TRANSCRIPT

Contact Repository Implementation Working Group Meeting Beijing

11 April 2013

Attendees:

Bart Boswinkel, ICANN
Luis Diego Espinosa, .cr (Chair)
Cristian Hesselman, .nl
Isak Jacobsen, .fo
Antoinette Johnson, .vi
Kristina Nordstrom, ICANN

Luis Diego Espinosa: This Contract Repository presentation working group meeting. The first things I want to do is introduce Cristian Hesselman. Maybe you can tell us a little bit (inaudible).

Cristian Hesselman: Sure. So I'm interested in this working group for two reasons. The first one is because I think that the Contact Repository will contribute to Internet safety, so to speak—Internet safety and stability. So I think that's very important and I think that's also going to be—it's also a potential differentiator between the future TLD community and the new gTLD community. So those are the basically the two main reasons I would like to join this working group plus that I like the topic.

Luis Diego Espinosa: Okay good. I don't know what is the procedure here to having him in the working group but you what is the procedure?

Bart Boswinkel: Normally, you nominate the person and then, officially, he has to be approved by the council which is a no-brainer. So subscribe to the email list et cetera, whether you want to be a full member or just an observer.

Cristian Hesselman: My proposal would be that I start out as a cabinet member, so to speak today because I also have to get some support from my organization. So up until today it will be a cabinet member and then I will let you know whether or not I can join the working group officially.

Bart Boswinkel: And then you have to go through the process. And so the candidate (inaudible) whether you want to stay on, yes or no.

Cristian Hesselman: That's right.

Luis Diego Espinosa: Okay, the order, following off the agenda means okay, we have from Cristian a few questions and a question from Antoinette. And a replay from (inaudible). Then we'll review the questions maybe.

Okay. I have a question here from Cristian. The first question is why did the Working Group opt for the centralized repository? I want to talk a little bit what I'm thinking here. Maybe Isaac can have an opinion. But the thing is it's not centralized. Maybe it's a convenient type of contact beside within this community particular because the contact repository is (inaudible) for CC managers for TLD manages maybe. No other infrastructure, operator.

Then in the case of contract repository incident response team like CERT or (inaudible) when incident occurs, they need to keep in touch not only with the TLD manager, maybe with some ISP, maybe with some operating system something like that. Then there need to provide some official access to an official database of contacts for emergency. Then I think it's not centralized. I think it's part of the broader contacts database. Then there (inaudible) we are not thinking-- we are not (inaudible) where physically it would (inaudible) the database but, with this methodology, I have some clout, some kind of clout like we do in DNS.

Cristian Hesselman: It's like a, how do you say that, a large (inaudible) repository which the actual implementation may be distributed across several sites.

Luis Diego Espinosa: Yes, we're getting details of what form, what operating system because we want to have some proposals from potential bidders and with that information we think what is possible, what could we have to adjust the specifications for a form of (inaudible).

Unidentified Participant: And maybe if you want to—this is like a tendering process where if you want to also kind of specify what kind of system you want, maybe there's already a requirement that says, okay, this assistance should be fully distributed, for example, or something like that.

Bart Boswinkel: To my knowledge, if you go through the requirements, at least it has to be redundant and one of the things is it needs to be available and updated 24/7. So you need to have an overhead structure which is probably more determining than the platform and the technical solution itself. And so one of the reasons why this is included is one of the core questions at the time when this working was formed was whether to build it ourselves or to buy it in, say, or hire it, tender it, in the sense of you go to Trusted Intruder of these type of organizations and so it's taken quite some time to get the momentum going. And if you go back another requirement is what type of overhead structure do you want because there are only a limited number of cases where it can be used that was pre-defined as a starting point. So you need also, in order to really make it work, you need two kind of structures. You need to have, say, the tendering organization— well most (inaudible) ccNSO or it could be also a group of ccTLDs. You need your overhead structure in order to manage the policy itself. So when do you need it, so the cases. And so that's the level we're at and we're not into the technical solution itself. There is Antoinette. Hi Antoinette.

Luis Diego Espinosa: There are—we already have some specifications of the system but more concept specifications, more done (inaudible).

