# Transcript

## DNS Security and Stability Analysis Working Group (DSSA WG)

## 25 August 2011 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 25 August 2011 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-20110825-en.mp3

On page:
http://gnso.icann.org/calendar/#aug
(transcripts and recordings are found on the calendar page)

**Attendees on the call:**
**At Large Members**

- Olivier Crépin-Leblond
- Cheryl Langdon-Orr

**ccNSO Members**

- Jörg Schweiger, .de (co-chair)
- Takayasu Matsuura, .jp
- Sean Copeland, .vi
- Katrina Sataki, .lv
- Wim Degezelle, CENTR
- Roy Arends, .uk
- Jaques Latour, .ca

**GNSO Members**

- George Asare-Sakyi – (NCSG)
- Scott McCormick
- Mikey O'Connor – (CBUC) (co-chair)
- Rafik Dammak, GNSO

**NRO Members**

- Arturo Servin (LACNIC) Adobe Connect only

**SSAC**

- Jim Galvin (SSAC)
- Mark Kosters (SSAC)

**ICANN Staff:**
Patrick Jones
Julie Hedlund
Glen de Saint Géry

**Apologies:**
Bart Boswinkel
Luis Diego Espinoza,.cr
Patrick Vande Walle – At large
Chris Wright, .au
Greg Aaron – (RySG)
Adam Palmer – (CBUC)
Rossella Mattioli – (NCSG)
Edmon Chung -At Large
Ondrej Filip, .cz
Don Blumenthal – (RySG)
Andrew de la Haye (NRO Member) - for the next 4 weeks
Mohamed El Bashir (At-Large)
David Conrad (SSAC)
Rick Wilhelm, Network Solutions

Coordinator: Thank you. The recordings have been started. All lines are open. Please go ahead.

Glen de Saint Géry: Thank you. Good morning, good afternoon, good evening everyone. This is the DSSA call on the 25th of August. On the line we have Olivier Crépin-Leblond, Jörg Schweiger, Matsuura Takayasu, Roy Arends, Mark Kosters, Katrina Sataki, Sean Copeland, Wim Degezelle, Patrick Jones, Jacques Latour, Mohamed El Bashir, Mikey O'Connor, George Asare Sakyi and Cheryl Langdon-Orr and Rafik Dammak.

For staff we have Julie Hedlund and myself, Glen de Saint Géry. Have I left off anybody? And forgive the bad pronunciation of some of your names.

Scott McCormick: Scott McCormick just joining.

Glen de Saint Géry: Welcome Scott. And we have apologies from Chris Wright, David Conrad, Edmon Chung, Andre Philip, Patrick Del Valle and Don Blumenthal. And may I remind you please to say your name before you speak for transcription purposes. Thank you very much and over to you, Mikey.

Mikey O'Connor: Thanks Glen. And thanks especially today for getting the audio going; that trick is complicated. The way the audio works is if you don't have a good phone connection you can listen to this through your speakers on your computer. But it's only one-way. And so it's really for folks who don't have good phone connections that we do that.

Our agenda is pretty much the same as last week's. We'll take a moment and see if people have any changes to their statements of interest. Right.

And what we're going to do is continue on with the threats discussion. I went ahead and read the three reports that were mentioned on last week's call and created a rough outline of what was in them. And I thought we would see if the same sort of consolidation process that we did with the work in Singapore would also work for those reports.

And as we do that I could use your help. It may not work in which case towards the end we'll sort of review this and see if there's a better way

to do it. But the other thing is that these are probably not the only two or three reports on the planet about threats to the DNS and we might want to think about other ones.

So as we go through this conversation if you think of other similar reports that we might want to review the same way take note of that and we'll also collect that list towards the end.

And then the other question to put forward to you is whether this process is good for us or whether it would be better to have essentially either me or some of the staff or both do this for you in advance. There's a case to be made on either side. And so this is sort of an experimental call and at the end we'll sort of review how the experiment went and see if we want to keep doing it this way or change course.

The other little procedural note that I'll make now is that during the regrets process right towards the end especially this morning we did get a fair number of people asking whether we can change the times of the call, maybe rotate the times of the call to make it easier for people in certain time zones to participate.

