Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
15 December 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 15 December 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-20111215-en.mp3
On page: http://gnso.icann.org/calendar/#dec (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
• Joerg Schweiger.de (co chair)

NRO Members
• Mark Kosters (co chair) (NRO)

GNSO Members
• Mikey O'Connor – (CBUC) (co-chair)
• Rafik Dammak, GNSO
• Rossella Mattioli – (NCSG)
• Don Blumenthal – (RySG)

SSAC Members

ICANN Staff:
Bart Bosinkel
Julie Hedlund
Patrick Jones
Nathalie Peregrine

Apologies:
Greg Aaron – (RySG)
Jim Galvin (SSAC)
Nishal Goburdhan (NRO)
Roy Arends, .uk

Nathalie Peregrine: Thank you, (Tonya). Good morning, good afternoon, good evening. This is the DSSA meeting on the 15th of December, 2011. On the call today we have Rosella Mattioli, Takayasu Matsuura, Cheryl Langdon-Orr, Rafik Dammak, Mikey O'Connor and Olivier Crepin-LeBlond.

From staff, we have Julie Hedlund, Bart Boswinkel and Patrick Jones, myself, Nathalie Peregrine. We have apologies from Nishal Goburdhan, Roy Arends, Greg Aaron and Jim Galvin. I would like to remind you all to please state your name before speaking for transcription purposes.

And I think Jörg Schweiger has just joined the Adobe room. And over to you, Mikey.

Mikey O'Connor: Thank, Nathalie. Welcome all to what is by far the most complicated Adobe room I've ever attempted to run, so we'll see if this works. The first order of business is always to take a short moment to check and see if anybody has an update to their statement of interest. Okie-dokey.

For those of you who just joined and didn't participate in the pre-meeting chatter, let me just give you a tour of the Adobe room that's in front of you. On the left side is a scale from one to ten that allows us to vote individually, just – on a number. At the very bottom of that, if your screen is quite small this may have rolled off, but at the very bottom of that, if you roll down, you've got a button that says No Vote, which removes your vote from that.

And then the next column, the threat sources – as we go through this exercise, I'll put the range up in that area just so that you know sort of what the numbers mean. So in this case, we're working on the non-adversarial threat sources. We only have one range to cope with, so it ranges from 10, which is a sweeping impact, all the way to 1, which is a minimal impact.

Then the next column is the spreadsheets – the table that we're going to be filling in. And my thought is that I'll just go through section by – you know,

cell by cell, we'll vote, we'll see if we have a consensus emerge. If we do, we'll put it in.

If we don't, we'll discuss it and see if we can arrive at a consensus, and then if we can't, we'll save it for further discussion. And then the last two columns on the right are our normal chat and agenda. So everything's a little bit compressed, especially if you're working on a small laptop screen.

Let me know how this works. If this turns out to be hard for you to use or confusing, don't be shy about saying so, because this is a pretty busy screen and it may just have too much stuff on it. And if it does, I'll rearrange it next time and see if we can get this right.

So today, and I think for the next few calls, probably quite a few calls, we're just going to work through these tables that come out of the methodology, and fill in our answers. And so starting right in, this is Table D8 in the methodology, this is non-adversarial threat sources. And I thought what we would do is just start up with this first one, configuration errors by privileged users.

So these are not – these are accidental or unintended threats to the DNS. These are not malicious threats, we'll get to those in a minute. And so I think what I want to do is just get your opinion on the scale on the far left.

Just go ahead and pound in your number and we'll see sort of where we wind up and see how this works as a way to capture our views. You'll note that as you put your votes in, your name is not associated with your vote. This kind of poll can be configured to do that, but I elected not to because I decided that it would be useful for people to be able to essentially do this anonymously, especially when we get into some of the more sensitive stuff.

This is really a matter of finding the consensus of the group. If we get to a consensus anonymously, then we don't really have to worry about it. If we

don't, then we're going to wind up discussing it on the call and identifying ourselves anyway.

So go ahead and put your votes in, two people have done it. By the way, I'm not at all adverse to the idea of the staff participating in this, especially Patrick, Julie, Bart, some of you who support the SSAC, for example. I think that there is great value in your opinion and so I would not restrict this just to members of the working group.

