(Closed Meeting)
ICANN - Singapore
Incident Repository Implementation Working Group
23 June 2011

>>BART BOSWINKEL: Let's get started. I'm Bart Boswinkel. I'm -- yeah, I'm ICANN support staff. As a starter, we just do a round of introductions. So I'm Bart Boswinkel.

>>ANTOINETTE JOHNSON: Good afternoon. I'm Antoinette Johnson. I'm a new volunteer for the working group from NIC VI.

>>MOHAMED IBRAHIM: Mohamed Ibrahim. I'm also volunteer, but I'm also on the ccNSO. But my issue is, when I'm in Somalia, I can't get access to the Web. So only when I'm in Nairobi or here. So you see more of me when I'm around. Next month you'll see more of me.

>>LUIS ESPINOZA: Luis Espinoza from dot CR. I was working in the working group that suggested the creation of the repository for this working group. And I'm interested to keeping the job.

>>KRISTINA NORDSTROM: Hi. My name is Kristina Nordstrom, and I'm with the ccNSO Secretariat, so ICANN support staff.

>>GABRIELLA SCHITTEK: I'm Gabriella Schittek, ccNSO support staff. And, Hitoshi, you're on the phone. Could you say something about yourself?
Can you hear us?

>>HITOSHI SAITO: Yes.

>>GABRIELLA SCHITTEK: Hello. Can you just introduce yourself.

>>HITOSHI SAITO: Hello, my name is Hitoshi Saito from dot JP.
(Indiscernible)

>>BART BOSWINKEL: Did everybody hear it?
Okay. Let's continue. We have apologies from Zoran Vlah, who is also in this working group. And he couldn't make it to this meeting. And I think the Wim Degezelle is coming. He's an observer from the European regional organization.
So okay. A couple things. And I will say -- I will start off, because that's probably the easiest. There are -- at this stage, there are a couple things the working group needs to do. The first and probably most important one is to nominate a chair. That chair is -- will be appointed by the ccNSO council at its upcoming meeting. But, as soon as we have a chair, then he or she can -- yeah, it's easier. It's very uncomfortable if ICANN support staff needs to act as chair. It's -- it's this working group is driven by the volunteers, like every other working group in the ccNSO. So that's one. The first one is nomination of chair.
The second one, if you look at the charter of this working group, there are a couple things this working group needs to do. And its first main task will be to develop a kind of a work plan with a schedule, so there is a bit of an idea how we want to progress. And it's probably very -- it's very clear we can't do that here during this meeting. Because that will be

very difficult.

But maybe it's an idea for those of you who do not have a full understanding of the charter to have a bit of a discussion about the scope and -- of the charter and what it really means. So that's more a suggestion.

The first question is: Is someone of you -- before we go into that, is someone of you willing to act as chair?

Doesn't have to be at this meeting, but, say, at the upcoming meetings. Luis?

Yeah?

Okay.

>>I second that.

>>BART BOSWINKEL: We've started. And we gave already an introduction of you, an observer from the European regional organization. Okay. But he has arrived. And we have a chair.

Do you want to do it from here, or do you want me to continue to give a brief introduction into the charter? It's now up to you.

Okay. So the charter of this working group, as I said during the ccNSO meeting, it builds upon the incident response planning working group. And so what they've done, I would say, they've identified four or five major -- or that working group had a couple of results. I think the first one is they defined a contact repository, the details for the contact repository. And they are all quoted in the charter itself.

The second thing -- and probably the major achievement -- is for that how the contact details or how the channel, in which instances the repository should be used. So that's more the use cases, as they called it.

The third major result was -- that's why they stopped, in fact, is they identified possible ways to set up this repository. So that was the planning. And this working group is taking up from that part of the working group. So that's dealing with, at the end of the day, with buy or make decision. It is the -- and, in order to answer that question, then you have to have a bit of an understanding and develop kind of models for how such a repository could be run. So that includes financial models or funding models, and that's not just -- it's a -- installing it, but also for maintenance and for operation.

And it's -- and then you have -- once you have insight in that, so for the make decision and for the buy decision. If you have a reasonably oversight of what is involved and what are the different elements of running such a repository, then we have one side of the equation.