And we'll take that up at the next co-chair meeting and come back to you with an idea or two about that. I know it's really inconvenient for a few people to participate. So there we are, that's it for housekeeping. And off we'll go.

So on your screen is the same thing that is the last entry in the wiki. If you want to follow along with the PDF the link to that page is on the screen up in the upper right if the type gets too small.

And from here I'm going to go to the next stuff which I went ahead and did last week. Last week we came up with two SSAC reports and an RFC that had to do with threats to the DNS. And so I went ahead and read those. Not going to open these all up at the same time because the outline got pretty gigantic but I'll do the first one.

The - show you what I found. SSAC 40 - or SAC 40 was talking about measures to protect domain registration services against exploitation. And 44 was a similar report but aimed more at registrants. So here we go.

The way that report was laid out I started pulling out things that I thought were vulnerabilities. And then in the report itself they delineated - this is going to explode on your screen - delineated a series of attacks that they actually reviewed against several companies that you can see listed there.

Then - let's see - I think I'm going to stop because this - as you'll see this gets very large very quickly. So if we take some of these vulnerabilities one of the things that came up in this report that was new at least for me was the notion that high value names themselves can be vulnerabilities because they become targets for attack. They essentially are almost bait if you will for the attacker.

So if we - I'm going to try and figure out how to lay this screen out so that we can move back and forth here. Bear with me for just a second. There that gets better. This way we can see them both at the same time. I mumble while I do this. Anticipating Cheryl - Cheryl is giggling in the background. She knows.

((Crosstalk))

Mikey O'Connor: So here we go. So you can see that high value names doesn't really fit really well in any of the vulnerabilities that we've got yet. And so I think that this is one that goes at the top level in this. And I put there unless somebody shrieks.

I'm also going to copy them in rather than drag them in because what this is becoming is the beginning of the outline for the report. And we may want to essentially just include this whole hierarchy in the report as an appendix or something like that or at least refer to it.

The next one that was mentioned in the SSAC report was registrar automation patterns and behaviors. And I think that there - do have some - and we could put it either here, we could put it up here or we could put it here. And I think that this was more - this was actually aimed at both some of these managerial issues and at the actual software itself. So again we're - I think go ahead and duplicate it there.

The next one talks about inadequate assessment of risks associated with loss of control of domains and registrar accounts. Now this is on the part of the registrar not on the part - this same point was made in SAC 44, the next report, where registrants don’t adequately assess their risks.

But in this particular case this is essentially a managerial issue on the part of the registrars. And again I would be inclined to put it in this kind of a category essentially a managerial choice. Pull this down. There.

If I make this one notch smaller can you all still read it?

Cheryl Langdon-Orr: Oh getting hard there.

Mikey O'Connor: Getting tough, all right, never mind. Thought I'd just check. All right so this next one is talking about how email is often the only method by which registrars attempt to communicate with a registrant regarding account activity.

And I think that this one could go into either a single point of failure kind of place or a homogeneity kind of place. For those of us who came up with these two do people have a preference on this? Again that - it's easier to rearrange later but I think it is a new one of these. Put it temporarily single point of failure category.

This next one talks about accessibility - the access and ability to modify contact and/or DNS configuration to all domains in a registration account through a single user account.

And I'm guilty of that; I have a handful of domain names and they're all under the same account and they're all pretty valuable. And if somebody got a hold of that account's credentials they could disrupt the whole thing. Again I think that's a single point of failure kind of thing. We're all right with that. Put it there for now.

The next one says customers are unfamiliar with registration protection measures. And that again could be a managerial choice. Eventually the way that customers are trained and periodically reminded of that. Put it over there for now.

Another point that was raised in this report is that registrars have different target markets and different service models and that creates diversity - the way that the registrars provision accounts it - there is tremendous diversity in both the software/hardware/user interface - even contracts from registrar to registrar.

I don't exactly know where to put that in our emerging taxonomy over here. Anybody got any bright ideas about that? I'm feeling like I'm doing a monologue so I think I'm going to stop and see if somebody's got an idea of where to put this because this might be a new category or it might fit. And I want to stop the monologue.

