was. Security management is the - and remember, this model was built for a single organization, and this is maybe the - one of the more touchy subjects in the ICANN context.

Because in this context I was delivering this report to the CIO's - the Chief Information Officers of 50 campuses and saying, "Well, you as the CIO's have a security management job to do. You know, you have to call the shots. You have to come up with a security strategy. You might want to establish a program management office. You might want to come up with a metrics policy," et cetera.

In this context, since it's - I think the odds are pretty long that anybody would sit still for a security management function, at least at the core, I don't know quite what to do with this.

I mean, it's definitely an edge-kind of function. Presumably, you know, folks like Rick and some of the other folks that are sort of at the front lines on this would have security management duties in their job title. So, maybe does belong in here, but I think we'd have to be careful.

Rick is asking, "Where does risk response fit in the framework?" And right now, Rick, that sits down here. It's the - this. And so maybe what we do is we come up with - I like risk response. Let's put that in there like that.

And the difference at least in our minds when we built that model way back in - you know, 12 years ago, was that there are folks that respond and there are folks that manage those folks. And the managers of the security function have jobs that they need to do. And this is - this was the list that we came up with at that time.

And the tricky bit is that, you know, this is a single organization model. And the reason it fell out of the - well, I don't know if there was a reason. I just didn't - it just didn't include - so what do people think? What do you want to do with this little rascal? That's the start of our first puzzler of this new model that we're building. Any ideas?

Rick is saying, “In reality, when risk materializes it’s an incident.” Yes, I think that’s right. And, I think those - this risk response clump is sort of the - you know, the stuff that we’re talking about there, Rick, whereas the security management function is presumably guiding the deployment of all this other stuff.

You know, what we were dealing with was an accountability issue where nobody was accountable for essentially managing the security functions in this 50-univeristy system. And what we were trying to do was describe what somebody ought to be doing and then going out to this coalition of - you know, just about as - college presidents are a pretty independent bunch. They sort of don’t like it much when the central administrator marches in and tells them what to do.

And so what we were trying to say is, “Well, this is something that falls mostly in your bailiwick. But if you're not doing it at all, that’s a problem.” And I suppose that we could take a similar line here, although I think that we as an ICANN community - I mean in the context I was doing this before, you know, I had a legislatively mandated central administration function that I represented. Whereas in the ICANN world, not so much.

Rick is saying, “Here at CIRA, our security function is a key stakeholder in our risk management process. They contribute, monitor, and respond to a significant number of our risks. Key stakeholder and collaborator of risk management.”

So Rick, is there somebody to whom the risk - or the security function reports? And if so...

Rick Koeller: Yes.

Mikey O’Connor: Rick, go ahead.

Rick Koeller: So it's Rick Koeller. So yes, the security management reports into our IT department. Risk management is separate. I manage - I'm responsible for corporate risk, so I - they certainly contribute a significant number of the risks and cost of risk, but they're not in the element of our risk management.

I think in the context of what we're doing, largely we're looking at IT security risk, not broader sort of business risk and that type of thing.

Mikey O'Connor: Yes. So you - so yes, I - so you're responsible for the risk stuff across all of CIRA, not just the technical risk?

Rick Koeller: That's right.

Mikey O'Connor: Yes.

And...

Rick Koeller: But...

Mikey O'Connor: ...that's one of the problems with this particular definition is this one is aimed at an IT function. And so, it's technical.

Now some of this stuff could map across into a broader risk function like yours, but yes; that's a key distinction.

I mean, one of the things we could do is for now we could staple this list into the outline, because I think that one of the things that's useful about a list like this is it's going to remind us that we have a discussion that we have to have -- oops -- because if we then change this to get rid of - maybe just get rid of the overall - get rid of the IT thing?

Does that finesse the issue that you're raising well enough Rick? Just dropping IT out of this?

In a way - oops, sorry. My stupid email program is whining ("I'll quit.")

In a way, that's part of the puzzle that we were formed to address is who's responsible? In a way, these are easier. You know, it's pretty easy to say, "Well, frontline medication is going to happen in the organizations that are on the firing line." The puzzler is who guides that effort and to what extent does that guidance need to be coordinated across a lot of organizations?

And, I think that's where people often get testy. I know that's where the college presidents got annoyed was when I would march in and say, "Well, we've got sort of an issue of sovereignty that we kind of need to deal with here." And the college presidents would say, "No. It's simple. I rule my kingdom. I am the total in-charge person for my college, and I will give up no sovereignty to any other college president in the system."

And then we would have the discussion, "Well, the trouble is that your security deficiencies may open up risks that effect your colleagues in that constituency, so you may want to consider ways that you can do that and still maintain your views about sovereignty."

