MARRAKECH – ccNSO: TLD Ops Standing Committee
Thursday, June 27, 2019 – 09:00 to 10:15 WET
ICANN65 | Marrakech, Morocco

JACQUES LATOUR: Good morning, Brad.

BRAD VERD: Morning.

JACQUES LATOUR: We have Erwin. Who's ... Joy Chang? Nobody?

JOY CHANG: Yes, I'm here. Good morning.

JACQUES LATOUR: So, what's your CC affiliation?

JOY CHANG: I'm with TW.NIC.

JACQUES LATOUR: Okay, thank you.

JOY CHANG: Thank you.

JACQUES LATOUR: So, [Svitlana]. Perfect. Okay. It's kind of noisy. A noisy room in here with the air conditioning running full blast, the coffee machine. So, we'll do our best. Okay, so I guess we start? So, today is a quick TLD-OPS Standing Committee meeting, and the focus of the meeting today is to review our disaster recovery business continuity documentation that we're working on. So, we have a drafting team meeting along with our standing committee meeting. Next. Yay. What we should do is put the names there, right?

ICANN 60, in Abu Dhabi, we had the disaster recovery workshop. We collected a lot of feedback from the participants on ccTLD-relevant disaster recovery and business continuity issues. And throughout the last three ICANN meetings, I guess, we've been compiling information and trying to figure out how to build the plan.

And today we have a first draft that we're going to review as a team, and hopefully ... The goal of the – instead of just having a deliverable for disaster recovery work plan, the idea now is, in Montreal we're going to do a tabletop simulation using the

documentation to see if it works or not, find the gaps, and document the gaps, and then update the documentation for the next meeting, which would be ... The other one, after Montreal?

UNIDENTIFIED MALE: Cancun.

JACQUES LATOUR: Oh, Cancun. Oh, perfect. And hopefully, by Cancun, we'll have the final document for disaster. Yes, and then we can do the big reveal on the beach.

UNIDENTIFIED MALE: And the workshop on the beach?

JACQUES LATOUR: Workshop on the beach?

UNIDENTIFIED FEMALE: Sand on the computers?

JACQUES LATOUR: No, we bring a paper copy. Yes, it's safer. So, we're making progress, and I will cover that today. So, Dirk was unanimously

approved as the drafting team leader, and he took that role very seriously, and we're making progress on the documentation. We agreed on what the playbook goals would be, is to make the DR BC PB IA. So, disaster recovery, business continuity, planning business. The BIA is business impact assessment.

So, to bring all of those disciplines, the ISO disciplines, also, usable for a small ccTLD. So, take the best out of each one, and just use the things that can actually be useable, and make it simpler. We want to focus on ccTLD-relevant activities, and so the documentation should support two or three, I guess, scenarios, that are well documented, that you can follow step-by-step.

And then, the key thing is the documentation has to be usable as-is. So, you put it in front of you. If you have a disaster, you can actually take it and use it and it should guide you through a disaster. So, Montreal. I think the scenario we're going to do is we're going to simulate a registry compromise.

So, a bad actor got in the registry. They do a bunch of bad stuff. They want to go public. I don't know ... Fred's going to come up with a couple of ideas. Not the absolute worst-case scenario, but just a bad case. And then follow through the documentation to make sure it actually does what it's supposed to do. So, there's going to be a communication aspect.

You need to communicate to the world that you're under duress, and I think that's the main goal. And if throughout the exercise we're going to find gaps, document those. Update the documentation to make it as simple as possible, but effective. And we make it public in Cancun on our website, once we approve the draft. So, we're making good progress. We'll review the document today, I guess page by page, and then we'll try to focus on making sure it's a template for the scenarios.

So, I think if we complete one template today, we can replicate the other ones after, offline, and have as many scenarios as we want, we can do, I guess.

I think I said all this already. At the ccNSO meeting, Régis and I, we did a survey, and the session is going to be closed to TLD-OPS members only. So, after this meeting, we'll send an invite on the mailing list. The reason is, we need to keep it only to the security people, to make sure that it's workable. We don't want to have too many witnesses just to come in and see how it goes.

We need people to participate and contribute to the document, and not necessarily just be there to say they were there, I guess. So, it's going to be a working workshop. I think that's what the workshop is. Work, shop. I guess. So, it is going to be closed to TLD-OPS and no invites. So, to be there you have to be part of the group.

REGIS MASSE: And like the first playbook we produced about DDoS mitigation, once we have the [inaudible], the release of the [inaudible], we will make it public after removing what is confidential for the group. And we have done this for the first playbook, and we will do it the same for this second, after the simulation.

JACQUES LATOUR: So, one thing we're going to need, also, to do the simulation, are going to be some actors. So, we'll need somebody to ... Hopefully Kim, or somebody from IANA to sit in the corner, and wait for people to give them IANA updates. I thinking we should have somebody that Twitter. And then, in the simulation, you go talk to that person, and then that person does tweeting all over the place, to show if the communication is working.

But also, for each of the groups. If part of the plan is to communicate out, and nobody goes to the Twitter person, then there's a gap in this group didn't communicate, and then we should figure out why they didn't communicate. So, I think ... Yes?

UNIDENTIFIED FEMALE: Yeah, Brett says he will be in Montreal, and happy to be an actor.

JACQUES LATOUR: Perfect. So, we need to come up with a scenario that, if the documentation says you need to do a communication update every 10 minutes, or 20 minutes, then if you do go through that Twitter person, or that communication person, every 20 minutes, then there's a gap. That means you focused too much on the technical, not enough on the communication, and that's where typically the disaster recovery breaks. Okay. But we already had all the TLD-OPS members as volunteers, right? So, they don't need to volunteer. They're all in. I should open up the chat window. Okay.