Not getting overwhelmed with ideas from folks so...

Cheryl Langdon-Orr: Well, I mean, Cheryl here. My knee-jerk is it probably fits under managerial. But, you know...

Mikey O'Connor: That's fine; knee jerks are fine. Just nice to have more than one voice on the transcript. Thanks Cheryl. Let's see the next one is the process to restore DNS information can take a long time. Even when unauthorized modifications to DNS information is discovered quickly. I would put that perhaps up in operational. Process is a key word.

Cheryl Langdon-Orr: Yeah I...

Mikey O'Connor: Go ahead, Cheryl.

Cheryl Langdon-Orr: Cheryl here for the transcript record. I don't actually see that as a vulnerability I see that as a consequence; annoying, irritating but it's not really a vulnerability.

Mikey O'Connor: That's a good point. Take a look - put that up under impacts.

Cheryl Langdon-Orr: Yeah, that I'm more comfortable with.

Mikey O'Connor: All right, good deal. Cool, all right. Going to skip this one, this was just a part of the report that delineated where they got their information. I don't think it - now we come up with several threats. So I'm going to change around my little screen here for a minute. Put them side by side, mumbling all the way.

So in this particular case the first threat that this report talked about was gaining control of the account or the user's password credentials. Surely we've got that in our threats. Trying to figure out a way to orient this so that we can see it better. Put the whole threats thing up in the middle of this. Just a tiny bit. No that's not going to do any good.

So I think that where I would put this one here - direct attack. Maybe - the next threat that the report talked about was - and attacking essentially through - I would use that as a technique as to how that happened. And the final one that was talked about in that report was blocking delivery of email notifications to the registrants by changing the configuration in their accounts.

And I think that that falls within this same category. Mark, I missed when you agreed but I'm glad I'm putting these...

Cheryl Langdon-Orr: I'm sure Mark was agreeing with me.

Mikey O'Connor: Ah, good deal. Boy I'm way behind the times. Thanks Cheryl. All right the next one is a section of the report that talked about prevention. And the reason that I wrote all these in is because one way to approach the threats conversation would be to take a lot of things like this and essentially turn them into negatives.

If a registrar did not verify registrations, for example, that could be a, you know, a consideration for us. It could be - and probably a vulnerability rather than a threat. If a registrar did not have strong password-based authentication systems, you know, that could be a vulnerability.

And so I was curious if people agreed with that approach. I'm not necessarily sure we need to do this on a conference call. You could for example tell me yes that's a good idea, Mikey, why don't you go off and take a stab at that and come back with the results. But I didn't want to go and do that too much on my own until we've at least had the conversation at the end of the call.

Because there's a lot of this stuff that I could go ahead and do but I wasn't sure about two things, first I wasn't sure whether this would annoy you and second I wasn't sure whether that would get me too far ahead of you in terms of stepping through the details of this.

Part of this process I think is us learning these things together. And I think one of the things that we need to talk about is whether it's a good idea for us to do that, which will consume a fair amount of time but will bring us together to the same sort of understanding or whether it's a better use of our time to go ahead and have essentially a pre-digested piece of work to review and edit.

So you can think about. And this is a really good example of a thing that could be pre-digested for you. In this particular case I think that one way to do this would be to - well I think I want to stop there and see what you want to do. Would you like to step through all of these on the call, turn them into negatives and place them in our hierarchy in which case we'll do that. Or would you rather have eventually staff work done before you see all this?

Mikey O'Connor: Oh. I'm now waiting. That's a question to the group. I may have put everybody to sleep...

((Crosstalk))

Cheryl Langdon-Orr: Cheryl here but I fear having it become a dialogue rather than a monologue which is all very nice for you and I but isn't all that engaging for everyone else, Mikey.

Mikey O'Connor: Right.

Cheryl Langdon-Orr: I'm (unintelligible) only because I think I understand that turning them sort of in the reverse order and making them negatives - part of me also would like to have them somehow wrapped up in a neat little puddle called something along the lines of, you know, not following - dare I use the terms - best practice models or something, you know.