And I think that in a way that's kind of what we're dealing with here, too.

Rick, go ahead.

You may be muted.

Rick Koeller: So - yes, I was.

Mikey O'Connor: Go ahead.

Rick Koeller: Kind of moving off the security management and it comes up in Patrick Jones' text comments as well about the Oversight Committee. And, it touches

on what you were saying there as well, Mikey, about you know a Board President saying he rules his kingdom. In this case, there isn't any one king.

So from a (longer-in) perspective, in addition to having distributed security management across the internet, you've got distributed governance monitoring challenge. So you know, the formation - typically, you would have a risk committee that risk management is reporting into and they're providing oversight and kind of validating on those risks that have been identified and plans around them so we're going to need to think about how that works as well. And governance ties into monitoring.

Mikey O'Connor: Yes, governance ties into a lot of stuff. Let's see. Cheryl has also got - let me read these comments into the transcript just so we've got that.

So Patrick kind of kicked off some of this when he said within an ICANN internal context the ICANN Security Team also performs this function in that we coordinate across the organization internally, contribute and monitor but also support our IT Department and provide an auditing function.

Patrick also goes onto say we also have a reporting function to the ICANN Board Risk Committee.

Julie then said it may be that when the Board DNS (RMF) Working Group produces their risk management framework hopefully based on functions that we may need to come back and align, adapt this framework that we produce.

Yes, I think that's right Julie.

And then Cheryl is saying, why not have security metrics as a subset of operational in our context?

And I could take that as a friendly amendment. Do we have metrics in here yet?

Let's put it in here as a placeholder now. There could be that what we're getting a jar that's got an awful lot of stuff going into it. You may want to comb that out a little bit.

I kind of want to go back to the governance question for a minute because I think that's an interesting puzzler. I think governance is where the conflicts between inside all these organizations and across all these organizations may get interesting and maybe that's where it gets resolved.

Rick you're kind of leading us in here. When the governance function was formed what were it's - what was its charter? What was its job to do in terms of this cross organizational stuff?

Can you expand on that a little bit?

Rick Koeller: Sure. So Rick's on again. So Governance Committee typically be in our organization and we're ten different business units, I've got a variety of both position and functional background. But it's really only three or four people.

Yes, so it's committee and its charter really is to be an overseer of the risk registry. To be able to independently kind of help validate the risk assessments and to validate risk plans to, you know, mitigate or, you know, take other action to reduce the impact of risk or probability of risks.

And that's essentially it, you know, but they're an important part of an ongoing process so.

Mikey O'Connor: So in the ICANN, well in the DNS Security Stability Reliability Resiliency Ecosystem, is there a group like this today or at least is there a group that thinks of themselves as doing this today Rick?

Patrick Jones: Hey Mikey, it's Patrick.

Mikey O'Connor: Go ahead Patrick.

Patrick Jones: So I think each - so individually participants in the ICANN space do this or I would think many of them do so my comments earlier were that within - internally within ICANN Security Team performs this function.

But from Rick's comments (CIRA) does this as well. I would assume that most of the major registry operators do this. I don't know. Others in the space do it as well. So it's done individually but there's not a sort of overseeing entity that does it unless I've misunderstood what you're asking.

Mikey O'Connor: Yes. I'm not sure I'd use the word overseeing. But, you know, I'm just curious if there's anybody that thinks of themselves as the, you know, the equivalent of this kind of a committee that is cross organizational.

And I can't think of one. But I wanted to make sure that there wasn't, you know, for example would DNS (ORAC) stand up and say well we kind of do that?

I'm not a member of that so I don't know what they do but would they think of themselves that way Patrick or anybody else who knows that?

Patrick Jones: So I'm not sure that they would. But this may be an area where it would be helpful to reach out to someone from - that's active in (ORAC) and ask them the question.

Mikey O'Connor: Yes. Well and this could be the sort of desk research process. I mean what we can do is we could posit this thing out there. And once we sort of described it, ask a few likely candidates like DNS (ORAC), you know, whether they feel like this is part of their pile or not.

So one - well we have - I think we need two of these things. Let me think about this.

And I don't know if it makes sense to put all that pile underneath this. I think that there's a - that these are different things just by the nature of what they are.

You know if I were in the college system, I'd be saying yes, you this - the college President. You should have one of these for your organization for sure.

But then there's some sort of meta-version of that that you ought to have.

And in fact we created one. We didn't set it up as a Governance Committee because that would have raised too many hackles but we did warn the group that it was pretty similar to this. That was system wide and encouraged that mostly to be a facilitator of collaboration and builder of trust rather than oversight because oversight may people too testy.

Let me see if I've missed anything in the chat.

Yes, I think Cheryl's in there. Maybe there should be a super group facilitation or SharePoint at least.