The second side of the equation, which is also in the charter -- and that's probably, from a cc perspective, is very important -- is how will this model or how will this repository be funded. And there are different funding models, and I think they were also identified in the rudimentary in the oversight of the planning working group. But it was out of their mandate to really delve into it. Say, for instance, you could -- you could foresee something that maybe ICANN should fund it from the SSR planning budget. That would be a suggestion. You could seek outside financial contributions. That's a model for funding. Or from the ccTLD community itself. But then you have questions how do you collect the money and how do you deal with, say, the smaller registries, the real small registries? There are some ccTLD registries out there with just 200 domain names. So then the funding -- for them, the funding can be a real issue. Just to give you an example, which you've seen it, as a result, say, the incident response planning working group already was in touch with one or two external providers. And I think, initially, was $1,500 or something to get registered. And on a year basis, it is almost -- yeah, don't quote me on the numbers -- but it was 800 to 1,000 U.S. dollars to maintain and, et cetera, the contact details.

So, if you do that year in, year out, that's a very expensive operation, especially for the smaller ones. So it's -- it's going to be quite an exercise. But at least that's something you can do.

So these are, initially, the two major tasks for the working group. And as -- once we have -- the working group has completed these two major tasks, then the intention is to get back to the community and come up with, say, a reasoned proposal based on this and see where the community wants to take it. And, if we have that feedback, it goes back to the council with the recommendation from the working group. And, depending on the recommendation of the council, then the working group will be asked to really start implementing it in the sense of organizing the implementation, either if it's going to be an external party, manage the RFP process, et cetera. That's later on in the game, if we ever get to it.

So my suggestion would be that, say, as a first start, we start thinking about a work plan and what should be included. And maybe the chair and we together could develop a work plan that can then be discussed online and/or on conference calls. And then, once we have it, then we have a reasonable oversight of what needs to be done and who can do it and maybe ask for additional volunteers. Because I think what is -- what is, at least in my mind is very clear, this is quite an extensive exercise, if you want to do it properly. To come up with funding models, et cetera. Maybe we could use the expertise from the finance working group as well. That's, again, an option that we could include in the finance -- in the work plan. But that's just brain dumping. Are there any questions at this stage?

(saying name) Are you clear on this?

Hitoshi?

>>HITOSHI SAITO: Hi.

>>BART BOSWINKEL: Do you have any questions or any comments?

>>HITOSHI SAITO: No.

>>BART BOSWINKEL: Okay. So I think to make it a bit more substantive this meeting, I don't know if any of you have an idea what could be included in the work plan so we have a bit of a common understanding what everybody expects that needs to be in this work plan in order to move forward. Or you could do it the other way around that Luis and I and,

together with -- that's an alternative route -- but that's up to you -- that Luis and I will start discussing what we think should be included in the work plan and then we send it out.

So, yeah, it's more your preference.

>> I want to hear opinions in this meeting about those two proposals.

>> Well, my suggestion is perhaps we should have a go at it now while we are here and at least agree on the bigger picture or what it is, our terms of reference, I guess.

And then if we have a document, we can take it back and work on it. Might as well, while we're here, utilize the time.

>> And this is...

(Off microphone).

>>BART BOSWINKEL: Okay. Let's -- You have an idea what you want to include in these terms of reference?

>> No, I actually want to look at others, just see if we can learn something from them. But to be honest, maybe I should also read the original document that proposed the working group. That might be another way we can -- But I am open for suggestions.

>> This is my first working group.

>>ANTOINETTE JOHNSON: Mine too.

>> The working plan is for this working group, how we proceed to obtain this --

>>BART BOSWINKEL: That's why it was included.

It is more or less defining the activities the working group will undertake and when. That's in principle. And if possible, you assign already some responsibilities. But it is probably what you normally see in these type of working plans. Knowing, say, these main tasks, how would you break them down, and then assign them to people, and then build on that is -- yeah, it's like starting is project.

>> It's not very different, like other working groups are supposed to experience. I thought we have some conference call meetings and define some lines or subject to work to. Maybe we can share some PowerPoint presentation or something like that with ideas, and discussing in these conference calls.

And about time, I'm not so sure, but we expect -- we mention that can take so long to define some projects, the chapter. Then I can follow the usually way that works the working groups. And I think it's in this way.

>>BART BOSWINKEL: Yeah, generally it's, say, what has been -- I don't know if you attended the FOI working group, but what's generally a very good way is say that initially you start working identifying some topics, and then put them in a kind of straw man document, either PowerPoint, and then you discuss it on these conference calls and we can use the Adobe room. So that's one.

The second thing is, and this is something you need to think about, is how often you want to meet. Some work groups hardly meet and some are very, very frequent, like again, the FOI and we have another joint working group, they meet every two weeks. Yeah, depending on the frequency you meet, you can make a lot of progress.