There needs to be a paddock which we put them in as well.

Mikey O'Connor: Oh.

Cheryl Langdon-Orr: And not really...

((Crosstalk))

Mikey O'Connor: Oh that's an idea.

Cheryl Langdon-Orr: ...which isn't threat or a vulnerability rather as a - yeah, I mean, where they are in prevention they make sense the way they're written but the lack of attention to them does something other than, you know, mean that there's a corollary to prevention if you follow my garbled logic.

Mikey O'Connor: Right. Yeah, I like that idea because what we could do is then we could make a paddock. That's not a word I use much. I would tend to use a jar but both are fine. And in that case what we could do is we could essentially put it in here. Say something like best - then we could take a whole bunch of best practices which have been suggested in these two reports especially and put them in there. Is that where you're headed with this, Cheryl?

Cheryl Langdon-Orr: Yeah, that kind of makes sense, yeah, yes, yes, yes.

Mikey O'Connor: Let's do that. That's at least a way to keep our...

Cheryl Langdon-Orr: Yeah.

Mikey O'Connor: ...outline going.

Cheryl Langdon-Orr: Yeah.

Mikey O'Connor: Yeah, all right. Anybody else got a terrible problem with that because that neatly solves the whole re-writing a report, turning things into negatives and perhaps process of doing that screwing things up which I am acutely aware of.

I think this same works here where we view these as best practices, multi-factor authentication, etcetera. And we say that registrars not doing that that's a vulnerability in their management approach. Sorry to make your eyeballs roll up and down like that.

Oh, dear, I - let me tell you a little personal history. This was the point at which I badly hurt my finger here at the farm and I stopped typing things and started cutting and pasting things is why there's so much. These are basically the findings from the report. And, partly I did it because I was having a hard time typing, but partly I did it because they are very good and I wanted to show them to you.

So I think I just want to step through these and figure out where we put them in our (unintelligible) notes essentially. Mark, go ahead. (Unintelligible) there.

(Mark): Yes, I guess I - is now the time to bring - for me to bring up my controversial suggestion? Because you kind of...

Mikey O'Connor: Yes, go for it.

(Mark): And maybe this'll get conversation going a little bit. And that is maybe - and you said this, as you were discussing this a little bit earlier. Is that, the sort of listing of best practices is whether or not someone like

ICANN should be looking at each of the registrars and registrees to see whether or not they follow those best practices.

And I know that's more of a solution as opposed to listing all the potential issues, but that's one way of solving the - a weakness that could be tin the system.

Mikey O'Connor: And what I decided would be a good idea is if we did (unintelligible) a record - it started, you know, we're going to - in our charter we are charged with essentially a three or four phase process where first we identify threats and we've sort of taken it upon ourselves to add vulnerabilities to that pile.

Then we're supposed to analyze those threats and determine the current state of affairs. Then we're supposed to identify gaps in where threats are not being addresses. And make recommendations if we find any gaps and if we can think of recommendations to close the gaps.

And it seems to me that that idea falls in the recommendations pile. And I think that what we're going to find is that as we go through this conversation, we're going to come across a bunch of recommendations and that we should capture them as we go. And then when we're closer to the end, come back and see if that's a good idea. Does that work for you Mark?

(Mark): That's perfect.

Mikey O'Connor: All right. So then, as you regular folks may have realized, this came up on the (unintelligible) call and I wrote it down then, so I don't even have

to type it again, I can just stick it into our pile of possible recommendations. Spell it; we'll capture it like that.

All right so, back to this one. Eventually what best - that the SSAC found in this first finding, is that there are differences between the registrars in their vulnerability. And that registrants don't have sufficient information to assist - to assess the extent to which a registrar is able to protect its domain accounts from attach.

And that, it seems to me in and of itself, is a vulnerability. Because if a registrant can't figure out the situation then they are making and choices about where to put their, you know, where to register their name. You know, I don't exactly know - again, I think we need a sort of a share all Meda approach to this. I don't think that these can be reworded into being vulnerabilities, but they're very important for our conversation and we need to figure out a place to put them so that we don't lose track of them.