I think most importantly, the workshop has to be fun, so that's another objective. So, we're going to spend the time to make it useful, but I think if we do it well, it's going to be a really good exercise. So, we've got to take this seriously.

So, any comments on that? It's all good? Okay, so Dirk is going to go through the documentation. I think that's the plan. So, we'll go through page by page, doing a review of what we have so far. And we'll capture comments, and maybe update ... Put the comments in the document real-time and see where we're at. Can we make him a presenter? You're good with that, Dirk?

DIRK JUMPERTZ: Yeah, fine. No problem. Just let me quickly find the document again.

JACQUES LATOUR: It's on Google, G-O-O-G-L-E dot …What is it again? Com. C ... How do you spell com? C-A ... No. C-O-M. Oh, yes. C-O-M. Yes, dot-FR. No. Dot ...

DIRK JUMPTERTZ: Just a little second. I'm logging into the thing so that I can actually share it. Alright, let's see. Where is this share? There. Share. Okay, so, you should see now my ... Oddly enough, it's my Edge browser. I don't know why I opened Edge, but it's Edge, apparently.

JACQUES LATOUR: You need to zoom in a little bit. Just make the font ...

DIRK JUMPERTZ: Yes. Is this better?

UNIDENTIFIED MALE: Yes.

DIRK JUMPERTZ: Okay. Just have to close little windows from the video conference, or the web conference thingy. Come on, go away. Thank you. Alright, there we are.

So, what happened is that in front of the document ... And to be honest, I haven't been able to clean up the document in the meantime, because I'm in the midst of an ISO 27001 recertification audit, so I had some other things to do in the meantime. But, this document is based on our internal documentation that we are using. So, I used that as an inspiration.

And then I created a completely new document in front of the other documents. So, it hasn't been cleaned up in the meantime. So, there's an introduction explaining what business continuity is. This gives a little bit of an overview of what business continuity is, how we should look at it, and what it is all about. So, business continuity, more specifically, is about what to do when you have a disruptive event and disruptive incident. This is not about this got broken down in your storage array, or this is not about a power supply that blew up. This is about something that is actually disruptive, that you cannot predict. Like, for instance, a flooding or a virus outbreak, or a cyber-attack. That kind of stuff.

So, we use internally the 22301 standard as a guideline to help us in creating the business continuity plans. There's also a little note

about its relation with the 27001 standard. This is all high level, just to give some context for the document. Do you want me to go into detail or do we allow people to look afterwards into the document more specifically?

JACQUES LATOUR: I don't know. Can you try to speak louder? Also, we have the air conditioning here competing with you.

DIRK JUMPERTZ: Okay. See if it works with a headset on, rather than just a standard mic. Alright, do you hear? Is this better for you?

JACQUES LATOUR: Yes, much better. Thanks.

DIRK JUMPERTZ: Okay, I use the headset. So, that helps. I was saying do you want me to go into detail for every piece of text, or just do we focus on the important parts?

JACQUES LATOUR: Do a high-level overview or an overview, and then for each other scenario we need to go in more details.

DIRK JUMPERTZ: Okay, perfect. The scope of the document, it's basically to help in answering these questions. How to determine the business continuity scope, how to determine the risks, how to embed business continuity in the company DNA, what is needed for an effective business continuity strategy, what are vital materials, how to draft a business continuity plan, how to test it, and how to improve. So, normative references. Some terms and definitions.

Now, for anyone who has ever read one of the ISO 2700, 22801, or any other of these standards, you will recognize some of the headers, like Context of the Organization. That's basically one of the headers you typically find here in an ISO document. The idea here is that anyone who wants to set up a business continuity plan should first think about who they are, and what is expected of the people involved.

So, in the case of a registry, most registries are more or less the same thing. They manage the name server infrastructure for its TLD. Or they outsource IT. It can also be an outsourced model. They manage a number of public services, which we call public services, but basically, that's things like a corporate website, a WHOIS interface, etc., or an RDAP interface. All registries manage some kind of registration services and depending on the level and the complexity of the registry, this can be a manNable process,

from a mannable process up to a completely machine to machine interface, with a dedicated interface like EPP.

And it typically would also have a number of business support systems, like an e-mail system, a [fall server]. Again, this can be internally, or this can be externally, but it's important that organizations do this exercise to basically understand what we are talking about, and where everything is located.

So, one of the first steps one can do is understanding the organization and its context. It's basically look at the different stakeholders that exist, and write down the expectations. For instance, if we look here at the different stakeholders, we have the government can be a stakeholder. This doesn't necessarily mean that the government is a stakeholder. It can be a stakeholder. You also have ICANN, of course. You have your board. You have the general public. Maybe you have even a link with certain country-specific CERTs. Your employees are also stakeholders. You have law enforcement that can be a stakeholder. Registrars, registrants.

This is not an exhaustive list, so you can fill in what is important here. So, for instance, the general public, the expectation would be that the ccTLD is always up and running. That can be an expectation. And so, that has a certain relevance to your business continuity.

So, it's important to do this mental exercise to basically have a good understanding of what the entire scope is of your business continuity, and what people are actually expecting. Sometimes, what I noticed in my practical experience is that the assumed expectation is not the real expectation.