So, again, that's a question for the working group that you need to answer yourself to how you want to approach it. You want to make it very intensely, at least the first time to get up to a working plan, that's your choice.

>> I can suggest once a month. I don't know if that's okay for you.

>>ANTOINETTE JOHNSON: I would agree with that.

>> That's fine.

>> Because if it's a long time between conference call and conference call, the idea is to try to interact through e-mail or something like that to take up some advance and prepare the sufficient information for each conference call meeting I think could be a good way.

You agree with that?

>> For me, it's from 1st of July that I am really on the other side of the digital divide. But that's okay. It's only another week to go. So I guess from then on, it would have been yes, so I am quite happy. But I also like the ccNSO model where the documents are shared and people can -- So maybe we can even have a go at it very soon, send something.

>>KRISTINA NORDSTROM: Can I just note that there will be a Wiki page? And you can use it however you want. If you want me to upload all the documents so they are in one place or if you want to edit and upload them yourself, it's up to you.

>> I was just thinking, wouldn't it be interesting for you if you, just as inspiration, look at the working plan that was made for the previous group? Not to copy and paste it, but just to have an idea. Because I think certain things will come back.

I will try to look at it but I don't have it in my folders anymore.

>>BART BOSWINKEL: It should be on the Wiki. This is Bart.

The Incident Response Planning Working Group.

And I think given this one is building on top of, say -- or using the outcome of that working group, I don't know, for instance, if you are aware of what that working group has produced, if you have seen the final presentation.

>>ANTOINETTE JOHNSON: Yes, I did. I did take a look at -- I think I did. Yeah, I think I did. It was a PowerPoint presentation. Yes. Yes, I did see that.

>> I think I did, too.

>> If not, that will be -- not the recommended. Obligatory reading for everybody in the working group.

>>BART BOSWINKEL: Yeah.

>> The Incident Response Working Group.

>>BART BOSWINKEL: Because I think that's the starting point, I think everybody needs to be at the same speed or same understanding. And we could even ask if there are questions relating to that project, I could ask Jorg Schweiger to address some of these questions from the working group

members so they fully understand it.

So Jorg is -- was the chair of -- yeah, is the chair of the formal working group. So he gave the update here as well as the starting point on -- that was Tuesday, wasn't it? Yes.

>> Yes.

>> Maybe I can share some ideas to let you know and let you thinking about. I was working with the incident response working group, and I was there when we defined the creation of this repository. And, in fact, there's something in my concern about this repository is the maintenance of the repository could be a huge task. Not in the way of technical or money or something like that, but in the way that keep the information of the contacts updated, and have no discrimination about some domain that put some money for -- not put some money for the repository. We need to create something that could be currency (indiscernible) and allow access to all the country code -- all the contacts in this repository. Because when some incident happen this kind of incident don't pay attention if it's a huge ccTLD or a small ccTLD. Simple. It could affect the whole community. Then the whole community must be informed about the incident. The whole community must take the opportunity to report an incident by example. Then this, too, shall be very, very easy to use, very open, and have the information updated every time.

And this could be the most hard thing because it's very easy to set up a new repository and getting many app on there but six months later it's completely outdated.

The hard thing is to keep update that.

And then maybe one of the very good input from this -- from the members of this working group is share some ideas on how strategies to use to keep that information update in the simplest way to be.

>>ANTOINETTE JOHNSON: I have a question. In the repository, you, record the incident? And do you also record the -- what I call the solution?

>>BART BOSWINKEL: It is -- Maybe that's why we have to go back to the -- say, the incident response planning working group.

This repository is about contact details.

>>ANTOINETTE JOHNSON: Okay.

>>BART BOSWINKEL: And given the sensitivity of these contact details for some ccTLDs, and knowing that, for instance, some other repositories, like our own, is not extensive or not up-to-date, is you want to define a set of contact details in case of incidents and who do you need to contact.

And what is defined by the working group as well, the previous working group, in which cases do you want to contact somebody. The next stage could be that, say -- And so that could -- And that means that it could be an external party who uses this for a particular incident. It could be a ccTLD who has an issue and discovers it and wants to forewarn all the other ccTLDs, or it could be ICANN. And that was going, again, a step back in time. That was the reason why it was -- that started this whole process, was the Conficker incident, I would call it.

Is -- At the time, ICANN staff started to push information, and it was not clear, first of all, was this a real incident. People questioned whether this was an incident that they should provide information. But secondly, and that was -- it wasn't clear that the information was coming from ICANN. That was some questions raised. And secondly, they couldn't reach everybody. They had to use the regional organizations. They had to use other ccTLD managers, because their contact details were the ones in the IANA -- in the IANA repository, so the IANA database. Some of them are out of date.