Because one of the things that I've started to realize is that the - at least some of these other reports tend to be somewhat narrower in their focus than our charter. This SSAC report is focused only on registrars. The next one is only on registrants.

Female: (Cheryl Himagi).

Mikey O'Connor: Yes, go ahead Cheryl.

(Cheryl Himagi): This fairly not an exceptionally good idea and that (unintelligible) start putting recommendations bundling together. If for example, in the recommendations we were to indicate that some sort of report card or

ranking that was available or allowed registrants to make informed choices could fit into where you're heading with this current part of the conversation.

It's not being prescriptive. It's not even being proactive; it's giving operability and accuracy of information for the domain name licensee, the registrant, to make the right choices and understand the risks they are around or taking when they go for option A over option B, Q or L.

Mikey O'Connor: So, what if we, in our possible recommendations started listing some benefits? Then they add that one benefit - who, sorry -- the decision making and said that - annotate this, hang on a minute. Otherwise we'll never know where that came from. How about something like that as an approach to handling some of these? Is that where you were headed Cheryl?

(Cheryl Himagi): Yes. It'll need a tweak and a bit of refinement and maybe a lot more, thinking on whether we just leave it improved decision making on - but yes, it think that's sort of heading in the right direction.

Mikey O'Connor: Yeah, well at least gets the - this notion captured...

(Cheryl Himagi): Yes.

Mikey O'Connor: -- somewhat closer to there and...

(Cheryl Himagi): It's more of a vaguely formed direction than it is a paddock and I do like my paddock.

Mikey O'Connor: Well, it's a paddock with a wide door or wide gate, that's left open at the moment.

(Cheryl Himagi): It's more of a general wave of the hand in the particular direction saying over there, but anyway.

Mikey O'Connor: Yes, and I'm big on those. I love general waves of the hand. Cool, okay. Mark is that an old hand or are you wanting to join in here? I just noticed that your hand is up. It's an old hand, okay.

Another finding in this report was that while there are a large number of registrars that offer consumer folks domain name registration services and a smaller number of registrars and brand management organizations that offer security services to high profile, highly targeted domain name holders.

SSAC notes that there isn't really a pure place secure registration service provider or at least they're rare. And partly this is due to the fact that security measures does to as prominent a role in customer decisions. And so, we may have a kind of cart and horse problem here.

It might be that consumers would take this more into consideration if they had more information about it. And so, we could maybe put this in your paddock - Mark's paddock in this particular case. There's, another part of the discussion about that recommendation. Be so bold - eww, as I attempt to say issue. Put that up there. Eventually we say that this is one of the issues that we've uncovered. We and SAC40, that this -

(Cheryl Himagi): But doesn't that - sorry, Cheryl who's just jumping in, 'cause it's that time and I can - don't allow us to perhaps look at future opportunities of

encouragement and ongoing education and, I guess, updating all the restraints. There's a vast difference between the rush of blood to the head on the planning of something where you think well, cheap and cheerful will do because I don't know how much resource or risk I want to put in in terms of my expenditure for example at the beginning of a project.

And then the ongoing investment in that changing and people forgetting to review. It's a little bit like, you know, having the fence around my paddock, but not recognizing that with 2400 vaults worth of electricity going through it, you know, the ducts are at risk in the bottom (unintelligible). Yeah, that type of thing. You do have to think about, get the end user or the registrant to consumer it to loop back from time to time and go if this now fits the purpose.

Mikey O'Connor: So I'm going to call that a vulnerability, and say that there is - I think I'm going to put it in here. I'm going to say this is - come on. I think that's what you're going for, isn't it Cheryl? That people check one but then forget to...

(Cheryl Himagi): They make a decision at one point and don't go back to review it and to - I mean, to some extent it's the registrant equivalent of the registrar managerial choices issue or issues.

Mikey O'Connor: Yes, and I'm not sure that that's restricted to registrants.

(Cheryl Himagi): Okay.

Mikey O'Connor: You know, that's - I think that that's for...

(Cheryl Himagi): No, but I was linking it to - specifically to that part (unintelligible).