Cristian Hesselman: I only ask because I didn't read anywhere that the system could be potentially a peer-to-peer system or distributed across several sites or something like that and that's something I would have expected in the documentation somewhere.

Luis Diego Espinosa: Okay. We are with that question or Isak, do you want to say something about that? Antionette, welcome. We are reviewing the questions from Cristian. We already reviewed the first question about the location of the repository.

The next question is what system repositories the working group is considering that might form a basis for implementing the contact repository. One example (inaudible) also is the DNS or (inaudible).

I think, my opinion, this type of contact is very particular because it's for emergencies. I think it's not the same contact—the contacts maybe don't change in years and maybe the person who appears to (inaudible) is no longer there and never have been updated or maybe, yes, but I think the contact for emergency, very specifically, needs very specific treatment because, in my opinion it could be confidential because, when you are asking, for example, some company or where you work, when some people ask for the technical contact, maybe you use some generic contacts like NOC or some call center form. But for emergency maybe you provide your private cellphone but only if you are aware that information will not be freely available for everybody. Then I think the (inaudible) of this information or the collector of this information will have a particular task and it should be clear what will be the purpose of the information and the information to be very well validate. Then I think we need to create a new contact.

Of course, if it's possible by example if the DNS org they have already emergency contacts could be (inaudible) or by example be the regional organizations. May they already have some information that can help a little bit. But at the end I think this repository to go contact-by-contact to search that information and specify what will be the use of that information.

Cristian Hesselman: So it's basically our task to set up the requirements for, say, what kind of data has to be in the system and how it should be accessed and then it's up to the implementer to actually decide which database to use for that purpose. I was just trying to conclude what you were saying. So if I understand you correctly, it's about we put in the requirements so we write down the requirements and they say, okay, these people that are the security contacts, they may need to provide personal information into the database and, as a result, it needs to be shared or secure or whatever and then, based on these requirements, we need to—we or let's say the tendering party needs to select an actual database that will realize these requirements and this actual database might be the DNS.org database if it fulfills the requirements that we have.

Luis Diego Espinosa: But I'm not so sure about that because I don't know if the DNS.org will be viable for this work.

Cristian Hesselman: I don't know either but suppose it is and it meets the requirements of the—

Luis Diego Espinosa: I don't know too much about this DNS.org database.

Cristian Hesselman: Again, it's just an example.

Luis Diego Espinosa: But the other example it could be the Trusted Intruder. Probably they would not provide because maybe they have some kind of arrangement of disclosure agreement about information.

Cristian Hesselman: All I was trying to say with this question is that if we do the requirements that we should be careful not to roll with a completely new system if there's always something around that meets these requirements.

Bart Boswinkel: That's the whole purpose and that's why—

Cristian Hesselman: I re-read the slides of the Emergency Response Working Group this morning and it also said that this was something that needs to be looked at. So which are the available systems and—

Bart Boswinkel: That's why we go—

Cristian Hesselman: Might meet the requirements of the contract repository.

Bart Boswinkel: Without—and that's the whole build—and that goes back to whatever external party builds that new platform but what you want is in fact go for a cheap, specific solution because that will handle and manage the whole database itself. And how they do it, it doesn't really matter as long as you've got a reasonable arrangement with them to work on it.

Cristian Hesselman: And must comply with the requirements.

Luis Diego Espinosa: We mentioned something—we definitely mentioned something about the security management or information security and we mentioned examples of possible platforms, (inaudible). I used an example of LDAD because it's native contact management. Is the management secure and it can be (inaudible) and have many, many—can be usable in this kind of database but. But if somebody wanted to put it in Oracle (inaudible), it's okay. Okay, then the idea of the, to continue with the question, the information of the contract repository maybe it needs to be collected from scratch but, if not so difficult I think because we are thinking about 15 or so, for example or 16—we are thinking about less than 200 (inaudible) if you think about contact by each (inaudible). We're thinking about 400 contacts. It's a free formation. Really the amount of information with the (inaudible).information. And the characteristics of the information require that you (inaudible) about the voracity of the (inaudible) information.

