KOBE – ccNSO: TLD Ops Drafting Team
Sunday, March 10, 2019 – 17:00 to 18:30 JST
ICANN64 | Kobe, Japan

JACQUES LATOUR: Okay, we'll start. It's 5:00. We're good to go? Recording? Hey, Erwin! Good morning! Hey, Jim. How are you? Alright.

So, this is our TLD Ops ICANN 64 Disaster Recovery Business Continuity Planning Drafting Team Meeting. We had a workshop two ICANN meetings ago and we started to write a document, and this is the drafting team meeting, so it's not going to be super exciting. We're going to review the document that we have. It is going to be exciting, right?

So, welcome. This is our project plan. This is not the same slide we had in the previous presentation because we moved this arrow here by about three pixels to the right, so it moved. So, if you compare this slide and the other slide deck, they actually move. It's real-time project management. Pretty good, eh? So, we're exactly there.

The goal is to have a draft document by ICANN 65 in Marrakech, and I think we're a long way still to get there, but hopefully we'll make it.

So, we have volunteers for this project, and we have Alejandro who is a volunteer. Dirk is actually on the chat connected, and later on, he'll share some information. And on the chat, we have Svetlana is connected. From our Standing Committee, we have Brett on the line, and Standing Committee there is Erwin, Regis, and I here.

So, we have volunteers. We have a document that actually made some progress, so we'll review that.

So, I think in our last meeting, TLD Ops Drafting Team meeting, we agreed that we would try to distill or bring the disaster recovery business, continuity business, impact assessment discipline usable for a small ccTLD. So, that's the main challenge that we're addressing. And we need to focus on ccTLD relevant activities which are the registry, the DNS, the WHOIS, and we may add the financial activities, getting the money in the registry. So, for the small ccTLD.

And it has to be usable. That's a challenge. It's got to be something practical that you fill in the blanks and the document is useful. So, that's what we need to do.

We need a leader. So, Regis and I are chair and co-chair and we're running the group and setting up all the stuff to run this. But for this initiative, we're looking for a leader to run this initiative,

either a Standing Committee member or a volunteer from our list of volunteers to this project.

So, right now, the last call was January 15, so we did a little bit of activity then. But between the last call and today there was no activity whatsoever on the document. There were about 40 changes done just after our last call and nothing after that.

So, when you're the leader, I don't know if we're going to elect one, appoint one, but it needs to be somebody that understands what we need, what the outcome is, and get the team working together and to make it happen.

So, I fear that if we don't have a leader, then this project might not go anywhere, at which point we need to determine if we stop this initiative, or find a way to get some money from the OCTO and ICANN security department, to get us a consultant to actually do the type of work that we need to do, and not rely on us to do all the work.

So, I think that there is value for small ccTLDs, so that could be bigger than just us doing the work. They're might be external parties that could help, and that I have no clue how to get funding to do something like that. We'd have to go back to the ccNSO.

This is the document that we have so far. So, I'm going to share, I'm going to go through the Google doc and then we're going to work on it, and for as long as we can, and that's it.

UNIDENTIFIED MALE: [off mic].

JACQUES LATOUR: I was going to appoint you a volunteer, as a leader.

UNIDENTIFIED MALE: I know, after I leave.

JACQUES LATOUR: Share. Share document. Doesn't share.

UNIDENTIFIED FEMALE: It's asking you to share my screen.

JACQUES LATOUR: Yeah. To use this application, you did to install the Adobe Connect add-in. It's installing the add-in. What's it called, the full screen?

UNIDENTIFIED MALE: [inaudible].

JACQUES LATOUR: [inaudible]. Chrome. Adobe Connect loading, Adobe Connect starting, Adobe Connect, connecting.

UNIDENTIFIED MALE: [inaudible].

JACQUES LATOUR: And, I should have tested this before. Yay! Yay, perfect. Boy, I don't know if we can do it. Can we see this? Alright. So, if we add the leader, the leader would lead, but we're leaderless, so I'll lead. No

UNIDENTIFIED MALE: Yes.