Mikey O'Connor: Ah, I see what you mean. All right, so then what we could do, take it out of there, put it down here. Is that what you're - oops, not that ways.

(Cheryl Himagi): Ooh.

Mikey O'Connor: Sorry, I was just testing your eyeball. Like that? Say that this is sample of that. Then like that Cheryl?

(Cheryl Himagi): Yes, that (unintelligible).

Mikey O'Connor: Okay.

(Cheryl Himagi): Not seeing a whole screen or any part thereof, yes.

Mikey O'Connor: Oh, really? You can't see the whole...

(Cheryl Himagi): I can, it's just - it's...

Mikey O'Connor: Oh yeah, seeing it full, I get it. Well, yes, this is the rough with these is that they get pretty big.

(Cheryl Himagi): Yes.

Mikey O'Connor: And the good news is that it makes writing reports a lot easier because you have a giant pile of material to edit, instead of having to write a lot of stuff. All right, go back to the findings.

Other finding that the SSAC came up with was that registrars could make more information about their security services available to allow customers to make informal decisions - informed, I'm sorry, decisions.

Voluntarily submitting operations to an independent security audit and publicizing successful outcomes of such audits would allow customer to choose a registrar based security requirements as well as cost and other ancillary features such as web and DNS hosting. (Unintelligible)...

(Cheryl Himagi): That (unintelligible) to the other one.

Mikey O'Connor: Yes, that seems to go with the first one. Right?

(Cheryl Himagi): Yes.

Mikey O'Connor: Way up here. Now, I have to take a moment. I am the co-chair representing the GNSO and point out that registrars, when asked to do this are - I don't know if we have any registrars on the call. So if I'm putting words in your mouth, and you're a registrar, feel free to jump in here.

But, one of the trouble with this is that this provides a map for bad guys if we do a - eventually an inventory of registrars this way. One of the things that we run the risk of doing is painting a target for attackers that say the flowing registrars are good targets for you to attack. And so I think we need, when we're - we get around to discussing this recommendation, we need to address that concern because it's a real one and...

(Cheryl Himagi): (Unintelligible)...

Mikey O'Connor: Somebody's...

(Cheryl Himagi): Cheryl here, my knee jerk reaction to that is a little along the lines of well tough.

Mikey O'Connor: Well, I just...

(Cheryl Himagi): (unintelligible) by the rationale that goes along the lines of yes, well if I live in a risk area and I love my doors and windows unlocked, but my excuse is I want the fresh air, then there you go.

Mikey O'Connor: Well, I dutifully taking on my job as GNSO co-chair and trying to represent several points of view here. And won't go a whole lot further on that right now, but...

(Cheryl Himagi): Asterisk it to have a great deal more discussion, yes, I think that's...

Mikey O'Connor: Yes, discussion to follow. (Olivier), go ahead

Olivier Crépin-Leblond: Thank you Mikey, Olivier for the transcript records. I think there's a difference that we have to point out here. There's a difference between having registrars actually saying what level of security they're implementing as part of their marketing material or their services. And at the same time having a list which is drawn up like a table of all the registrars out there and comparing them and showing which ones are implementing what (unintelligible).

I agree that such a list would probably then be an absolute road map as to showing which ones are the weak registrars that any hacker would have a great time playing around with. And I think that such a list, if it does get - if the group does decide to do or draft, and maybe it is outside the scope of this group. But if there is a decision to draw such a list, I would say that it would need to remain confidential. Thank you.

Mikey O'Connor: Well, I think that certainly that's one approach. I think that they should do is --hijack my own title here - (unintelligible).

Olivier Crépin-Leblond: May I just add to this please? Olivier still, thank you Mikey, Olivier. I was going to say it should remain confidential. But that said, if such a list does get drawn up, that list should be shared with the incumbents and so it would serve as a case of get your act in order, it looks like you are - you're a weak point here. But I'm not quite sure how that would be transmitted, what channels of communication would be used. Thank you.

Mikey O'Connor: Another approach to this would be to make the list a pass/fail list. Not a pass/fail list, but essentially a list that only lists registrars that are, you know, going to be able to resist attacks.

(Cheryl Himagi): That still points the others out by omission.