So, that means that, for instance, you can think that maybe your registration platform has to be up and running all the time, but in reality, if it's down for a week – not for a week, for a day for instance –that might well be such a big problem, and it's not expected by, for instance, your registrars, in case of a business continuity issue. So, it basically helps you in steering your business continuity.

One that is extremely important, especially within our ecosystem, but also from a global perspective, is your supply chain. It's very important that an organization identifies who their suppliers are, and how critical these suppliers are. Something that is very traditional is a telecom supplier. Or maybe you're using Amazon Web Services for some aspects of your business.

Again, it's important that you make an inventory to understand who your critical suppliers are, because if you have a business continuity issue with one of those suppliers, well, then also it becomes also your business continuity issue. So, it's really important that you figure out who is actually truly important in

your supply chain, and who is less important in your supply chain. So, I can imagine, for instance, that the local pizza delivery boys are less important than your data center and housing center. This is, for instance, a little example that basically shows how this can be filled in.

Then determining the scope of business continuity. In our case, we specifically say that operational continuity is the cornerstone of our business strategy. So, we are looking at keeping the business running at a minimal level, that's basically it.

So, we're not focusing on any other type of business continuity. Because business continuity can go very, very far and very, very broad. You have also a part that is called financial business continuity, where you're looking at your banks and money flows, and things like that. Some of these parts can be important, but we are here looking at making sure that your TLD is up and running and that you can actually service your registrars and your registrants, and everyone who is a stakeholder.

Leadership. This is also typically a part that you will find in an ISO standard. This is kind of important. This is continuity. It should not be an afterthought and it should get sufficient importance. It is also not a one-time shot. It very often requires a review analysis and a review of the process of making it always up to date.

Let me give you a practical example that is specifically for us here in Europe. A couple of years ago, we had business continuity plans, but these were typically highly technical business continuity plans. And then things happened in Europe that made us rethink our business continuity strategy. One of them was that we had a number of terrorist attacks happening both in Belgium as well as in Sweden. We have a location in Belgium and Sweden. And so, we were basically not prepared for that, and a lot of technical organizations are not really prepared for the impact of societal threats, as they are called, into their operational things.

So, for instance, when you have a terrorist attack, you would be surprised how people would react, because suddenly, people might react in a different way. And this can also have a major impact where you would no longer be able to actually access your sites, or people would have to stay home. So, it's quite important that one thinks about all these different aspects of business continuity and all the different threats that exist and take that into account. And that means that you have to review your business continuity strategy, and your business continuity plans, every single year. So, it's really important that leadership puts this on the agenda as a recurring activity.

So, the planning part basically gives an answer on how to develop practical business continuity plans. If you take any book about

business continuity, they will talk about business impact analysis, risk assessments, etc. That is really great for any traditional business, but the great thing about the registry business is that they're more or less the same. The threats can be different, the way of how you do business can be different, but high level, they are more or less the same organization.

So, here we can actually take a shortcut and make it go through the entire business impact analysis in a very quick way, and already present some of the templates that can be used to fill in everything. So, what we've done here is actually take the shortcut and already give a number of things that people can easily fill in.

So, one of the first things that is important to do is understanding what threats you are going to look at. Some of these threats – or hazards, as they are sometimes called – can be very exotic. For instance, if you look at traditional business continuity planning, you will see that people will look at a meteor impact. Well, okay, that's fine, but meteor impacts are more of an academic thing as anything else. So, you have to look actually at the thing that are really applicable to your industry. And in some cases, this can be a political thing. In other cases, this can be something very technical. In a third case, this can be nature that is a problem.

So, here is a very simple list. And this again is a non-exhaustive list, but this can be very useful for an organization to quickly have

an idea of what are the threats that are really dangerous for us. So, natural disasters, obviously, there can be fire, flood, etc. In some cases – and this is really important, the occurrence part is really important because this can actually change. For instance, you might think that tornados, for instance, are completely not important. But as Jacques has illustrated two sessions ago, tornados do happen also in Canada and can have an impact on your business, oddly enough. I remember that a registry in Europe had some issues in reaching their data center because of a snow storm. Now, where they are located, that's not very common, to have snow storms.

But these things, they do change. So, you have to make sure that the strategy registries, or hazard registries, are also updated every year because they can change.

Now, occurrence is always a very difficult one to actually fill this in, and so I've given in some of the guidelines here. Highly likely, likely, rare, unlikely, or out of scope. Obviously, you shouldn't be looking at your own registry alone. It's more looking at your environment, at the country where you're living, or the place where you are located.

So, for instance, it's not because you've never had a cyber attack or DDoS attack, that this is something that is very unlikely to happen to you. You look around in your industry, or in the

industry in general, and you will see that a DDoS attack or a ransomware attack is very highly likely to be an actual threat. It doesn't necessarily mean that it actually happened, but it can happen, very likely. So, this is the thing that ...

So, this list is basically an overview of all the hazards and the threats. So, we have the natural disasters but also human resource and medical related. So, if you're living in a part of the world where epidemic illness is a thing, then this is a thing that you should also fill in. Maybe in other countries ... And I remember, I had recently a discussion with somebody with had a serious skills and staff shortage because of political turmoil that is happening in the surroundings. So, this is again something that should also be filled in.

There are cyber threats, of course, like DDoS attacks, hackers, data loss, ransomware, cyber-war-related activities. I think the last one is something that is actually relevant, as since this year after we've seen some of the DNS attacks that happened, which were attributed to potentially cyber-war-related activities. Then there's, of course, some external threats that you can have, like recessions, civil disobedience, terrorist activities, war, invasion, you name it. All these things can be very relevant for certain registries, and they should also be taken into account.