JACQUES LATOUR: So, this is the playbook that we have, so far, and all the comments. So, the goal, like I said, is to make it work for a small ccTLD. I think the key audience for this document is Alejandra. We need to make sure that whatever we build here is something that you can use, and you're the sounding board to say, yes, no, this works, or it doesn't work for me, or it resonates with me, or not. I don't think we should expect you to write this document, but if possible, we'd love for you to say this is too complex. Or, yeah, this actually works for what we need.

So, the framework that we're using is the Plan-Do-Check-Act. That's a lifecycle. So, we've got a table of contents with stuff here. I think we need to find a way to make it more as a template than a document that says you need to do this or you need to define something. We should have a form with stuff you type in, that you input information that you need to do.

So, it's got … This is more of a template or a document that will explain what [the IPC] is. It's not a template. It's not a document. You could use the one and follow, implement or execute. I don't think you could use this. You'd need to be able to use this in case of a disaster. You just look at it and follow the steps, and that's the document you use, instead of having a document that tells you how to build a document that you use, right? That's what I'm trying to say. Does that make sense?

UNIDENTIFIED MALE: Yeah.

JACQUES LATOUR: So, maybe we need to define this document. Maybe we need to define what the other document needs to do. So, this is the [inaudible], and then we need an actual usable plan.

Sure. So, [Derek] is saying, can I share one of my templates? Yeah. So, you're going to make him presenter.

UNIDENTIFIED FEMALE: He already is.

JACQUES LATOUR: Okay, there we go. So, we need templates. Yeah, templates, exactly. So, it's going to load the template.

Okay, so it says this is the one about cyber security. It's a two-page document, and then if we scroll down, well, it's got the procedure number. So, this is what you would execute if you have a cyber security event. Yeah, this is a good template.

So, what do we call this? So, it's a template, it's a plan, it's a BCP plan for a certain scenario, right? The GDPR [tied] to the phone numbers. Yeah, what are business numbers, so that's okay. Okay, so because we need an incident report form.

So, we need templates, simple, I think simpler templates like this that are pre-filled with information, for a couple or a bunch of different scenarios, like the top five scenarios that a ccTLD would see. So, we would have … And so what did I have in the other document?

So, we need to pick the top five risks for the ccTLD, if there's a data center failure, if there's a natural disaster, volcano, power, flooding, execute this plan. If there's a data compromise, hack, that would be the template there, simplified. If you lose all your staff, because of a disease or contagious thing, then you fill in the template with steps, “this is what you need to do”. But we need to pick just a few scenarios and have templates for that. For the DNS, for the registry.

UNIDENTIFIED MALE: [off mic] and human resources, I think. That's the main issue that [inaudible] and if we have two or three examples in each, then I think it can be a real help for [inaudible] ccTLDs.

UNIDENTIFIED MALE: I think, first, you need to have the overall crisis management plan, when is this a crisis, how, what's your crisis team, etc., just for any crisis. Just an overall plan for your disaster recovery, and then underneath that, you can have a few scenarios, specific scenarios, and they can also be very specific to the ccTLD. So, especially to DNS infrastructure would be one of the most important things we run, so that would be one of the scenarios at least.

JACQUES LATOUR: Kim, are you dialing into the bridge or no? Okay, I'll just share something.

BRETT CARR: Hello? Hello? Hi, it's Brett here.

JACQUES LATOUR: Hi, Brett.

BRETT CARR: Hi.

JACQUES LATOUR: So, that's it. I don't know if you can see that properly. So, that's what we're talking about. So, I have to zoom in more. The initial decision-making, if we have a bunch of diagrams, and then you've got staff, somebody detects an event, and then you assess. There's a process to assess the event, determining the critical nature of the event, and if it's obvious that it's a disaster, then you'll run the appropriate plan, and then if you're not sure it's an actual disaster or whatever, then you need to bring it to senior management or execute a team to determine is this a critical event and do I need to execute a plan?

So, that's kind of our initial decision-making to start the whole thing to figure out what happens from there. So, otherwise, stop screen sharing.

DIRK KRISCHENOWSKI: Hi there, I think I'm connected now.