Mikey O'Connor: Yes, but the nice thing is there's thousands of others. And so, unlike a table which says this particular registrar has not implemented this defense...

(Cheryl Himagi): Yeah, yeah, yeah, I'm with you there.

Mikey O'Connor: It's a much less helpful road map for the attacker.

(Cheryl Himagi): For the less savvy attacker perhaps/

Mikey O'Connor: Yes. So, -- and I'm - I got to change - you know, we have to remember that the original proposal was registry, registrar, and even registrant in some cases, security. So, it's not just registrars that - be listed here. So we have to come up with another term.

(Cheryl Himagi): Well, many of these things end up to be a whole chain.

Mikey O'Connor: Right.

(Cheryl Himagi): And you'd - a little bit later on in our process, I'm actually looking forward to the point in time where were looking at critical risk points and parts where on analysis it's a failure or potential failure point. In which our higher or lower likelihoods and things like that.

Mikey O'Connor: Yes.

(Cheryl Himagi): I get all excited at that point in those processes.

Mikey O'Connor: And yes, that's the analysis part.

(Cheryl Himagi): Yes.

Mikey O'Connor: And...

(Cheryl Himagi): I'm not trying to push us there yet, I'm just saying that too will come.

Mikey O'Connor: Yes, and I think that gets back to this question that I've got for the group, which I'm noting it's two minutes until the top of the hour. I guess I'm not going to get to that today. But - which is how quickly do we want to go through this assemble a list of threats cycle.

I just realize that I lost track of time. So, (Olivier), you got your hand up and then I'm going to have to wrap this up for today.

Olivier Crépin-Leblond: Thank you Mikey, (Olivier) here. I guess I'd really like to hear from the registrars and the registrees on this specific point. There is - I can see - I can foresee some opposition to something like this purely on either commercial grounds or on the fact that some business models do not take into account demand for a high level of security. Because it's for a small communities or - it's a big - it's a very large subject as such. It doesn't seem to convert so. It'd be interesting to engage registrars and registerees as early as possible into this.

Mikey O'Connor: Yes, well and I...

Olivier Crépin-Leblond: To find out what they think. Thank you.

Mikey O'Connor: ...I think one of the tricky bits here is that we are getting quite a ways ahead of ourselves in terms of this. This is a recommendation, which is at least two or three steps away.

Olivier Crépin-Leblond: That's the other concern I have, we might be running a little further than we should at this time.

Mikey O'Connor: Yes, I think that's right. I think at the same time, it's good to capture the notes. But, we're a long way away from being able to support or recommend this, I think. We've got some work...

(Cheryl Himagi): Oh, yeah.

Mikey O'Connor: Okay, it's the top of the hour and I hate running long. So, just a very quick show of hands in the Adobe room, whether you - if you would like to continue this fairly slow educational, informative process for building our list, give a check mark by your name.

If you would prefer that this get done in advance and that you're taking - you're being taken through a - essentially a pre-digested documented, indicate that with an X or a thumbs down. I'd just like to take a quick poll of the folks on the call as to your preference on how to proceed.

Well, we're evenly divided right now between folks who would like to continue this and folks who'd like a pre-digested - oh, pre-digested in moving into the lead. Anybody else got opinions on that? You can use any variant of the thumbs up or thumbs down that's clear.

And if you don't know how to do that, there's a little icon at the very top of the screen, which is where you raise your hand. But in that drop down menu, you have other choices as to - thumbs up Arturo, is the slow step by step, whereas thumbs down would be pre-digested.

Probably pre-digested by Mikey, but it stays in this thing. Okay (Mark) and anybody who needs to go, you know, we're getting a pretty strong sense here that pre-digested is the way to go. And so, I tell you what, I

will do that for next call. I'll show you what I've done and see how you like that. And with that, we'll wrap it up. Thanks all and we'll see you in a week.

Female: Thanks, Mikey, bye.

Male: Thanks Mikey.

Female: Thank you.

Male: Thank you Mikey.

Mikey O'Connor: Glen, I think we can stop the recording. And...

Male: Thanks Mike, bye,

Mikey O'Connor: See ya.

END