But this doesn't necessarily mean that you can do a lot about these things. But at this moment in time, when you're doing this kind of exercise, don't bother about the fact if you can do something about it or not. Then there is financial. In some cases, this can be interesting to all, so put it in your disaster recovery plans, if they are applicable.

Technology and infrastructure. These typically are the bigger and larger failures on technology. For instance, you have a fiber cut somewhere that would actually cause your entire data center to go dark. I don't mean that the electricity is gone, but that you don't have any data connectivity anymore. Again, these are the kinds of things that you can add. Supply failure is also quite interesting. That sometimes is forgotten and can cause quite some issues. You have for instance a critical supplier, and that supplier goes bankrupt or is being purchased, acquired, by another, and this can have an impact on your business.

So, that's a list that is a very interesting exercise to do, and to give you basically an idea of, okay, what's the threat landscape? As they say in cybersecurity. Or, what's the different hazards that can happen to your organization?

So, risk assessment and management. Risk assessment is ... I always have a lot of discussion with this, because the definition of risk I'm using here is the ISO 31000 standard to describe what

a risk is. Very often you hear people mixing up risks with threats and vulnerabilities. So, it's quite important that you define and have a good definition of what a risk is.

So, for instance, it's not the risk that a power supply will blow up in your server. The risk is actually what's the financial consequence of this thing happening. And depending on how big the financial consequence is, you might decide to do or not do something about it. So, what we've done here is we've defined six different risk types: a financial risk, and operational risk, a reputational risk, a legal and confidence and a human risk.

Again, this is a non-exhaustive list. Maybe you define some other risks. But every one of these risks, there will have a certain level that is not acceptable or not tolerable for the organization. For instance, you can have a financial impact. For instance, you have a number of servers that blow up for one reason or another. There's a fire incident, for instance. And replacing those servers would cost you an amount of money. It might be that it's so expensive that it actually would endanger your continuity. So, that's where we are talking about financial risk, operational risk, reputational, legal, confidence, and human risk.

In our case, for instance, we do not accept any types of human risks. So, if there are casualties, that is potential, we don't accept

that. So, we will act upon those risks, and we will just say that risk is no longer [inaudible].

So, there are some examples here of financial loss of one million Euros. It's in Euros in this case, we maybe should translate that in other currencies. Might lead to the factual bankruptcy of the ccTLD manager. So, if that threat actually happens, then you know that this is not acceptable, and you will have to do something against it, either beforehand, or create some business continuity plans to do that.

Okay. Here's a simple risk assessment, business impact assessment. So, this is a very simple table that one can do. So, you have a threat category. A cyber DDoS attack. Is this applicable to you? Can it happen? Yes. And then you just go and think about what is actually the different risks? For instance, if you have a cyber-attack, a DDoS attack, there will be a certain financial risk that is applicable. There will be a very high operational risk. There will definitely be a very high reputational risk because it will be public, it will be visible to the public. There might be a high legal risk, or there might also be a high governance risk.

So, this is the way that you can do a very simplified business impact assessment and risk analysis. This gives you an idea of what are the threats that you really should look at. Those are

typically the ones that are highly likely to happen, with a huge risk, or a huge impact.

The other thing that is also important – and this is something that the leadership needs to define. What is your risk appetite? Your risk appetite is how you look at risks. So, some organization can be extremely risk tolerant, and others might be completely risk intolerant, depending on the type of risk. So, for instance, some organizations might say, “We don't want to have any kind of legal risks, because we don't want this.” This is something that typically needs to be defined by the leadership.

And then there are ways of dealing with those risks. For instance, in some cases you basically can't do anything about it, so you will have to accept the risk. But in other cases, you might say, “You know what? We are going to reduce the risk. We are going to reduce the impact if such an event is going to happen.” And that's something that you do beforehand. That is how you translate your business continuity strategy in a treatment plan that you will use to optimize or to reduce that impact level.

So, again, I took here as an example of the threat category, cyber, DDoS attacks. Is it applicable? Yes. What's the occurrence? Highly likely. And so, what are the different risk mitigations that are possible here? For instance, here, leadership can say we do not accept that risk. There is no way that we accept that a DDoS

attack will take us out of [the year] and brings our ccTLD in danger.

Can we avoid the risk? Obviously not, because it's inherently something that will happen. There are unknown adversaries, and so DDoS attacks will happen. So, then you can say, okay, let's define a number of things we can do to reduce that risk. From here I took as an example ... Well, for instance, for your DNS, you can look at Anycast solutions, or scrubbing services for other services.

And how do you contain the risk? And containing the risk is actually where your business continuity kicks in. And this is developing a DDoS business continuity plan, including additional technical measures, communication plan, and support plan. So, this is basically how you would define your business continuity plans, and which plans you are going to develop first.

So, finally, we have the business continuity plan itself. I created a small template. It's actually a copy of the template that we use internally, and it's a combination of the business continuity plan, which is typically high-level, and more or less a disaster recovery procedure, which is typically more low level. And in any case, you should see a number of things coming back. You should see always an assessment phase, a containment of the event, so you'll see the assessment phase.

How you contain the event, how to recover to predefined levels within the RTO, which is the recovery time objective and the recovery point objective. And then, how you step down.

The last one is actually quite important. What this actually means is this is the end of your crisis where you step down, where you stop handling the crisis and you go back to business as usual. This does not necessarily mean that you are back in the situation before the crisis.