Now what's emerging is that we've got a pretty good dispersion in this, and so I think what we need to do is let people who are kind of at the extreme ends, right now the range is between 5 and 10, tell us why you think that way. Because you may be thinking of something that the rest of us aren't, and as that comes out, we'll pound the eventual conclusion of all that into the assumptions area. So, you know, why doesn't somebody chime in, you know, whoever voted 10, why don't you jump in and give us your reasoning, because you may persuade the rest of us that this is more of a concern than we thought – or whoever put in the 3.

Don't all speak at once. Come on, come on, come on. Somebody speak.

Jörg Schweiger: Hello, Mikey, this is Jörg for the record.

Mikey O'Connor: Go ahead, Jörg.

Jörg Schweiger: So actually it was me putting in the 3 in there, and the reason for doing so is that I feel that the impact wouldn't be so severe, even if it was for .com and the root, if it was configuration errors for any zone aside of those two, I do not see an impact on DNS itself whatsoever.

Mikey O'Connor: So if we assumed the worst case, because I think that's what we have to do – the assumption for a worst case in this one would have to be a configuration error of either .com or one of the root servers, correct?

Jörg Schweiger: Yeah, that was the first assumption I could figure.

Mikey O'Connor: Yeah, okay, so worst case – let's assume that, that it's either .com or root server configuration error. If we assume that, how does your vote show up there? You know, if we assumed that this was a configuration error to the root or to .com?

Go ahead and change your votes, folks, and let's see if we hone in on a consensus. Jörg, do you still think that's a…

Jörg Schweiger: Pardon, a what?

Mikey O'Connor: So, you know, now what I'm saying is in the assumptions, I'm assuming the worst case…

Jörg Schweiger: Yeah, I got that.

Mikey O'Connor: …that this is a .com or a root server configuration error. And now what does that do to your vote in terms of the number? Does it change it from 3 or would you still think even in the .com or root server configuration error…

Jörg Schweiger: Jörg for the record, once again. Let me put it the other way around. Could anybody voting 10 describe the scenario that is so severe that it rectifies to vote it 10?

So who is thinking of which kind of scenario that would be devastating to the DNS? I would love to hear such a scenario just to change my voting. But for example, if I – if you've been listing, for example, WHOIS, well if something's happening to the WHOIS, is that really going to be a problem?

I doubt that. So my question still would be misconfiguring something, what might be the worst scenario of misconfiguration and what is somebody else envisioning of what could happen?

Mikey O'Connor: Thanks, Jörg. Let me catch us up, there's a lot going on in the chat. Mark Kosters is saying .com would be an across the board problem whereas root servers would only affect one constellation of machines, so maybe that's lobbying for a reduction of my worst case scenario. Patrick Jones is saying if it's a configuration error in one or only one root server, there's very likely limited impact if the other 12 are fine.

So Mark is saying it could be a 3 and it could be a 10, and that's where I'm saying I think what we have to do is assume the worst case. You know, I think the assumption that we have to describe is what is the case where it could be a 10 when we call it a 10? And it sounds like it's a .com configuration error.

Who's our lonely 10? You have to reveal yourself, speak. Ah, Rosella is coming back in, maybe it was Rosella. Olivier, go ahead.

Olivier Crepin-LeBlond: Thank you, Mikey, it's Olivier for the transcript. I didn't score the 10, I scored the 6 on this. I can understand the possible, potential disruption of configuration errors by privileged users.

There was actually an instance quite a few years ago that took place that – I think it was – was it InterNIC at the time or was it already called Network Solutions – where they made a boo-boo in one of their configurations and the .com zone didn't reload properly. And so it had a vast amount of – it caused a vast number of problems because the zone might just not reload if there is a major configuration problem, which is sometimes just done through a comma or a semicolon or something that was mistyped, or a space or a tab at the wrong location. However, I do understand that these days there are a lot more processes and no one actually edits the zones directly, so I can

imagine that any operator input configuration error would probably be caught prior to it going live.

And so that's why I've scored it a 6 and not a 10. Thank you.

Mikey O'Connor: That's a pretty articulate summation of what was going on in the chat.

Jörg Schweiger: Mikey, this is Jörg, for the transcription.

Mikey O'Connor: Go ahead, Jörg.