Cristian Hesselman: My first guess would be that it's not only going to be a technical problem, what you're saying is that it's essentially kind of a simple system. It's not that difficult. So we could build it ourselves. But there might also be some sort of political angles so to speak in that people will not see the relevance if it can also be done through some other system that already exists. So it's not purely a technical—

Bart Boswinkel: No and it's also a managerial problem. If you think about it and this goes back to, say, what you just discussed, so in order to make it really functional, you need to ensure in a way the contact details are refreshed regularly and this goes back to said discussion you had about the type of contacts. And one of the issues we find, say, for example for the ccNSO secretariat is that our contacts with, say, our own community are not updated. So you need somebody who chases—you need an organization that chases everybody and that is—that's again a management task and that's probably far more important than the other thing, than a technical solution.

Cristian Hesselman: I understand.

Bart Boswinkel: And again, this same management organization needs to be available to 24/7. That means also by definition that you go to a larger organization that is set up for this and that makes it expensive. And that's why you can't trust to go to, say, one of the ccTLDs although some of them do have 24/7 security and emergency teams of their own, they're not 24/7 productive. For that reason some cc's or most ccTLDs, even the larger ccTLDs themselves are too small for really having 24/7 productive teams available.

Cristian Hesselman: I'm also thinking that maybe that it's possible to do some automation there instead of, like, it's like having a central organization that you need to call in order to update your contact details. You can also do it yourself, for example.

Bart Boswinkel: Yes, you could do it yourself but, then again, it is unique to ensure that it's done properly and according to the rules so that people don't enter their own details et cetera. It's a balancing act. If you want to make it sure because what you don't want to do, and this goes probably to your third question , if you start doing this you want to ensure that it's only used in specific cases and people can trust that it is used in specific cases and that the alarm is coming from a trusted party. And again, therefore, you need a very solid organization that is not—because this goes back to one of, say, the third question you have about use cases, say, this is all the result from the Conficker situation—is when ICANN started sending out emails, just simple emails, and they could have been (inaudible) whatsoever and people were requested to delete some domain names. Now that's not easily done. And that's why you need to create such a structure.

Luis Diego Espinosa: Some of these ideas to keep up to date information in a manner in some way to say—there's some ccs that have managed their contacts, their customers in a very personal specific form. They have some group of persons keep calling, keep sending out letter mail. Not on email—letter mail. If you see the table we use in the presentation, there are five different ways of contact and electronic is only one. The email, the other one is fax, the third one is the letter, the other one is (inaudible) or telegram. The other one is, I don't know, it's (inaudible) there's five different types of contact and the need is to check every (inaudible) of those contacts. In some cases the emergency took down the Internet too. Some kind of emergency. I know.

Bart Boswinkel: I'm jumping out of bounds—

Luis Diego Espinosa: Yes, that kind of thing you cannot estimate it completely. The third question, can you say maybe the question please? Not just read it. I want to hear what is the question.

Cristian Hesselman: Actually, this question came after I talked to a colleague of mine who is evolving DNS.org and, like I told you, they also have a database like that. But he said it's never been used and usually people—so you suggested that people need to trust each other first before they contact each other and, of course, this is something you facilitate with a repository but you also need to facilitate that they can actually trust each other. So maybe what you just said, the contact information is always up to date and you know that, when somebody calls you, then something serious is going on. I mean, this is something that you somehow need to manage, in short. I don't have the answer but, I mean, you need to somehow facilitate that people actually use the system when it's necessary.

Kristina Nordstrom: Sorry, this is Kristina. Can I just remind you to share your names before speaking so there will be a transcript.

Cristian Hesselman: Okay.

Luis Diego Espinosa: This is Diego. I think the user of this contact database, maybe we need to find out in some of the report documents by—the user is not global, it's not a universe, it's not an internet user. I think the user of this contact database will be the instant response teams, basically. CERT, many of them. And the way that they can access the database will be treated like a service or a kind of agreement between this repository and these entities. And one of the proposals for (inaudible) is create a standing committee that can handle that population of factors of the database.