I'll give you an example. Imagine that one morning people enter the office and they discover that half of the office has been plundered and the rest has been destroyed. So, basically, your office is no longer accessible, and so you end up with an issue. So, the crisis team kicks in, and they decide that everybody is going to work from home for the time being. At that moment in time, the crisis is handled, and so they can step down. Once they appoint somebody to clean up the mess and to make sure that the office is accessible again, there's no longer a need to do crisis management. The rest becomes a project and you do that with your standard operational approach. So, actually, I used the same example. I just referred to this example.

Some definitions of RTO and RPOs. This can be very important. Then a little thing that a lot of people forget, and that's vital materials. Vital materials is making an inventory of the things that

you need to be able to handle the crisis. This can be a lot of things. These can be contact points, these can be contracts, these can be log-ins and passwords. All the things that you basically need to be able to handle that specific crisis. And you will see in one of the further examples how this actually translates. The actually business continuity plan and the disaster recovery procedure.

So, once you have a scenario and the highest risk, it's time to draft a plan of a procedure, and one can decide to write down a detailed plan for every single step to execute during the disaster. Now, you can do that, but the problem is, it doesn't really work very well. So, don't do that. The idea is that you create a guideline, a map, that helps people to get from A to B. And how they will get there depends more or less on the situation and the actual thing. It can be very easy sometimes, but sometimes is might be very complicated. You cannot put all these things in a piece of paper.

What you do, on the other hand, is that in that piece of paper, which should be very concise and very simple, just have the highlights. This is a thing you should do. Don't forget about this thing. Then do that. And that's basically it. This becomes much more clear in the example.

So, this is a template. It has a reference number because you need a reference number to be able to refer to that business continuity plan. It handles a specific threat. Where does that come from?

Those are the ones that you decided to have business continuity plans, because they are most probable to happen, or they already happened in the past.

You have a scenario that describes the conditions that trigger the plan. You say when the plan is activated. The RTO and the RPO, if relevant. Who is in the crisis team? That includes the names and phone numbers, and basically anything that you need to be able to contact that person, who basically will handle everything that is coming next.

Always important: predefine what your priority is. You don't want, during a crisis, to have a discussion about what the priority should be. This is something that you do afterwards if they were not correct, but at the moment itself, do not discuss anything about how you should define the priorities. You know your priorities and you focus on the priorities.

The first step you do is an assessment. You try to understand how big the damage is, what is going on, and how you have to handle. Next step you do is typically containment. Make sure that the disaster does not happen any further.

A silly example, you enter the office and one of the pipes has broken off, and there is, like, a couple of ten thousand liters of

water everywhere. Well, the first thing you should do is close the water before you do anything else. That's containment.

Recovering. Describe the course of action that you do for minimal operational readiness, and then step down when you step down and stop handling the crisis. Very important: predefine your communication. It's up to the discretion of the person who is writing the business continuity plan to how far in detail one wants to go, but there are some things that are obvious, like internal communication, external communication, what you're going to communicate, who the communication lists are.

And here, again, once you have the entire business continuity plan, it's really important to use that as a preparation step. Because you will for instance have in your communication that we need to communicate with our registrars. Okay, that's fine. But then you need an e-mail list of all those registrars. Where is that list? That's your preparation part. Vital materials. This is part of that list. For instance, is a part of those vital materials.

Again, you think about what do I actually need during that crisis to be able to handle that crisis? And these are your vital materials.

Last but not least, something that is very often forgotten. You should take some records. You should take some notes. Especially when we're dealing with things that afterwards need

some link with law enforcement. For instance, you've been hacked.

So, obviously, you need records, and you have to make sure that those records are stored safely and securely because afterwards you will need them for law enforcement and any case that could happen afterwards. I'm going to scroll a little bit further because there is an actual example to clarify a little bit of all these things in the annex. So, allow me to scroll a little bit further.

Here we are. So, this is an actual example of a threat, a cyber threat, and a specific case; ransomware. So, you have a ransomware attack. Everybody knows what happened with Maersk about two years ago, the big international transport company. Did they have a business continuity plan? I don't know if they had one. But if you start thinking about it, if such a thing would happen in our organization, what would we need to be able to handle the crisis? This should be actually in that business continuity plan.

So, here we have a scenario that says a ransomware infection made a limited number of Microsoft Windows laptops unusable and lockdown. Infection can be localized in one office or is spreading throughout the organization. This is the scenario. You write your own scenario.

So, when will it be activated, this plan? Kind of obvious, immediately after detection. What is your recovery time objective? To be honest, you can't put an actual number in that you would guarantee that you would be able to do so. So, it's going to be something very vague, like as soon as possible. So, who's going to be our crisis manager here in this case? We have a technical manager, a business continuity manager, and general manager. So, there are some numbers, there are some e-mail addresses, so you basically can contact them.

What will be our priorities? Well, you're protecting the availability and integrity of the Windows server infrastructure. You isolate the affected systems, you restage in the affected systems. So, very short, what are your priorities? You don't go into detail. You don't necessarily go into detail in how you're going to do all of these things.

What is your assessment? Is the infection spreading? Who was or is the patient zero? Where was the infection actually introduced in the organization? Can you actually find that? Can you isolate the infection?

These are the things that you initially do. Once you know that's a ransomware infection, this is what you have to look at. This is the priority in the assessment phase. Containment phase. Isolate everything. Do not discuss what you are going to do. You know

here, already, what you're going to do. You're going to contain the thing. You're going to contain the incidence. So, you isolate the infected machines, you shut down non-infected machines. That's your focus.