JACQUES LATOUR: Okay, I'll just, I don't know how to stop the screen sharing. I would—

DIRK KRISCHENOWSKI: Maybe I can get you from back—

JACQUES LATOUR: Yeah, share your document again, Dirk.

DIRK KRISCHENOWSKI: Okay.

JACQUES LATOUR: And that is going to make it, yay!

DIRK KRISCHENOWSKI: Great, right. So, this is one of the examples of [inaudible] important business continuity plans that we use. It's basically the result of all the exercises that we do for the risk assessment. So, in the end, we ended up with a number of business continuity plans.

Now, this is basically giving an overview of all of the actions that need to be done, if a specific scenario would occur and things need to be fixed or things need to be done.

So, this one is specifically about a cyber threat, and we detect a hack, for instance, that we describe some scenario, and then it says when it has to be activated, if there is a recovery time objective, recovery time point, who the crisis team is, what the

priorities are, how the assessment should be done, how the incident has to be contained, what are the different recovery steps, how the instance can be stepped down, something about communication, who needs to be informed about the incident, and what needs to be said about the incident.

Vital materials are kind of quite important because that one describes what you need to be able to fix the incident, and last but not least, the reports that are required to be kept, especially with cyber incidents because afterwards you might have police and law enforcement involved in this kind of incident.

So, basically, this is a document that gives an overview for all the different departments so they can build their own procedures, directions and procedures on top of that. But, basically, I wanted to share this because it's giving you an overview of the end result and what might be useful for a small TLD is in the set of these documents. Of course, they are the result of an initial risk assessment, defining what the risk appetite is of the organization, etc., and based on, of course, and inventory of threats and specific dangers that exist.

By the way, I also have that to share. This, see, I'm going to upload this. We have an internal thing called the BCMS manual, and that contains the entire methodology on how we get to this thing. Also, for instance, it contains a list of threats. So, this also

describes what threats that we are taking into account for business continuity and what the occurrences are of these specific threats.

For instance, you have your natural disasters like earthquakes. In our case, obviously, these are rare, but it's clear that for other people that might be very likely or even very highly likely. Flooding, on the contrary, is more likely for us. Then there are also some HR and medical risks that have been taken into account – or threats, rather, taken into account. Supply chains risks, like service delivery failures.

Acquisitions and mergers can happen so that one of the partners that you're working with suddenly becomes no longer available. Things can happen like that. Cyber threats are also very important these days, that we look at three specific cyber threats, DDoS attacks, Ransomware, and data breaches and hacks [inaudible].

Technology and infrastructure. Now, that might be interesting because anything related to technology and infrastructure, we decided to put it in the ISMS (the information security management system,)like hardware problems, network operators that break down. That kind of stuff is not considered as being business continuity-related stuff, unless it goes way

beyond their service levels. So, then you end up in a service level failure.

Other things like aviation incidents, [real] incidents, etc. External threats, this might be actually kind of weird that you see highly-likely that terrorism is highly likely. Now, in Europe, we have had our share of terrorist attacks over the last couple of years. Happily, this has been reduced over the last year. So, that's another thing that is quite important.

Strikes can be also quite an interesting activity to deal with. Not necessarily a strike into your own company, but a strike that hits the entire country. The French know that about their Sunday events that happened in the capital, over the last couple of months. Burglars can also be problematic.

So, that's basically the entire scope of all the threats that we've looked at. And out of that we did a risk assessment, and the ones that were truly important to us, very highly to happen with a major impact, resulted in the business continuity plans that you see. So, that's basically how we approach it, and I think it might be useful for a smaller TLD to have a shortcut in that way, to figure out how to create a business continuity plan.

JACQUES LATOUR: So, that's good. So, we need to … This is a long list. So, we don't want to build plans for all of this, but we could pick the top five in there and have a template plan for each one of those, and then if the small ccTLDs want to have more, then they have a template they can go from, but if you build five or six, we don't need to. Maybe five or six, and then go from there, and then we—

UNIDENTIFIED FEMALE: Hi. Or maybe do have the long list and only develop five or six in detail. So, maybe other ccTLDs can have an idea what else to think about, just to have the list, but not develop them all, just like this is a suggestion and then develop the most likely to happen.