Jörg Schweiger: Just answering Olivier's remarks, nevertheless, for example if there would be some problems occurring with the reload of the zone, well what would we end at? The worst thing that could happen is that we were still writing on an old zone. Well, does that really affect the DNS itself? I doubt that.

Mikey O'Connor: Yeah, I think that the – and we also have to be careful to separate, you know, if the major zone files and major root servers are pretty well protected from configuration errors by well-written software, then I think we have to downgrade this risk, because it would be hard for someone to make a configuration error unless they could override it. Oh, Rosella can't hear, we've lost our audio on the bridge? No, it's there.

That's too bad. Rosella, you might want to try coming into the room again and maybe that – because the room is broadcasting the audio. Of course, you can't hear me say that, argh. Could somebody kind of type that all into the chat for Rosella and let her know that the audio is working on the bridge and that she might want to retry?

She's the one that scored the 10. So what I think we're kind of honing in on is sort of a mid-case range, 5-ish, 6-ish, 3-ish. If we were to – let me clear this poll and – although I don't want to – well, yeah I do, because Rosella can't – there we go.

Yikes, what have I done? Help me, it's flashing back and forth. There we go.

So configuration errors are harder, says Mark. Not because software is more robust – oh good, it's working, hooray. So Nathalie, I think Rosella's back.

Mark, are you able to speak or are you so totally muted – can you speak through your computer speakers or something? I think we need a little clarification of what you're saying in the chat. Mark is saying it's not going to work well if he does that, for the transcript.

We'll pause for a minute and let Mark do it. Why don't we go ahead and revote and see sort of where we wind up? This may – we're coming in at a few people at 5, still some folks at 1.

Why don't we just go ahead and – or 3, I'm sorry. The other votes there – I'm going to sort of declare a 5 unless somebody screams, because I want to kind of move us along. This is taking quite a while.

So it looks like we're heading towards 5. Let's call that one a 5. Oh, interesting – just put that up wrong – oh, here we go, we'll ease all this stuff in there.

Sorry about the learning curve, folks, but okay. Jörg, are you still at 3? Are you willing to go along with a 5, or is that a heartfelt 3, in which case we wouldn't, that's part of the consensus.

Jörg Schweiger: This is Jörg. Mikey, are you addressing me, I was just fiddling around with the keyboard and so I didn't hear you well. Were you asking me?

Mikey O'Connor: Yeah, are you at 3…

((Crosstalk))

Jörg Schweiger: Yes, it's still me with the 3, yeah.

Mikey O'Connor: Okay.

Jörg Schweiger: Because when I go through the definition and the definition is saying wide-ranging, involving a significant portion of the five resources of the DNS, and given all the redundancy we really do have and given the assumption that this is a configuration error that is not by intent, so I really doubt that there would be such a massive impact. Because usually, you do not administer each and every root server and you do not administer each and every server that is, in a way, associated with name serving for .com. And if you just do not do that, then I just do not see a wide-ranging proportion of the server resources that would have been affected, so that's why I'm still lobbying and advocating to downgrade this issue.

Mikey O'Connor: Okay, fair enough. How about you 5s, what do you think? Are you willing to go with Jörg on that? If you are, go ahead and change your votes.

We have three holdouts. One of you holdouts, tell us why you want to keep it at the wide-ranging level. I think Jörg raises a good point there.

Mark is typing away. Anybody who can speak, want to jump on the…

Patrick Jones: Hey, Mikey, it's Patrick.

Mikey O'Connor: Yeah, go ahead, Patrick.

Patrick Jones: If you're going to repeat this for the next call or two and hopefully there'll be some additional participants on the next call, it might just be the best to sort of note that there were four people that thought this was a 5 and three that were a 3, and rescore it, and maybe the score changes a little bit over the next few calls.

Mikey O'Connor: So just put a range in, maybe, and then revisit it.

Patrick Jones: Yep.

Mikey O'Connor: Yeah, that's a good idea, I could buy that. I may break my own…

Patrick Jones: Just an idea.

Mikey O'Connor: Yeah, that's a good idea. I'm going to have to – sorry folks, I'm going to have to do a little spreadsheet manipulation here, because I think I have some – oh, God, where is it? All right, I'll do – I'll put it here.