At the moment of such an incident, that somebody comes and says yes, but I have this important meeting with somebody. Might be fine and dandy, but no, that's not a priority at that moment. The containment phase is the priority.

Some kind of obvious thing, recovery phase, affected systems we consider as lost, and will have to be reinstalled, potentially, so employees might be offline for some days. This is just what happens during the recovery. This is your step done.

So, once you have basically contained everything, and the infection's under control, then you start looking at, okay ... Just step down. So, you make sure that you identify the ransomware for signatures, identify the initial strain. How was patient zero infected? So, once everything is done, you can actually step down and do business as usual.

Communication. In this specific case – and I'm not saying that this is the way of handling any ransomware infection. This is a specific case. Internal communication [inaudible]. Why? Because only internal PCs and laptops were infected. There was no infection of

your registration platform, or anything like that. Like I said, this is only an example, this is not the example. Vital materials, documentation of the infrastructure, and set-up password vaults to access different system. Distribution list of confirmed communication and employees. Can you put them in this document? Yes, you could. But then the document becomes very big. Maybe that's not such a clever thing to do. But again, it's up to your own implementation of how you want to do this.

Another way of doing this can be like, okay, I'm going to put some references where you can find this information. Or I actually have them on a USB stick. That's also possible. Then records, create a record. So, this is a filled-in example of one of business continuity plans. Okay, where were we? Right, support.

Now, to be honest, your initial set-up of your business continuity thing will take some resources. Maybe you can have an external person helping out. It's quite a lot of administration, it's a lot of inventory work to be done. But once you've done this, that's biggest bulk of the work. The years afterwards is going to be a lot less, because you have everything already in place. You have your inventory of threats and hazards. You have your inventory of critical suppliers, etc.

So, the updates afterwards are very limited and very small. So, the initial effort might be relatively great, but once you've done

the initial effort, it shouldn't be taking that much of an effort to keep it up to date.

Awareness, of course, is always a bit of a difficult thing. You have to make sure that people are aware of these business continuity plans. And also, of the certain threats that exist, and that there are plans in place that people must follow. With awareness also comes training. So, these are very closely linked to each other. To be honest, the best training you can do is by doing either tabletop exercises, or actual simulations, set up so that people actually understand how this works.

Communication is extremely important. This is often a little bit forgotten. In a small organization, this is actually one of the more easy things, especially with internal communication because you basically can shout at each other.

But in slightly larger organizations, this can be ... Especially when they are geographically spread all over the place, this can be quite difficult to implement. Also, don't forget that when you're thinking about communications, don't always assume that your means of communications are available. So, it might be that say, “You know what? We're going to use a couple of communication means, so that we basically assure that people get the right information.”

I'll give you a practical example. We have an office in Italy, and so occasionally the earth shakes in Italy, some smaller earthquakes. Happily, that's not close to our office. But if you have such a thing, sending out an e-mail to everyone is not sufficient. That would not trigger the response from the people to be informed about "don't come to the office". So, you would need maybe having multiple means of communications. Maybe call them, or text them, message them. Use Twitter, use e-mail, etc.

Another thing that I find very important, make sure that you have to improvise your communication. So, have some communication templates ready. Especially the ones that go out in the public. It's really a killer when you have to think about, how are we going to word this? Because to be honest, if you really have a crisis, your mind is going to be wandering somewhere else, and in some cases – this is actually something that I have found out in reality – somebody who might be super cool when they're doing an exercise, when the actual thing happens, they might not be so super cool anymore and completely in panic mode. So, this is something that is truly important. Wherever you can prepare, be prepared by creating templates and making sure that they are there, so that somebody else can take over if the person that needs to do it is not capable of doing it.

JACQUES LATOUR: Dirk, we've got 20 minutes left.

DIRK JUMPERTZ: Okay, I'm almost done.

JACQUES LATOUR: How much time? Yes. Quarter past ten. Oh, okay. And then we need to talk ... Yes. Okay, thanks.

DIRK JUMPERTZ: I think I need four or five minutes. Maybe faster.

JACQUES LATOUR: Okay.

DIRK JUMPERTZ: Okay. A lot of stuff with the communications, predefine and prepare to how many communications should be set. Set a priority schedule, evaluate the need for an external crisis communication consultant. This last one can be quite important. Like I said, crisis communications is a specific type of communication, and it can always be helpful to have somebody who can help you, especially when you have to deal with media

Operation. that's basically making sure that most of the things that you have discovered during your setting up of your business continuity, lessons learned to reduce risks. You take that up in your standard operational practices. For instance, if you discover that some of your servers or some of your equipment doesn't have dual power supplies, or dual network interface cards, it might be interesting to put that as a default in your purchase.

Business continuity tests. This is really important. You can create the best business continuity plans in the world. If you don't really test them out, they are just paper tigers. They are quite impressive, but they're just paper. They don't do anything. So, testing and drilling the business continuity plans is really important. Anyone in emergency services will tell you this. This is the thing that actually makes the difference between life and death in many cases.

And so, it's really important to test them, to see that actually they work, and then to drill them, for those that are really important to you and that might happen occasionally. You can do that with so-called table-top exercises. That's the definition of a table-top exercise, where you basically sit around a table and somebody creates some incidents on paper, and then you see how people react and how they do it. This is basically how we want to do it in [inaudible].

And then we have real simulations, where you actually try to be as close as possible to the real-life thing. Now, obviously, you're not going to cut all the power to your servers in a data center to simulate this, although I know somebody who would love to do this occasionally. But you're trying to do it as close as possible, to actually see that your people are drilled. We do that at least once a year, where we basically turn our production systems from one data center to the other data center.