JACQUES LATOUR: And then the actual plan would be something like this, but for the five or six that we pick, then we have the step-by-step. What did you do?

UNIDENTIFIED MALE: [inaudible].

JACQUES LATOUR: Then we do that step, that five or six, all the different steps, and the action item, and maybe this is a lot of information there, but I

think we can summarize it down to a smaller plan that is practical to use.

So, Dirk, on the backend, you have actual plans, right, for each one of these?

DIRK KRISCHENOWSKI: Yeah. Well, the idea is that we tell people. First, we tell the operations department to build their own procedures that are applicable to the specific plan. So, this is the overall plan that gives guidance to what needs to be done. So, let's take, for instance, the item about communication. So, here you have your communication. It is obvious that the communication should be done by the communications manager.

Now, in a smaller TLD, this can be already the same people that are dealing with stuff, but the important thing here is that the templates are ready, the templates for the communication are ready, so that you don't have to think about figuring out how to do that.

The other thing that is also important is that the communications manager might have to think about that he needs to be able to communicate without access to his communications means. Like, for instance, if this is a Ransomware attack, you might have

the issue that your mail system is down because it's completely encrypted, if you have your own mail system.

So, there is a lot of preparation, of course, to these kinds of things, where people need to think about, "Okay, this is actually feasible if I cannot access my infrastructure," but that's not all in these plans. These are just high-level overviews that give guidance, not exactly that tell you step-by-step what to do.

To be honest, in my experience, doing that from a business continuity management perspective doesn't always work very well. So, if you try to do that, and you try to write it down a step-by-step plan, then it's quite difficult. And the barking in the background was my dog!

JACQUES LATOUR: Yes, so let me, so I'll share. I'll go back to the Google document, if I can share. So, here we have planned your DR, your BCP, and then we have do and act. Is that useful, or not? Do we need to be? Because if you have the template, and you fill the template with what you want, you are kind of doing it. The planning is already done, if you have a template, and that's all you use.

Maybe the next phase in maturity, if you start with something super simple, and then you go the next step in maturity, then you start adding planning, and then if you do one more layer, then you

do a cycle, a lifecycle. But for a long time, all you could have is just the little guidebook that you have. That could be good for years until you reach a point where you want to do more.

UNIDENTIFIED FEMALE: Yes, I think it will be more useful to have something to put into practice soon than to have to think, and overthink, and write and elaborate. Because, to be honest, it will be difficult to even start to do that. It would be like, okay, that sounds like very time consuming, I'll do it later, and later might not come. So, I think it is best as you said, Jacques, to have something more practical, maybe fill the templates and, yes, when that's done, that's step number one. Then, well, if it's possible, then we evolve and then we add some more, and hopefully in the end, we'll have a decent, complete disaster plan.

UNIDENTIFIED MALE: Yes, I think the templates must be very easy to fill because every ccTLD will have a special constraint, a special, new service-level agreement and things like that. So, I think if we can fill the templates easily with all the new information, the plan phase is done with that, and then after that, if there is a crash or an issue, you can take this information and use them to make the other phases.

JACQUES LATOUR: Dirk, does that resonate with you, or?

DIRK KRISCHENOWSKI: Yeah, I think so, because that's maybe also a way forward is going the reverse way, going and looking at the result, agreeing upon the result, and then build from the result up to how you get to that result.

So, if we agree like, okay, this is a template that we can use, and then it's just a matter of defining how you fill in the template and you already have something, and then you can make an annex with all the potential threats. Likewise, as I said before, it can be a list where people pick out the things that are applicable to them.

So, if they believe like, okay, we have to also take into account financial resilience, then you can put financial threats also into your account. Maybe in some countries they need also to take governance and the government into consideration. Then, that becomes also a threat that can be taken into account. And then, if we explain how you fill in the templates, or what should be in the template—not how you fill in the template, but what should be in the template—then I think people can quite quickly have a basis of something that they already can prepare themselves for.