Ha, there we go, good deal. Because if I put it in here, it's going to – if I type – it breaks my – I got too cute with this spreadsheet and I have an error check in there for that. So let's leave – that's a good idea.

Let's see, oh okay, we've got a thing in the chat. Mark is responding to Jörg's question, wide-ranging? And Mark is saying because it is, it could be bad if it's a .com configuration error.

We had one in '97. Rosella is with Mark. Mark says it burned down the Net for 24 hours and Rosella's then asking a question, is DNSSEC covered by this?

Yeah, this is configuration errors by privileged users, and I didn't put DNSSEC in there but we certainly could. So let's – Mark is saying – well, this is – oh, really, why – dang, I wish – Mark, next call you have to be on the dang conference call. This is too hard having you type this whole thing into chat.

Mark is saying I would only have it be DNS on configuration errors. And I guess the question is why, so Mark, go ahead and type your answer in there. Or if there's somebody who can speak, for crying out loud.

What a ridiculous thing to have a conference call where nobody can speak. Note to participants, please log on to the conference call in the future.

Man: Okay.

Mikey O'Connor: Okay, you speak.

Don Blumenthal: This is Don, am I being heard?

Mikey O'Connor: You certainly are. Go ahead, Don.

Don Blumenthal: Okay, at least I got it right this time. One thought off the top on DNSSEC is are we talking about now or later? I mean, would a configuration error now on DNSSEC really have that much effect as opposed to later on when it's a lot further deployed?

Mikey O'Connor: Well, that's a good question.

Don Blumenthal: Question, I know.

Mikey O'Connor: Yeah, I don't know, you know, I think that's a question for all of the cells. I think one of the questions, which I've sort of presumed an answer to, is that we do the worst case. And I think we would have to put that in the worst case category.

So I think if we were to follow the worst case rule, then it would be whenever it was the worst case. So if the future is the worst case, then that's the case we'd have to put in.

Don Blumenthal: Okay.

Mikey O'Connor: So I think we need some more stuff in our assumptions. Oh, not that way – I'm learning a lot about how not to do this. Let me think about this.

Don Blumenthal: It's Don again, just curious the way these votes are breaking out. Is a conclusion of a 4 an option?

Mikey O'Connor: You know, if it was – if everybody moved their vote to a 4, I think then we could call that a consensus. If we have…

Don Blumenthal: Okay, I gotcha.

Mikey O'Connor: …two groups, one holding a 5 and one holding 3s, then we don't really quite have consensus and it means that we've still got a topic for conversation. So if everybody agreed that it was a 4, then I think we'd be fine with that. But in consensus we don't force that, because what dispersion in the results means is that we still have discussion to have on this.

Don Blumenthal: Okay.

Mikey O'Connor: And so I see a fair number of people moving towards 4, but still some 5s. Anybody in the 5 camp want to hold out for that? Or shall we call it a 4?

Mark Kosters: Sure, Mikey, let's call it a 4.

Mikey O'Connor: Hey, I love that voice. That sounds fine, what's the big deal here? Or did you jump on the conference call?

Mark Kosters: I only have so much battery left – life on my phone.

Mikey O'Connor: Ah, I see, the old Mark Kosters' I don't have enough battery excuse. I've heard this excuse before.

Mark Kosters: It's worked before.

Mikey O'Connor: Well, it got a similarly grumpy response from your Co-Chair, as I recall. So why don't you put a standing item on your calendar for Wednesday night that comes up and says, charge my battery. Okay, we are at 4.

Hey this is pretty cool, the way we did this. I like this.

Mark Kosters: The problem here, Mikey, is that – I mentioned it before – is if you have a single organization running a core service like VeriSign does with .com, and there's a config error, it's across the board. Whereas, if you have a config error in a root where there's multiple administrations running it, administered by multiple organizations, then it's less of a problem. And then you have other services like WHOIS, which people like to have, but is not entirely reliant on it as a service that needs to be up 24 hours a day.

Mikey O'Connor: Right.

Mark Kosters: So you have a, you know, you have so many variant degrees, it's hard to sort of come up with a number.