Bart Boswinkel: At least oversee it. You don't want them to handle it. Because, at the end of the day, if you really look, drill down, you need to act quickly. So if you look at the use cases from the previous working group, you need to act quickly. Again, this goes back to the trust what you're talking about, you need to trust this management team of the database itself or the repository that they will use their contacts and start signaling based on the agreed use cases. So they need to check and this is going back to the slide and that makes it complex. You need some structures and some feedback mechanisms that can act quickly but enough checking and balances that it's only used in specific cases and that it would be done quickly. So therefore, again, you need almost a central contact group that initiates how—where the platform itself and how it's done doesn't really matter. But that makes it, again, an additional cost factor unfortunately. And this entity itself, if you go for it, that one needs to be trusted as well so that's building up the chain of trust from that angle.

Luis Diego Espinosa: Yes, Diego. I think the trust on the repository would rely on how great and how precise the information in there and that trust to be built by the repository itself. And this needs a lot of work and (inaudible) but once the repository is trusted enough, it will create its own reputation in some way. Then in this way the ccs that should provide from (inaudible) repository, they must feel confident about who—which entity is providing the information. And the idea that can be handled by an organization like ccNSO within ICANN. I hope that provides some (inaudible) for us.

Cristian Hesselman: This is Cristian again. My point was just to also, if we're talking about requirements for the system, then we should keep this in the back of our heads because I think this is a crucial requirement that we build the system and the organizational structure around it such that it facilitates or enables that trust. To me that would be a key requirement for the whole working group.

Antoinette Johnson: This is Antoinette. You're speaking about trust. Could you elaborate more on it? I'm trying to connect that dot.

Cristian Hesselman: Well because it's somewhat of a vague concept. I just—it's like what we just talked about. I mean, when you're part of a CERT team and there's something going on, you need to be able to trust the system that the information that's in there is correct. And so that's basically what I'm talking about. And then you will also know that you end up talking to the right person that can maybe do something for you or that you can do something for that person. So you need to somehow build up a trust relationship with the system. So all the CERTs that are affiliated with this system, you could trust it. That's what I'm saying.

Antoinette Johnson: Okay, thank you.

Cristian Hesselman: So maybe another suggestion but I'm not sure if this is relevant is to maybe there are similar systems in other industries, for example, that we can maybe look at and see how they did it.

Bart Boswinkel: What do you mean, say, in other industries?

Cristian Hesselman: Well, for instance, I don't know, maybe when it comes to the airline industry or something. So industries that also operate on a global level where certain incidents happen and then they need to get in touch with each other. I'm not sure that exists.

Luis Diego Espinosa: Yes, but what I found is that the same response team, incident response team has its own contact base. Then this model of share of only contact information is not very common in the industry. The only example we have is Trusted Intruders in Europe.

Bart Boswinkel: There is another one I think, say, from Bill Woodcock the Beckett House Clearinghouse—Beckett Clearinghouse, for instance, in the ARENA. They do a lot but that's smaller again. And so you have some over-rising CERTS that work together, say, at least—but most of them end up with Trusted Intruder because that's ARENA so that's in the network industry.

Luis Diego Espinosa: So the other example is from Canada. Jacques Lacroix. He has been working to create some kind of further (inaudible) company from—for emergencies. And he was talking about organizations and ISPs and government. I cannot think but it's something that they are thinking about. It's not exactly something we can follow because it's not something in production. But yes, I think it's a good idea to maybe at some point check what the DNS.org are doing and some of their experience in this would be helpful to (inaudible). I think the document is very simple. That way we are defining some concept or way of running this and that is to find some possible leaders or providers and see what they can offer and try to fit a little bit or adjust a little bit what could be—

Bart Boswinkel: I didn't understand which type of structures you need to manage it because that's another thing. It's only worth, say, even starting the process, initially you'd need to be—how should I phrase it? So if only, at the end of the day, 50% of the ccTLD community uses it then, I think the cc community or the ccNSO or we, it doesn't matter, have failed. Not all of them will use it for whatever reason but I think, in order to really make a difference, you have to go to 80% to 90% of the cc community to make that difference, what you talked about. And that's going to be hard and that only works if, say, that is related to your third question with outreach whatsoever. And it needs to be affordable and they need to trust whoever is there. So trust is one element, affordability is the other one. We worked on, yes, send it to the working group—so just based on the fees of Trusted Intruder, the one-off subscription was, I think, 900 euros one-off and then around 60 or 65 on a yearly basis—on a monthly basis. And that has to do with follow-up and maintaining the contact details over time.