When you have the possibility, try even to incorporate that in your normal operational activities, so that you don't really have separate instructions to do that kind of stuff, but try to incorporate it as much as possible into your day-to-day operational activities. Now, some of these things are quite simple to do. Like, for instance, if you have an [officer] that's not acceptable, that's an easy thing to do that you can actually simulate, and then see that that what you thought would work actually works.

Improvement. This is the last stage. This is your yearly review, and what was really, truly important there is to look at your threats and your hazards. Do they change? And yes, they do change. Is there something in the legislation that might have changed? Is there something in your own business model that has changed? Is there something in your own business that is completely

different? Then these are things that you can take up in business continuity. And I think that's it. Yes.

JACQUES LATOUR: Thanks, Dirk. I think it's really impressive. Any comments on the chat, or from the RDNs?

DIRK JUMPERTZ: One, two, three. I should check the chat.

JACQUES LATOUR: Yes?

LEONID TODOROV: This is Leonid Todorov, APTLD. I'm sorry, I was late for this presentation, so I captured just the last part of it. I believe that this is a very impressive piece of work. Very impressive and very practical. My only concern is that when it comes to communication and the further promotion of this playbook, there might be a need for some kind of abridged version. Bullet points, whatever. So, that to make it, I don't know, more digestible for some non-native speakers. This is my sense.

Because once again, imagine a ccTLD manager in charge of incident response, from a small registry. He's got his hands really

full, and he will need, like, one, two, three pages for that. Because he simply has no time. In very simple language. I mean, that's very close to that ideal simple language I would think of, but still, I guess, that's very important. Yes. And with that, it would be a perfect manual. Thank you.

JACQUES LATOUR: Okay, thank you. I think the goal of this ... Well, if Dirk scrolls down a little bit. The goal of our exercise is to build a couple of these business continuity plans. The example annex. Yes, that. So, the goal is to build the top five scenarios that a ccTLD we think could be impacted, to document those. Once you've read the top part once, you understand what to do. But this is what starts the disaster.

Originally, we wanted to have a one-pager. It's impossible. Two-page, impossible. Ten, impossible. I think that's pretty much the shortest we can do. At [zero] we have a [inaudible]. So, I think this is really short. To make it shorter, I'm not sure. We can do a video. But this will be translated in many languages once it's final and public on the website. Thank you.

Alright. So, his is really good. So, the next question is how do we do the tabletop exercise or the simulation in Montreal? Do we populate five of these examples? Or, we were thinking to do the

registry is compromised scenario, document a good plan. We could do that today, to document a plan for the scenario. So, do we want to plan the logistic of the scenario today, or figure out what are the top five plans we need to work on and then go from there?

UNIDENTIFIED MALE: I think what might be interesting is to have ... I think your question is very good, Jacques. The top five threats are hazard scenarios because I'm quite interested to know what type of different things there are. Some might say a hack is our top, but then maybe some other people might say, "Yeah, but political turmoil is much more important in our situation," or something else. So, it might be interesting to see what lives with the registries as their gut feeling and understanding of potential threats because they are very different.

Handling an epidemical outbreak is completely different from handling a ransomware attack. In one case it's more a technical thing, and in the other case, it's more human-resource-related stuff. So, I think your suggestion of having the top five is really important. I would love to see that input.

JACQUES LATOUR: Let's go to the develop a threat/hazard register section. Because there you get the list of threats from the ...

UNIDENTIFIED MALE: Yeah, here they are.

JACQUES LATOUR: So, maybe we pick one natural disaster, one cyber, one external, others and ... Which one? You don't know? No, but... So, we're going to take the time and effort to document five plans. So, do we want to do a plan on natural disaster and volcanic activity and then document? So, we should pick five in this list and then ...

UNIDENTIFIED MALE: I think we can start with natural disaster because at the beginning of this workshop, I just want to remember that it was the goal of the document. When we made the first workshop, it was about the natural disaster recovery.

JACQUES LATOUR: No, it was about the ... Oh, yes, exactly. Yes.

UNIDENTIFIED MALE: It was when we were in Puerto Rico, right? And they had a natural disaster recently, so we should take that as an example, basically.

JACQUES LATOUR: So, what I'm proposing is that at the end of the document, in the annex, that we have a one-pager that documents natural disaster and hurricane/tornados. And then if we go cyber, we can do cyber, document cyber, and hacker. And the scenario in Montreal is going to be based on that.

UNIDENTIFIED MALE: I'm going to move rooms, so I'll be back with you in a minute.

UNIDENTIFIED FEMALE: I just have a question. For example, when we do a natural disaster, we will take into consideration lots of key people? Because I was thinking, for example, in HR and medical, it says loss of key personnel. So, that would be a good one.

DIRK JUMPERTZ: Yes, absolutely. Some of these hazards, they do overlap. So, lots of key personnel that can be ... The HR loss of key personnel is if

you have one or two specialists in your organization, that they resign. This is the loss of key personnel, specific for this case.

JACQUES LATOUR: You want that? People are nodding in the room. So, we have one, two three. So, we have external, financial, technology, supply failure. So, we need two in these scenarios. Which one?

UNIDENTIFIED FEMALE: Well, I think one of the worst could be electricity failure. Electricity failure that can be one of the worst things.

JACQUES LATOUR: Supply [off mic]. These are just examples, and then once you have the document, then you can use these templates to help you build your own. But at least you've got something to start with. So, if we start with scenarios that you could reuse readily, then it makes this document even more useable. So, one more.