So that was discussed here as well. They are not describing -- They are not accurate.

And other ccTLD repositories -- like, for instance, CENTR has details for ccTLDs who are members, and maybe some nonmembers as well. But again, that's used for different purposes so you always get to the wrong people. So that's another thing you want to -- that is specified already in this repository.

>> Maybe to complement that is this contact repository will be part of our more wide system of incident response than this contact repository (inaudible) half the characteristics to be accessible by X number of incident response systems. It's a good idea to know how will we work this, how we'll work this repository, because it could be access from CCERT or CERTs, something like that, or I don't know if the project of the DNS CERT is going on or something like that going on. But the idea is this contact repository have the trust information about how to contact the responsibles in the ccTLDs. Is it the -- And it should be a tool used by other systems, not exactly a complete incident response tool. This is the idea.

>> So if I understand correctly, then, this working group ultimately will have to come up with solution on how to answer those questions, basically. How do you go about abating the ccTLDs or informing them about incident and so on.

The reason why I was interested in this working group because we were just going through the CERTs and CCERTs in Africa and similar access come up. How do you talk to the CERTs people? And now we are forming AfCERT which is a whole continent. So hopefully I will share that with you as well and there might be something we can exchange or learn from that as well.

>>BART BOSWINKEL: Sorry, this is Bart again. That was one of the solutions that the formal working group already looked at, is, say -- and they came up with, as an example, this model, I think Jorg contacted I.T. something in Germany. I forgot the name. And that is used as a repository by some CERTs in Europe as well, very widely.

But that was very, very costly, precisely for the reasons you just described, for maintaining the contact details. What they did, they contacted the people in the repository every month just to check, automatically. And that makes it very costly.

So it's the maintenance, probably, where you will have considerable issue.

Say building it, because in principle, I think it's a very simple

database. But once you have the data in, then the next step is you need to be ensured that you -- yeah, that the contact details are up-to-date.
And somebody needs to do that.
If the purpose is -- for the purpose it should serve.
>>MOHAMED IBRAHIM: Any timelines, any closure time? Any sunset?
>>BART BOSWINKEL: That's why the first step for this working group is to come up with a work plan. Because then you define your own timeline. And, once you have defined your own timeline, there is more or less -- it's soft commitment to maintain that timeline. Otherwise, you have -- that's the risk of, say, these complex working groups that you run on and on and on and on. Never ending story. That's what you want to avoid.
>>LUIS DIEGO ESPINOZA: Maybe an idea -- I'm not so sure about this. I'm not so sure about this, in a very short time that is realistic. Not realistic. But maybe suggests would be have closings meeting in the next ICANN meeting, having something like face-to-face meeting. And in that meeting we can close with the goals of this, of the working group. I don't know if it's too soon.
>>BART BOSWINKEL: I guess it will be too soon.
>>MOHAMED IBRAHIM: Maybe you have a preliminary report.
>>BART BOSWINKEL: What you probably want to do -- I have no clue. I don't know how -- so it looks very complex at the surface. And is -- and then you need to consider a reasonable timeline, given that you are all volunteers. And so that's a bit of juggling.
>>LUIS DIEGO ESPINOZA: Okay. I understand. Then we can take into account the next ICANN meeting to have a face-to-face meeting to try to push -- because the face-to-face meeting is helpful, because you can push the things faster than the conference. Because the conference sometimes you go slow because it's difficult to communicate and have everybody there. Then maybe -- then the second -- maybe in six months, something like that.
>>BART BOSWINKEL: If you aim for that, you can do two passes at such a work plan looking forward and have some idea in the back of your mind. Okay. The Dakar meeting is very early. Maybe the first meeting in 2012.
>>That will be in Costa Rica. I hope so.
>>So do I.
>>I want to see Brian Ruiz.
>>LUIS DIEGO ESPINOZA: I don't want to keep this forever. I suggest that we can push the things to finish, then, the first meeting in 2012.
>>BART BOSWINKEL: That's my advice. Be very realistic about it. You've got a couple things. Okay. You've got -- say, if you want to have two meetings, for instance, at the Dakar meeting, we can arrange it. So early in the week or maybe later in the week when you have spoken with people. So that's one way of doing it. So that's very clear. So we'll schedule at least one meeting of this working group in Dakar. Also be realistic about the time you can spend on this. And maybe it's just a matter of collating information and seeking to understand the issues first and then writing it up in, say, whatever you want to call it. Maybe something in the progress

report. And that doesn't -- a progress report, as you have seen with the planning working group, could be even a Power Point with some additional lines to it. So a report doesn't always have to be a written report, in my view. As long as the information in there is contained in that report is clear. Because I know drafting will take a long time. Any comment?