Now if you just save the 50 euros a month, that's 600 euros a year and, if you talk about a small ccTLD with just one person because there's some of these ccs out there, then you have already an issue. Or people with just two or three and, hopefully, it is never used so it's just—it is, and in some cases, it's an investment. So that's a bit of the trick as well. And so because we know at the time of the formal working group when they defined the used cases, et cetera, Trusted Intruder came up but it would have been too quick, too fast to get to involve ourselves with Trusted Intruder as a cc community. So these steps needed to be made in order—and this document goes back to the council—the ccNSO council and just afterwards you can go out for tender or as a basis.

Luis Diego Espinosa: Okay, any other point in that question? No, okay. Okay in the email, Antoinette, she has some concern about marketing of the repository and do you want to talk a little about the subject?

Antoinette Johnson: Antoinette. And my thought before I shot that question to you was I think that we probably need to start thinking in the back of our minds how we're going to—I'm going to use the word sell—sell it to the community because, in speaking with people individually, personally, they keep asking me so what is this contact repository? And they keep asking that question and, again, it's kind of piggy-backing off of are we reinventing the wheel for something that already exists? So we probably need to think of—I'm going to think about it and I'll give some more thoughts back to you on how to make it really stand out as to what it is, various directives, very simply stated, and why it's needed. Why we'll be looking at the Who Is information, am I correct with that at some point in time?

Bart Boswinkel: Yes, absolutely.

Antoinette Johnson: Okay and, you know, so that we can at least—everyone keeps asking the same question. What is it and why is it needed?

Bart Boswinkel: This goes back to, say, and because I think the timeline between the previous working group and this work and the conflict of this incident is quite long by now. This goes back to these kinds of incidents, say, with large attacks when you're vulnerable, say, recently there were some at the level of—with smaller ccTLDs, either through registrars or other ways that they are under attack out there so that they can be pre-warned. So when it happens somewhere, that you know that this might hit you so you can take the precautions.

Cristian Hesselman: So this is Cristian again. That's also one of the questions I had. I mean, have there been events in the past where this system would have helped?

Bart Boswinkel: There's only one and that's going back—the Conficker. I don't know how it—otherwise and, in that sense, it would have been useful but maybe it's used for (inaudible) time because, again, this is mostly done on the basis of trusted relations, say, between two parties—is that probably I think ICANN should have some figures around it, say, if there were incidents and if something like this would have existed or something else or if they are involved in some incidents where they have pre-warned because this is all about pre-warning some ccs of an emerging attack, or whatever, that would fit the use cases.

Cristian Hesselman: Are you suggesting we could ask ICANN if they—

Bart Boswinkel: I'm sorry, I'm Bart, the transcript purposes asked. When they hear my deep voice, then they know it's me.

Luis Diego Espinosa: I want to add something to the (inaudible). The security issues or security concerns in the Internet have been increasing constantly. For example, today we have a meeting with the DSSA, the DNS Security and the WBP Advisory Group and we have a meeting with some contractor they make (inaudible)—they make some risk management framework, something like that. But at the end it's more like the same thing. More specifically, in the side of the DSA and more like a framework but, in the end, it's risk management. Then I realized the name of DSSA is not the better name we can have for the working group because, at the end, it's risk management. If you said risk management, everybody will understand. If you say DNS Security (inaudible) what is that? Then, Antoinette, maybe, thinking about your concern about how to sell this way, how to say this, maybe we can think about a fancy name for the country repository because maybe, in this way, that would mean something real important. But if you are hear and you understand what is the purpose of the working group, you start to understand that it is important and would be important and it's a good thing to have this kind of information available to any emergency in the future. Then I think what they think about to create the name and (inaudible) security (inaudible) or—

Bart Boswinkel: Sorry, Cristian, but I think at the time—by the time we've completed the report, it's also time to (inaudible) through and I think that would be a good marketing thing in which case would it have made a difference if you would have a contact repository because then you can show to the broader community, at least the cc community and say, in this case, something happened and at least we've done or and that and that would have been easier and more quicker and you would have been more aware. At the end of the day it doesn't solve or it doesn't avoid

the attack itself, it's just assisting ccTLDs to beware and to take the necessary precautions.