DIRK JUMPERTZ: Jacques, I would also suggest that not only we fill in the annex thing, but we also fill in this risk assessment thing because this can also be interesting in figuring out how you could prepare or reduce the risk, for instance. So, if you're thinking about

electricity failures or any of the other ones, there might be some steps that you discover, and that you have to put in your business planner for the next year, for instance, because you can actually reduce the risk to basically zero, if you do some other stuff.

JACQUES LATOUR: So, we should add that in the annex underneath, right?

DIRK JUMPERTZ: Yes, yes. I think in the annex, we should have the primitive business impact assessment, which are just a couple of words, and defining how big the risk is, and so a very simple risk assessment. And then you have the remaining, which is actually your business continuity plan. So, I'll update that accordingly.

JACQUES LATOUR: Okay. So, one more. External?

UNIDENTIFIED MALE: Terrorist activity seems quite a pertinent subject.

JACQUES LATOUR: Okay, we'll do one on that. So, we have a natural disaster, hurricane, tornado, typhoon. Loss of key personnel. Especially if

you're a smaller ccTLD, that's super relevant. Cyber/hacker, somebody going in and doing bad stuff. External, terrorist activity. And then electric technology, and the electric grid failure. So, we got five. Perfect. So, for each one of those, we'll document the risk, document the BCP plan, document the impact assessment, I guess, and then build a bunch of templates.

So, the drafting team and the standing committee will work on that, I think. And then the goal is to have that complete by Montreal. And definitively the hacker scenario needs to be well documented, so we can do a table-top simulation.

UNIDENTIFIED MALE: What I can do is we had some experience with a similar exercise that we've done in the past, where we had an external company doing this. So, I could basically suggest to mimic the way that they've done it. So, what you do then is you have basically two teams. One team is the team that gives the input to the crisis team. And so, you run through the different scenarios, you run through the different steps that can happen. And so you're giving an input, and they act and react on that using the business continuity plan.

JACQUES LATOUR: So, tentatively it's going to be Sunday afternoon, I think, starting at 13:00-ish. 13:30, tentative. Maybe two or three blocks. Two blocks. I think the first part would be with the audience, to go through the document again, and to go through the scenarios that we have at the end. Go through the cyber hack profile, and then we'll talk about what a table-top simulation is. How does that work? What's the framework? Who's the master? What are the role of the people?

And then, at the end, we'll do a flip chart. Lesson learned . So, I think while we're doing the assessment we'll have flip charts and we'll need to document the gaps if there are any. If people don't understand certain aspects of the plan, that if it's not clear for everyone then we need to document that and address those gaps.

UNIDENTIFIED MALE: It sounds like it might be wise for us to have three blocks, Jacques. It just sounds like there's quite a lot of work there.

[DIRK JUMPERTZ]: Yeah. Well, the first thing I still need to do is I need to still clean up the document. Because at the end there is the entire stuff that we did previously. So, what I was planning to do was to cut and paste it in separate docs, but I haven't had the time to do that yet. So,

it's going to happen in the next two weeks, or something like that, as I'm not in the office next week. And then, so that we have some clean documents. And then, indeed, you're right. We should maybe put the annex in a separate document so that at like four or five different documents that can be copied and pasted, and worked on.

JACQUES LATOUR: Something just occurred to me. So, if we're going to document five scenarios – if we have electric grid failure, if we have the hacker – should we break the audience in five groups, and each one address each of the scenario individually?

UNIDENTIFIED MALE: I think that depends on how big the audience is, right?

[DIRK JUMPERTZ]: Oh, by the way, doing one of these exercises is quite time consuming and quite some effort. And especially when you're not used to it. Because very often people are playing a role, and sometimes they're not doing things that they are supposed to be doing. It's kind of really weird when you're doing that kind of exercise. I noticed that Evan was saying something, that he was doing something similar, one of these days.

The funny thing is that tabletop exercises are very difficult, in the sense that the people that are going to be there are all from different ccTLDs and have all different ways of handling things and different roles. And typically, in the crisis team, you have very specific roles that are there. So, let's say they have all security officers or technical people. Then you don't have a real representation of the people that are within your organization. So, that can be kind of tricky to do good table-top exercise.

UNIDENTIFIED MALE: I think it might be better to concentrate on one or two, at the most, depending on how many people are in the room.

JACQUES LATOUR: I agree. One. I just changed my mind. Back to one. Yes, only one.

UNIDENTIFIED MALE: Make a note of that in the minutes. Jacques changed his mind.

JACQUES LATOUR: Yes. Leonid?

LEONID TODOROV: I think that that is very great and breaking the audience in five groups should work, as long as you have a mentor with a clear-cut methodology to sort of streamline and align whatever roles and responsibilities and reflections they might have correcting, slightly adjusting, their performance. Thank you.

JACQUES LATOUR: Yes, absolutely. We'll have that. Okay, so we have a plan? Yay. Any questions? AOB? Any other business? We got two minutes to go.

UNIDENTIFIED MALE: I just want to thank the volunteers, and especially Dirk, for this very good job. Because it was not easy, it was something important for TLD-OPS groups. The TLD-OPS group wants to thank all the volunteers and hopes we'll have new volunteers are the same for the next workshop.

JACQUES LATOUR: I agree. Thank you very much, and the meeting is closed. See you in Montreal.

UNIDENTIFIED MALE: Yes, see you in Montreal. Bye.

[END OF TRANSCRIPTION]