Hitoshi, any comments?

Questions? Hitoshi?

Sorry.

>>HITOSHI SAITO: I'm here.

>>BART BOSWINKEL: Any questions or comments from your end?

>>HITOSHI SAITO: No.

>>BART BOSWINKEL: Okay. Thank you. So --

>>LUIS DIEGO ESPINOZA: I have slides here from the past working group, but the slides never go to the final report or something like that. But this idea to clarify the -- could see this repository. And I want to share with you this idea. I have it here. But because we are in -- the idea is there's a contact repository here. Maybe something like LDAP protocol that could be accessed for any order. Incident response system. And it maybe defined some rules here. How could access this repository. And important thing is how to maintain this repository. Yes.

And this is more like -- I like the idea how to clarify what we are doing. And been working in this way, I can send you some graphics with ideas and receive from you some input.

>>BART BOSWINKEL: Yeah. And you all know you subscribe to the e-mail list. We've created a dedicated e-mail list. So that's easy. You all subscribe to it. We have a Wiki page. And so for more, if you want to go outside, say, something like a progress or whatever. So the charter is there. Also, on the dedicated web page for this working group. So these are the -- especially, if you start using this or want to use other tools for presentation, et cetera, and for discussion. And for every call we can set up an Adobe room as well. And they seem to work pretty well for meetings. Because then you have all the things, everybody looks at the same thing at the same time.

So maybe to end the meeting, because we're getting close to 6:00 and --

>>MOHAMED IBRAHIM: I think if you want to share with us, I'm happy to send you a draft work plan, if you want.

>>LUIS DIEGO ESPINOZA: My idea is to send this as soon as possible. This is a draft. But it's to give an idea. And feel free to provide any other comments or things. We can start with this graphical idea what we need to do. And after this we can start to put some more information about this.

>>BART BOSWINKEL: Maybe that's another thing. Say what I'm thinking of is that you can already see, say, having this repository and looking into funding models, et cetera, and for the buy or make, say that's already in the charter, you've got the three phases for this -- for such a repository which are important regarding funding saying, first of all, is -- making it or having it. So this -- building such repository. Either you use already

existing one, or you ask people to make it. So that's part of the cost function. Second one is indeed -- and that's going to be the most difficult one -- is maintenance. And I know the former working group had already some requirements regarding the maintenance. That's in the charter as well. That's the result of the program working group of this previous working group. And I think there is a third phase as well mentioned in the -- if you look at -- it's reasonably specified this one.

>>MOHAMED IBRAHIM: We're panning on sending out request for proposal.

>>BART BOSWINKEL: But that's the next phase. May I have a look at it, please. I haven't seen it for quite some time. What is implement, maintain and operate. So that's -- say, you could have cost factors. And other relevant -- to implement, maintain and operate and maintenance and operate -- yeah, it was used to -- I think operate is sending stuff out when there is an incident that could be -- I think one of the proposers had additional costs when they really have to send stuff. Because, yeah, that's something different than maintaining it.

And the different funding models, it's not just funding. It's also the management and governance models. And governance models is should it be owned by the ccTLD community? But then you have a question -- or managed by the ccTLD community. But then you have a question of, yeah, what happens if somebody leaves the ccNSO or is not a ccNSO member or should it be run by ICANN? And then you have a list of things. That's another way of looking at it. Some of these -- there are two major components from the workload. And they delve into it. There should be a lot of material out there to fill in some of this. It's not more or less explore. It's more providing an overview to see what we can come up with. That's another way of looking at it.

>>LUIS DIEGO ESPINOZA: Okay. Then the first two things we will do is send this report and get a proposal and start with that.

>> Okay.

>>BART BOSWINKEL: Thank you. Hitoshi, any questions from your end or final comments?

Hitoshi, are you still there?

>> He's in Japan?

>> Not too far away. Maybe in the north.

>>BART BOSWINKEL: Hello?

Hitoshi?

>>HITOSHI SAITO: I am here.

>>BART BOSWINKEL: Do you have any other thing you want to add or have questions about or remarks?

>>HITOSHI SAITO: No.

>>BART BOSWINKEL: Okay. Thank you. Okay thank you all very much. This is the end of the first meeting. And we have a chair!

>> Thank you.