Cristian Hesselman: And this is Cristian. So I think the best way to sell it, if you want, is to actually link the repository to real world events that have occurred in the past and then maybe go through a hypothetical scenario of what might have happened if you would have used the contact repository. So for example, even then once we have, we're seeing these (inaudible) attacks on banks and this is what we're seeing a lot. I'm not sure this system would help there but you could go through a scenario in which you would, you know try to detail how the repository would play a role in, say, fighting off those EEDOX attacks. And that will give you a very strong argument to implement this system.

Now I remember what I wanted to ask you, Bart. Is it possible to ask ICANN if they are aware of any incidents that have happened in the past without naming and shaming that might have—in which case this system might have helped?

Bart Boswinkel: I think they are more than willing because they really say, initially, in the previous working group, ICANN staff was involved and they were a bit pushy about it. It got created very quickly and they wanted to take it over. And that's a bit of the political background if you look at it and that's why the cost aspect is so important. This goes back to ICANN could do it, probably, and they would pay—and they could afford to pay it as well. But then comes in the political question, who determines what? And you know by now, as well as I do, that the ccs are a bit reluctant to let ICANN do it for various reasons and it doesn't build on the trust of, say, the repository itself as well.

Luis Diego Espinosa: Diego. Well, during today's presentation, we have a question from (inaudible) asking who is database for this controversial story, for all these contacts. Like I were touching here in my opinion, this is a different kind of contact. It's not—and (inaudible) comment about that too. He said that the, well, it's true, that the protocol. They have some protocol who is from (inaudible). He's not suitable for these kinds of contacts. Thinking about the (inaudible) I'm thinking about the database itself and the new one proposed by IETF working group is just, work on progress. We cannot wait to (inaudible) that protocol finish. That is because I was suggesting to use something like LDAP that has been there for many years and is very well proven. But the point is we have not established our fixed technology to do this. The question about Who Is, well, I don't know if somebody has comment about the Who Is by itself. Not the protocol. More thinking about what they want to create. Let me rephrase this. If some of you think in some point maybe this contact—emergency contact information could be merged with other information to create an extended Who Is or something like that. Thinking about in this ICANN meeting having, I think, at least three sessions about Who Is. And there's some people from ALAC I think is talking about the pertinence of the information within the Who is database. But I think we should keep it simple and go further with this stand-alone, independent database of contacts but if somebody has a different opinion, then I'd like to hear it.

Bart Boswinkel: This is Bart. Why did they ask about Who Is? What is—why did they link it to Who is? Just because, in my view, Who Is is a bit—it's sending out a query to a database and then you get some data back. So you need the database anyway and so that's more information than they—or all the information that's contained in the database but public for whom? Is it between the ccTLDs that they can query it? So that's one. But then you have the issue what do you do if you need to contact somebody out of bounds? Because then it's the requestor. You want to have my information but why do you want my information? Then everybody should have, maybe in the case of every cc should have and this goes back to Cristian's thing, I guess. If every cc has a trusted Who Is can be only accessed externally by all the other, or 200 or 300 ccTLDs, that becomes also very

unmanageable. Because who do you allow? Who do you allow in to see your information?

Cristian Hesselman: This is Cristian. You mean who do you allow in in terms of who can access the—

Bart Boswinkel: Yes, who will query you with the Who Is?

Cristian Hesselman: Well I think, without going into the technology details, I think that where it's potentially—the potential follow up of Who Is that allows you to specify rules like that. At the same time, you can also argue that if you want to be able to reach other CERTs out of bounds, so to speak, or out of band, so without having Internet access, then this doesn't work. So then you would, maybe you would even have to revert to an app on your phone, for example, that would have everything in there so you would either be able to go through the Internet or through the DSN network or maybe through the (inaudible) system. I don't know.