But maybe that's - maybe governance is too hard a term. What can we call this besides governance? Call it a SharePoint for now. Coordination, oh I like that. That was from (Julie Hammer).

Whoop, and then having done that we've probably got some things that and moving that sort of up, starting to rank these by core to edge a little bit. That may be a fool's error and (I) may stop doing that. But at least to kind of get the notion across that these are starting to become sort of different things.

How am I doing on time? Oh we got sometime, yes.

Anything else on what we've got on the screen so far? And then I'll circle back to those diagrams and see if we need to staple in anything else.

Okay, let me go back and take a look at some of this stuff. And we spent a lot of time on the frontline definition of it's a response because that was a problem that the legislature had with what we were doing because we weren't doing a real good job there.

There was an interesting conversation about compliance. Again this was sort of a sovereignty issue.

And Rick in terms of the structure that you've got there at (CIRA), where did this compliance stuff fall out?

Did it wind up in that committee or was it tending to be more decentralized? How does that work?

Rick Koeller: (Server teller). I got to think about that. Ponder it. I can't say that we have a - in the context of risk management we don't have a compliance more than function.

Man: What does that mean?

Rick Koeller: You know a discreet function that way I guess. You know certainly if we are dealing with an incident, our incident management practice and process kicks in. And depending on the severity of it we've got protocol to follow that.

Can you elaborate Mikey on more the compliance?

Mikey O'Connor: Yes. What we were dealing with...

Rick Koeller: In this context.

Mikey O'Connor: ...was again a 50 campus deal. And where we wound up with all this was there was a model where at the core, at the central administration, it was sort of our job to come up with good ideas and promulgate those ideas out to the 50 institutions.

And so, you know, we would - we developed a whole bunch of tools and techniques and so on and so forth. And this was sort of the list of things, the clumps that we tended to focus on in the central administration.

And then what we would do is we would get - oh I think I can make this a little bit bigger. There, that's good.

We would - there was really no appetite at all in the college and university system for a policing function to go out to the 50 campuses and check and see if they were in compliance.

And so instead what we would do is build essentially a compliance toolkit that the campuses could use themselves to self audit how they were doing on implementing all this stuff.

And then the committee would keep an eye on those self audits and, you know, again it got dicey as to whether people wanted to share those and so on.

Oh Patrick's got something in the chat. Hang on a minute. Oh Patrick you've got your hand up. Why don't you go ahead and take it from here.

Patrick Jones: Yes. So I don't want to open up a can of worms. But and so please disregard the word DNS (CERT) in this document.

But I think the content of it is still useful. This is a Collaboration Analysis Report from a workshop that was done in April of 2010. Some of the participants from the DSSA were at that workshop.

So I point to it as an example of some of the things that were discussed back then about the need for coordination and collaboration. And the types of qualities of the entities that currently exist in the space.

So I'll leave it at that.

Mikey O'Connor: It sounds to me like I need a notes jar. I can steal.

Patrick Jones: The document is at the top of the link and if there was a handy way to drag and drop the PDF link directly into chat I would do it. But I'm having difficulty.

Mikey O'Connor: Hang on. I (have to get) that into the - oops, it didn't take me to where I thought I was going to go. Hold on. Oh come on dear. I want to see if I can just pull it.

Ah, that's the problem. Okay, so this is the report, got it. Okay, so I can copy the link location for the report.

And put it in here. So this is the operational. I'll just skip the DNS (CERT) thing. Operational requirements and collaboration analysis and staple that. Oh that's ugly. Well that's close enough. I can fix that later.

Anyway it captures the - and there's a whole bunch of good stuff on that page. Wow, look at all this stuff. I'm reading the page that Patrick points us to.

Patrick Jones: Again with the qualifier that it's not about DNS (CERT). I'm just raising this as it's...

Mikey O'Connor: Right.

Patrick Jones: ...historical information that's been collected in the past and take it for what it's worth.

Mikey O'Connor: Right. But if we expunge that word and also expunge the notion that this is something that ICANN ought to run, it's still a pretty good bulleted list.

I think I'm going to steal that bulleted list if it's okay with you Patrick.

Patrick Jones: Yes.

Mikey O'Connor: Okay. I'm going to steal those and staple them in here. Because I think that's a good list. It's kind of tall but there we go.

So this is a list of things that it's pretty incident focused. But it's not a bad list of things to think about.

Cool. You know I think in a way this is right at the heart of why we were formed to try and resolve the dilemma of getting this kind of stuff done in a way that is acceptable to the community which is in a way a lot like what I ran into with the college Presidents. I hadn't thought about that until now but there you go.