Mikey O'Connor: Well, and part of what we, I think, are doing as I listen to us talk, is we're combining the threat source conversation with the threat event conversation. And I think that what we do in this one is we get ourselves to the place where we find a tentative worst case and we evaluate it that way. But then when we talk about WHOIS server versus root server versus .com versus DNSSEC server, those are actually threat events, and we get a chance to put these together…

Mark Kosters: Okay.

Mikey O'Connor: …as a – but…

Mark Kosters: So if we do that, if we do a worst case and say okay, .com, and I've had personal experience with this – it melted the Net for 24 hours.

Mikey O'Connor: Right.

Mark Kosters: And it made front page headlines around the world in '97 when that occurred. And so then it's a 10. But if I was on the outside, I'd say, "Well, why did someone score a 10 on the WHOIS service being down, that's crazy."

Mikey O'Connor: Yeah, that's crazy. And see I think that where we get to solve that problem is when we do the threat events combined with threat sources, which is coming up a couple of tables…

Mark Kosters: Okay.

Mikey O'Connor: …down the road. And there, what we can say is, well, a configuration error of WHOIS is a non-event, whereas a configuration error of .com is a huge event. And so I think that what this is is a hunt for the worst case which we then stick into the assumptions.

Man: Okay.

Mikey O'Connor: And then rating the worst case – and in fact I think as this conversation is going on it's – this is a really good conversation about threat events that – what I'll do is I'll go listen to the transcript and pick off the threat events that we started describing in here.

Man: Okay.

Mikey O'Connor: So, you know, this is all good. It feels slow and painful and halting but in fact I think it's – it's quite productive. Bart, go ahead.

Bart Boswinkel: Yeah, I may be a bit daft but what do you mean by worst case and – excuse me – in this context? If you look at sources and have a worst case you start combining it almost automatically with say the – with the event itself.

Mikey O'Connor: Yeah.

Bart Boswinkel: But if you want to separate the two it's very difficult to talk about worst cases as well in my opinion but…

Mikey O'Connor: Yeah.

Bart Boswinkel: …I may be daft.

Mikey O'Connor: No I think you're not daft; I think that's part of the reason we're having so much trouble. And I think part of the problem is in the methodology which is the methodology says go through and identify your sources of these, you know, these non adversarial threats. Well we did that pretty well I think.

And then it says well tell us the range of effects. Well you kind of can't unless you make these sort of assumptions about well, you know, what are we talking about? Are we talking about the WHOIS servers or are we talking about the .com zone?

And so I don't think that we're crazy when we're having trouble with this. I'm not exactly sure how to proceed however. I think actually we're on the right track because the conversation about the worst case was actually quite productive in terms of identifying some threat events that I'll just capture after the call and throw into the pile.

And the range of effects number may not matter a whole lot except as a conversation starter for the, you know, the worst case and the threat events that that implies. So, you know, I'm pretty comfortable that we can sort of go ahead and have this conversation and get a lot out of it and at the end of the

day we may come back and say, you know, the numbers are completely silly but we can come up with numbers much later in the game when we put these together as source and event.

So let's stumble along some more. I'm kind of into muddling through and stumbling along. So we'll see how we do on a couple more. Okay I'm going to try and clear this pole without making it blink our screen like crazy. That's a lot better.

All right so now we're onto the next one. And I think that in many cases the threat events are similar in this one. You know, it would have to be a business failure of VeriSign or somebody else. I don't know, let's talk about what Barb brought up in this context. I mean, because if we said – if we presume that it's VeriSign that fails then we wind up, you know, kind of with all 10s. If we – and do we want to do that? I just don't know. Thoughts, people?

Yeah, I agree with Jörg. Jörg is saying it seems like we're voting on how good a job VeriSign is going to do. And that may be a key conclusion that we reach is that we have one key provider in an architecture that's designed not to have that. Patrick is saying again it's a big range; we've had register fly with 2 million names under management. That's an example from the registrar space.

Other thoughts, people, on our assumptions behind these? I mean, what we could do is we could say leaving VeriSign aside what do we think the range of effects is so that we take one, you know, that one sort of skewing example out of the pile. Olivier, go ahead.

Olivier Crépin-Leblond: Thanks very much, Mikey. It's Olivier for the transcript. I think that we should not leave VeriSign aside. And the main reason is because it actually is a threat that could happen. We could see future other behemoths in the industry. At the moment it looks like VeriSign is the biggest person or

the biggest elephant in the room but there might be others that would be created or might be created through the new gTLD process.