Bart Boswinkel: So it may be, the question relating to Who Is, and it's also somebody who queries the information, that this is more of a push thing than anything else. Information is pushed out. If there is an incident, I need to contact you and I need to know how to contact you. But with the Who Is, I need to contact you first so I get the contact details so I can send you information. And then you need to allow me to look at your information and, if you try to do it by, say, creating a web of trust, then you need to do it for all those who you trust.

Cristian Hesselman: Cristian, I'm not really sure that I completely understand but I do see that the—so the question about Who Is was triggered by someone by (inaudible) who was on the Board of DNS.org and he claimed that, okay, this (inaudible) around but, of course, there was no consideration of, let's say, the out of band thing so to speak. I'm pretty sure that's not supported. So it's probably an additional requirement that we put on the repository that makes certain, let's say, technical solutions possible or not possible—excludes certain technical solutions. So it needs to be very clear on the requirements.

Luis Diego Espinosa: In addition to that, I think the access to the information is not the same like Who Is. Who Is is open to anybody to anonymous question but could be restricted with the new protocol but is more like general information which you can query or anybody can query. In this case, like I said before, the current information in the (inaudible) repository will be accessed only if we follow some kind of emergency protocol. It's true some of the emergency response teams so, basically, it's different kind of provider service I think which will keep and separate service.

Cristian Hesselman: And I think I suddenly realized what you said by push because, basically, what you want, if you want to integrate this into an incident response process, you want to be as independent of any network connectivity as possible. So you would basically have something on your phone, for example, as a member of the CERT team, that would have the contact information of your peers in it. And it would be the, let's say, updates of that information would be pushed through your phone so that you would always have the latest copy on it. Perhaps that is what you mean, Bart.

Bart Boswinkel: Or the incident itself, say, the warning of the incident. That's pushed out. Say, that's the basic information that is pushed out. That's why you need the contact details. So if I want to warn you, because I'm aware or I want to pre-warn you of an imminent attack, then I need to send it out to you. And therefore I need your contact details inbound and out-of-bound.

Cristian Hesselman: It's Cristian again. I understand that but this is also—it also has a little bit to do in my opinion with the scope of the system. Are we talking about incidents that are about to occur so I am warning you, for instance, that I have, let's say, my

servers are going down because of the EEDOX attack? Or am I contacting you after I'm being EEDOXed saying that, okay, Bart, I need your help because my servers are going down. I need you to run secondary for me. Something like that.

Bart Boswinkel: And this goes back to the use cases. The use cases as they are defined right now is, say the way I understand it, but then I'm just an entomologist, is these are large scale incidents that are imminent to occur. Going back to Conficker. It's not because I've been attacked and I warned you, that's another—that goes first that I say I've been attacked and I need your help. Is another system (inaudible) and as far as I am aware from the use cases, this is if it's not querying out, can you help me?

Cristian Hesselman: This is Cristian. The problem is, I didn't see the use cases on the website so maybe—

Bart Boswinkel: It should be. There is a presentation and they are defined in the presentation from (inaudible) and they are—

Cristian Hesselman: I wonder if they're not in there as far as I can tell. Anyway it doesn't matter. So the scope is basically incident warnings. That's what this is about.

Bart Boswinkel: Yes.

Cristian Hesselman: And I think that's important to know.

Bart Boswinkel: It's not to assist each other. And this goes back—that's why you need a Policy Board. If you have a Policy Board because that Policy Board determines the use of the emergency and, based on that, if they change the rules, then you can use it for other incidents and queries to assist as well.

Luis Diego Espinosa: Well, we're more (inaudible). Maybe we can go to the next point. Yes, talking about the next conference call. Before this meeting we worked on the frequency of every two weeks. I think we can keep on that frequency and try to have some kind of report finished for Durbin, I think. It's a short time but we can think. Do you agree with having a conference call every two weeks?

Antoinette Johnson: I have no problem with that. Antoinette.

Isak Jacobsen: Isak. I have no problem with that.

Luis Diego Espinosa: Okay.

Bart Boswinkel: We have rescheduled that say for every two weeks or so. See if we can conclude it Durbin. That will be nice.

Luis Diego Espinosa: That will be nice for me too. Any other business? I think we need to close. No, it's okay? We're done. Thank you.

Antoinette Johnson: You're welcome.