Then, if they use terminology like vital materials, which is basically thinking from what you need, let's say, in a suitcase to be able to deal with the incident, then that can be a very, very practical way of dealing with things. I do agree that traditional business continuity management or information security management always works with risk assessments and event risks, but I think for most smaller entities it is extremely difficult to do and becomes very academic as an exercise.

So, going bottom-up, instead of top-down, might for a lot of organizations actually work.

JACQUES LATOUR: You said that the word result, working from the result, this is it exactly. I didn't know what that terminology was because it's not in my terminology, I guess. Well, we start with the outcome, with the end, and then because we know what the major risks are for ccTLDs, and the DNS and the registry. We know the result.

UNIDENTIFIED MALE: [Inaudible] result.

JACQUES LATOUR: So, if we start there, and then you enhance, then yeah. So, Dirk, would you be interested in leading this?

DIRK KRISCHENOWSKI: I knew you were going to ask that. [Inaudible] volunteering. I knew I should have stayed in bed [inaudible]. No, of course, no problem.

JACQUES LATOUR: Okay. So, the Standing Committee is here to help also.

DIRK KRISCHENOWSKI: Thank you.

JACQUES LATOUR: Yes, okay. Now, I think, I don't think we need to go further in the document. I think focusing on building a document that has the results of the outcome of what the BCCP plan and disaster recovery activities, I think this is going to be a good first draft of this and see how we go from there, and then if we do that, then it makes the ccTLD relevant, and it makes it simple to use. If we have these two things, then I think that's the objective of this project. So, I don't think that it's a lot of work, we just need to think the end result instead of the process of getting there, which I think is what we started to do.

UNIDENTIFIED MALE: Yeah.

JACQUES LATOUR: We started to document how do we get to the end result instead of just going there. Brett, does that work with you?

BRETT CARR: Yeah. Yeah, sounds good to me.

JACQUES LATOUR: Erwin? Regis? Agree?

UNIDENTIFIED MALE: Agree.

JACQUES LATOUR: Alejandro? I don't know?

ALEJANDRA: Yes.

JACQUES LATOUR: I don't know who else is on, etc., and is Svetlana, no?

UNIDENTIFIED MALE: [inaudible].

JACQUES LATOUR: Not there?

UNIDENTIFIED MALE: She was there, she was there.

UNIDENTIFIED MALE: I think she's gone. She's gone, right?

UNIDENTIFIED MALE: She was there at the previous meeting but I don't know if she still is there.

UNIDENTIFIED MALE: I can't see from here. She's not there.

JACQUES LATOUR: Okay, alright, so what we'll do is, in maybe a month, three weeks from now, we'll set up a new drafting team meeting. We'll send a Doodle out, and then meanwhile we can keep contributing to the document. I think I'll put some stuff in the document and add more, but we'll do a Doodle for the drafting team in a couple of weeks, and then I'd really love to have the first draft by Marrakesh, something we can share. Do we want a physical

meeting in Marrakech, an in-person meeting in Marrakesh? Do we want one?

UNIDENTIFIED MALE: All four of us?

JACQUES LATOUR: Yeah, well, I think the week before we could have a conference call.

UNIDENTIFIED MALE: Yeah.

JACQUES LATOUR: And then the Standing Committee will report on the result.

UNIDENTIFIED MALE: [Inaudible] to book the room.

JACQUES LATOUR: Yeah, and I don't think we need to book a room for this. That was an experiment, so that's good to know.

UNIDENTIFIED MALE: A small room.

JACQUES LATOUR: Yeah, you have the dial-ins, but if you can get that, yeah. Alright. So, I think we're good. This was a good meeting. I think we know where to go. Then, thanks, Dirk, for volunteering.

DIRK KRISCHENOWSKI: You're welcome.

UNIDENTIFIED MALE: Thank you, also, Dirk.

JACQUES LATOUR: Thank you. Talk to you soon.

UNIDENTIFIED MALE: Alright, talk to you soon.

UNIDENTIFIED MALE: Go back to bed now!

JACQUES LATOUR: Alright.

UNIDENTIFIED MALE: Bye.

UNIDENTIFIED MALE: Bye.

[END OF TRANSCRIPTION]