And so it is, at the moment, likely to affect a lot of people. And it certainly is a threat. So I don't think that we should just take the biggest threat out there out of the equation and think well because the biggest threat is not there then we don't really have a threat.

Mikey O'Connor: Pardon me while I screw up your screen. Yeah and the other one that comes to mind is Go Daddy in the registrar space, another large player. But I'm wondering if we aren't – I mean, I wasn't thinking of taking it out all together. I guess what I was thinking of doing was saying we've noted that all of these non-adversarial threat sources or at least quite a few configuration error, business failure, key hardware failure, key networking failure, would be a 10 if it happened at VeriSign.

And so we want to note, you know, we want to note that and put it aside and then say for all other cases what's the impact. But I don't know, any thoughts?

Olivier Crépin-Leblond: Mikey, it's Olivier.

Mikey O'Connor: Yeah, go ahead, Olivier.

Olivier Crépin-Leblond: Thank you. In our question we actually put business failure of key provider so I would say that a key provider is an organization like VeriSign.

Mikey O'Connor: Yeah.

Olivier Crépin-Leblond: Non-key provider is an organization like xyzocl@gih.com type.

Mikey O'Connor: Yeah.

Olivier Crépin-Leblond: And so if we asked a question as business failure of key provider then yes it's going to be high.

Mikey O'Connor: Yeah, okay fair enough. Yeah, that's true. That's true. Okay that's – unless people have more clarification what we would do and then – oh Patrick added an important point that there are only a few players in the data escrow space. Mark noted that he tentatively put in a 10.

So why don't we go ahead and see how we feel about this. Use your little voting deal. Let's see if we've got lots of votes for 10 in which case – oh 8, 9, 10 coming up high. Oop, one 5. See how that's shaping up. Certainly 8-10-ish.

So somebody put in a five. Why don't you chime in and let us know why you're thinking only a 5?

Jörg Schweiger: Guess who, Mikey?

Mikey O'Connor: Oh it's Jörg again. Go ahead, Jörg.

Jörg Schweiger: Well, so Jörg for the transcript. Actually it depends on how we would define business failure. And if my recollection is correct then business failure was, for example something like bankruptcy of a different organization. And well if some – if that – first of all is that correct or what do we mean by business failure? Or is this just some kind of business process performed by a certain entity that is not working correctly?

Mikey O'Connor: No it means that the entity (unintelligible). It means bankruptcy or injunction or, you know, some business event that stops the organization from being able to do its job.

Jörg Schweiger: Okay so in this case it's probably once again a bit of a problem for me to distinguish between the threat source and the range of the (attack) on one

hand and the likelihood that has come into place quite naturally on the other so…

Mikey O'Connor: Yeah, but that one we get…

((Crosstalk))

Jörg Schweiger: And definitely I'm not advocating that VeriSign – nothing could happen to VeriSign but I would strongly doubt that even if it would there wouldn't be somebody in place to just pick up their business and make sure that the DNS for .com – and that's what we are talking about as an impact – is still maintained. So it might – it might have some impact but I strongly doubt that it really would have a severe impact because somebody is going to step in and that's why I put in a 5.

Mikey O'Connor: Yeah, except that I think there again we're making the mistake of conflating – combining the threat events with the threat source. And in this…

Jörg Schweiger: Yeah, I agree.

Mikey O'Connor: …I think we have to say, I mean, what we could say is – to clarify this is a business failure of a key provider for which no failover or, I mean, you know, that's the whole failover registry failover process which I think Patrick might have had a lot to do with writing that report. But there's an SSAC report about that in which there's, you know, and I think – I don't know the history very well but I think it came out of the RegisterFly failure.

So I think that we can go ahead and presume an unmitigated problem for this that if it occurred without appropriate failover what would the impact be? And it would be pretty broad. And then we go into the discussion of – because where I think that leads us is okay where do we have to concentrate our attention and resources to make sure that this doesn't happen?

And I think that comes later in the analysis when we do the threat events and then the likelihood discussion and also the mitigations because I think where that conversation leads us is to a conversation with VeriSign that says well do you have a failover plan that handles the possibility of a business failure of VeriSign?