Okay, now Cheryl was saying in the spirit of that it's fine. Patrick, sure, understood Patrick's SAN (CERT) run by ICANN works fine. That was one that probably needs a little unpacking.

Cheryl you want to jump on and Patrick SAN (CERT) run by ICANN works fine. Sorry to put you on the spot.

Patrick Jones: I understood what Cheryl meant.

Mikey O'Connor: Oh okay.

Patrick Jones: But yes.

Mikey O'Connor: All right. Well you can unpack it. Cheryl's either on mute or...

Cheryl Langdon-Orr: (Unintelligible).

Mikey O'Connor: Oh there she is. She's very faint.

Cheryl Langdon-Orr: I seem to be on mute.

Mikey O'Connor: Oh there you go. Now I can hear you.

Cheryl Langdon-Orr: Am I (just) faint now?

Mikey O'Connor: You're very faint.

Cheryl Langdon-Orr: Okay SAN (means)...

((Crosstalk))

Mike Langdon: Extremely faint.

Cheryl Langdon-Orr: ...without, SAN without.

Mikey O'Connor: You know I can tell that you're talking Cheryl but I can't hear the words. It may be that your phone is dying or you may be trying to reserve the slumber of your (spousal unit). You're speaking very quietly or something.

Anyway I don't want to belabor it. If you want to retype it in a longer version, oh SANs equals without, okay, so understood.

Patrick without (CERT); yes, I understood what SANs meant. I still don't understand the sentence. Understood Patrick so Patrick is the committee? No, sorry. Understood Patrick comma, without - oh so you're saying that something run by ICANN would work okay, Cheryl?

I didn't think so. That's why I wanted a little unpacking. Well we'll - we've got plenty of time to figure this one out.

Okay, Rosella says, that works out - oh you were there, cool.

And then Patrick's got the right - oh good, that's the right link. Let me get that in the notes because that link that I picked up is wrong, wrong, wrong. Yes, there we go. Get rid of this one.

Okay, I think, you know, we're coming up on five minutes to the hour. Let me just - I'm going to strip some of this down so we can see the - make that one and that one we know cold. All right, so now we've got the whole thing.

Let's go back to Julie's chart for just a minute and see if we picked off the big stuff anyway.

Yes, I think we've got all of this at least started in our conversation. So I think with that I'm going to declare victory for today. Oh, publish this out to the list then I'll start doing status reports and all that good stuff and maybe we'll reel in some people that have been slumbering because this ought to get people fairly excited when we publish a list like that.

And so and maybe just to wrap this up, Patrick at that meeting where they came up with all those good ideas did they come up at all having not read it yet, did they come up with any strategies on how to move forward or was the presumption that an ICANN (CERT) was the way to move forward and this was flushing out what it would do?

Do you want to comment on that?

Patrick Jones: So Mikey it's Patrick again. So the Collaboration Analysis Workshop results were posted for comment along with some other material was in the first link that I put in the chat which then later became this - recalling correctly that fed into the DNS (CERT) Concept paper. But, you know, later that was (just about) and determined that was not the right path to follow down.

Either way the discussion from this workshop in D.C. brought up some really relevant and useful material that I think has either been somewhat forgotten or it's still relevant today.

So that was really why I included in the link is if the DSSA is talking about the things it seemed to trigger in my mind some of the same conversations that came up back then.

And why not look to what was discussed a couple years ago and see is some of that still relevant or have things changed enough that there's some interesting new things that could be identified?

Mikey O'Connor: Yes. Well I love mining work, good work that was done by others before us. And we have the advantage of, you know, being able to see into the future which they couldn't.

And so maybe what we can do is extract a lot of the knowledge and wisdom from that and avoid the pitfall that they fell into and get the best of both worlds. So that seems like a good thing.

Okay it's top of the hour folks. And I think this is a good spot to stop. We'll pick this up again. This is basically the conversation we're going to have for a couple of more weeks. I think the thing that we want to start thinking about between now and next week's call is some way to organize this so that then

we can start doing the desk research that says which organizations do which of these things.

And, you know, I think that in many cases especially when we get down to risk response the list of organizations that actually respond to risk is huge. It's, you know, essentially all of the registries, all of the registrars, etcetera, etcetera, whereas some of these other ones it may be a little bit sparser.

Rick's not going to be with us. Dang, you were a big contributor today Rick. Thanks for joining us and we'll see you in September.

Anyway with that Nathalie I think you can wrap up the call and we'll reconvene in a week. Thanks folks.

Woman: Okay, thank you very much.

Woman: Thanks so much. Bye.

Woman: And now you may stop the recording. Thank you.

Man: Thanks very much Mikey.

Man: (Unintelligible).

Woman: Bye.

Mikey O'Connor: See you gang. I think we're getting.

END