If the answer is no then I think we've got a different situation to document than if they say oh yes we do, we've got these agreements in place and, you know, etcetera, etcetera. Oh, hello, sorry. Kill off an application that's being annoying. There.

So given all that, Jörg, would you be willing to sort of ride up into the 8-10 range or do you still want to advocate for 5 on this?

Jörg Schweiger: Yeah, I absolutely agree to what you just said before. If it would come with the additional condition saying if there wouldn't be something in place to make sure that bankruptcy doesn't happen then it's okay with me. And again I think it's very valid to say it all comes down once again to the question if VeriSign is doing a good job over there or not.

Mikey O'Connor: Right. Well but, you know, some of these escrow providers and so on. So what if I typed a little caveat into our definition that says business failure without a failover path? Does that do it? Olivier go ahead.

Olivier Crépin-Leblond: Thank you, Mikey. It's Olivier for the transcription. I think that we are just identifying threats here and perhaps identifying this threat as being high will provide the answer as to what kind of recommendations this working group should make. And certainly the working group should probably, as seen from how we feel about business failure, make recommendations about having such scenarios in mind and failover scenarios in place for not only for VeriSign but for everyone else, for each one of those organizations.

And I know that this is in the works so, you know, obviously we can just highlight that although we have identified this as being a very high threat there are scenarios in place at the moment or being designed at the moment. Thank you.

Mikey O'Connor: Yeah. And I'm positive that the mitigation is identified later in the methodology that we get to capture that at a later point. So last call, Jörg, I'm going to sort of lobby for a 9-ish kind of vote on this unless you throw your body on the tracks. Are you okay if we went into a 9 on this one, Jörg?

Jörg Schweiger: I'm not feeling comfortable with it but, well, okay if…

((Crosstalk))

Jörg Schweiger: …record my objections here.

Mikey O'Connor: Okay, all right. Okay a lot of this recording is going to happen after the call by the way because I have finally reached my limit; I can't do a mine map of the conversation and all this other stuff at the same time.

Okay it's – we've got – let's try one more just clear out our answers. Now we're on the nation state. These are the accidental ones. And when we were describing this before these mostly fell into examples like legislation in the US like SOPA – SOPA stands for whatever it does, I don't know. But, you know, badly thought through policy or legislation or law that accidentally breaks the root.

And I think that an example of the rationale for that could be found in the paper that Steve Crocker and all those other folks wrote that was quite concerned about the impacts of some of these legislation. So I've seen some folks come in in the 8 and 9 range.

((Crosstalk))

Mikey O'Connor: Go ahead, Mark.

Mark Kosters: So this is Mark. Is this a state that would be core to the Internet use? Like I think about Singapore, United States or England or the Netherlands or Germany where there's large exchanges.

Mikey O'Connor: Right.

Mark Kosters: But places like Iran, you know, yeah so they're isolated and they have their own sort of firewall or China on the other hand. They are of little consequence for those outside the country but for those who are inside the country it's a different story. So how do we measure this?

Mikey O'Connor: I think we're doing a great job of describing threat events again.

Mark Kosters: Yeah.

Mikey O'Connor: And so I captured one dimension of that. And I think what we have to do is assume a worst case that it's a country that's central to the infrastructure like the ones you rattled off that, you know, makes a mistake. But then I think what we do is when we list off our threat events we describe those others so that we can say – so that we can put that nuance into our evaluation of those.

Rosella, I added Russia to it. Patrick added…

((Crosstalk))

Mikey O'Connor: …and SOPA might be an 8-10 whereas a small ccTLD taken out accidentally by a nation state may…

Jörg Schweiger: Mikey, this is Jörg for the record.

Mikey O'Connor: Yeah, go ahead, Jörg.

Jörg Schweiger: One aspect to this we are talking about something that would happen accidentally, right? We are not talking about the ethereal track but we're talking about something that by accident would happen. So my question towards this would be how do we evaluate the risk if we do take into account that this very state or this very nation is doing that by accident?

It might be a different story if US government or whoever would pursue certain rationale but if we are just not voting for this in this very section I don't feel that the evaluation should be as high as it currently is.

Mikey O'Connor: The distinction that we made when we listed these is that we have nation states sponsoring adversarial threats with the intent of breaking the DNS in our adversarial threat sources.

Jörg Schweiger: Right.

Mikey O'Connor: This one is where a nation state – and I'm going to stick with the US example because it's just current. They are not intentionally in the SOPA legislation trying to break the DNS.

Jörg Schweiger: Correct.

Mikey O'Connor: They're trying to accomplish a different agenda (about) the whole IP thing. But it's an unintended consequence of legislation that if, you know, if it passes could have pretty destructive impacts on the DNS. And so I would separate the adversarial attacks from this kind of an attack. And it's not an attack…

((Crosstalk))

Mikey O'Connor: Go ahead.

Don Blumenthal: It's Don. And I noticed Patrick posted a comment in the chat room. I'm having some of the same discomfort I think with this concept of (unintelligible) versus not when it comes to national legislation. I've been up to my ears and beyond in SOPA and the other legislation.

And, you know, these bills are deliberately written the way they are. And I'm having trouble with saying that the effects on the DNS are accidental.

Mikey O'Connor: We could take this one out of our non adversarial threat sources. That's what I'm hearing you saying is that right? And then Patrick is agreeing with you. Jörg, is that what you're saying too essentially that…

Jörg Schweiger: Yeah, absolutely. Everything is done deliberately and if something would be done unintended it wouldn't have such a severe effect as currently being indicated by the votes.

Mikey O'Connor: Oh okay.

Jörg Schweiger: So we might just remove it.

Mikey O'Connor: All right well that's…

Don Blumenthal: It's Don again.

Mikey O'Connor: Go ahead, Don.

Don Blumenthal: Part of the problem is that something can be introduced and at first glance it's, yeah, unintended consequences. But when you have repeated statements explicit or implicit that we don't care it moves the agenda to the deliberate.

Mikey O'Connor: Where – does anybody object to the idea of taking this one out of non adversarial threat sources altogether tentatively? Okay I think then that's what we'll do. Oops I'm confusing which screen. I'm going to make a note here. Okay it's one minute to the hour and although this felt a little awkward at least I feel like we've been having a pretty substantive discussion that's been really productive.

So let me take this last minute to just do a kind of a check-in on how this process feels to you. Is this feeling productive to you or not? Should we essentially carry on this same way next time? Is there something I should do differently? What are other people thinking?

Don Blumenthal: It's Don. It felt a little awkward at first but once things got rolling and there was more back and forth I thought it was working well.

Mikey O'Connor: Yeah, I'm really glad that we're recording this because there's a lot that's going by that I'm going to have to back and listen to the transcript to capture. But it's, you know, we're all sort of learning this together. And at least for me it felt like it started to get not too bad.

Okay it's the top of the hour. I'm going to wrap it up and we'll – I don't remember are we meeting next week or not? We are, right? Nathalie, can you remember right off the top of your head whether we're having a meeting this time next…

Nathalie Peregrine: This was yet to be confirmed; it hadn't been decided yet.

Mikey O'Connor: Oh that's right. Okay so I'm going to give a very quick poll. I'm going to clear this one and I want you to put in a 10 if you're available next week, which I am so there's my vote, and put in a 1 if you're not. I just want to get a sense as to whether we should meet again next time. It's looking like at least four people can, five. All right so we'll go ahead and meet again next week just before Christmas, Holiday season starts at least in the US.

And Bart is suggesting that we look again at the distinction between sources and events. Yeah, that's definitely a lesson learned for me today, Bart. I'm going to reflect on that and see if there's a way to fix that. It may be that the way to solve this is to jump forward one table in the methodology because I think there's a table where we put threat sources and events together and I kind of want to think about that a bit so I will take an action to do that.

Mark is saying he likes the voting stuff. Two weeks from now will not happen, Don, that is correct; that's the intersession between Christmas and New Years in the US and so much of the ICANN staff is on vacation and many I think of the participants on this working group as well. And, yeah, the day indeed will happen; the meeting will not.

Okay I think that's it, folks. Thanks a million. We'll see you in a week. That's it for me. Nathalie, do you want to shut down the recording?

Nathalie Peregrine: Thank you. (Tonya), could you please stop the…

END