SAN JUAN – ccNSO Members Day 2, Part 1
Wednesday, March 14, 2018 – 09:00 to 10:15 AST
ICANN61 | San Juan, Puerto Rico

UNIDENTIFIED MALE: ccNSO Members Day 2, Part 1, from 9:00 AM to 10:15 AM, Wednesday March 14, 2018 Room 209B ccNSO.

UNIDENTIFIED FEMALE: Carrie, are you on the phone bridge?

[CARRIE]: I am.

UNIDENTIFIED FEMALE: Can you hear us okay?

[CARRIE]: Yes, I can.

UNIDENTIFIED FEMALE: Okay, can you dial out to Leonid right now?

[CARRIE]: Yeah. So, I just dialed him and he said he wants to dial out right when it starts.

UNIDENTIFIED FEMALE: Okay, thank you.

[CARRIE]: Yeah, of course.

KATRINA SATAKI: Good morning, dear colleagues. Good that there are so many of you hear, despite excellent party we had yesterday. First, I have to star with some announcements. First of all, as of today morning, Adobe Connect is not available due to security reasons, as you can see announcement on the ICANN website in the application, which means that those who want to join remotely have to dial in, which means that they cannot raise their hands or submit their questions in this Adobe room. They have to either speak up or send e-mails to either ccNSO secretariat or each room is assigned, has its own assigned e-mail address. So, if you go to ccNSO sessions that we have applications and everywhere, all this information, you can see where to send your questions.

I know at least at this moment we have at least one remote participant. It's Leonid. Leonid, hello. I hope you can hear us.

LEONID TODOROV: Yes, hi. Hi, everyone. Yes, I can hear you very well.

KATRINA SATAKI: We can hear you also very well. If you have a question or you want to say anything, then please feel free to do that.

As of our discussions yesterday to attract more volunteers, one of the suggestions discussed was to have more chocolate. Thanks to Giovanni, that's what we have. Please feel free to take one or two … Three. Giovanni allows to take three. Then, you'll just have to participate in working groups.

I think that's all about announcements. Let's move forward to our session this morning and its impact on natural disasters on ccTLDs. Yesterday, Pablo already started [inaudible]. He told us a lot about climate change and how it has impacted the … What impact it has on the island here on this region. It's clear that we'll see more and more natural disasters around the world.

Sometimes we tend to forget that those disasters impact not only registries, or in our case, ccTLD registries, but they have also impact on registrars and registrants. So, this is one of the things we would like to discuss today. Is there anything we can do first to help our fellow ccTLD registries? As far as I understand, it was already discussed during Tech Day and many ccTLDs collaborate together to ensure that their infrastructure is resilient and secure and is ready to face disasters like that.

Today we have, again, two presentations from people who have learned their lessons probably the hard way. This is our opportunity to learn from them and see how we can be better prepared. How can we address these issues and what can we do to help first ourselves perhaps and then our fellow ccTLDs?

Second, another question that I would like to ask and our presenters maybe in the audience what can we do to help registrars in the affected areas? Apparently we also have to think about registrants in these areas because if you have no electricity, if you have no food, then renewal of your domain names probably is the last thing you're thinking about. But, once everything is back to normal, it's not good to discover that your domain name is long gone just because you didn't have possibility to renew.

With that, I will give the floor to Pablo to continue what you already started yesterday.

PABLO RODRIGUEZ: Thank you so much, Katrina, and good morning, everyone. Once again, welcome to Puerto Rico. Yesterday I got trigger happy with my presentation in continuing with the presentation right after the welcome message. But, thank you for that great introduction, Katrina. Without a doubt, climate change is real and we will experience more and more of this, especially in the region, the Latin American region, Latin American and Caribbean region, but throughout the world. Throughout the world, as we have seen.

So, what have done Puerto Rico, what dot-PR did is we set up two colocations. Two colocation that were exact mirrors of each other in order to ensure that we had redundancy within the island and that helped us maintain or DNS services throughout the entire atmospheric phenomena, atmospheric event. So, that's one thing that we suggest that you do. You need to ensure that you have redundancy in your country, that you have a robust infrastructure, and that you have taken the measures necessary whether you do that or you contract another company to do your backend, but the idea is that you need to maintain that level of service. That service, period, and at the level of service that you would normally want to do that.

In our case, we kept two colocations, one called critical hub and the other one called AT&T and that's what kept us on before, during, and after the hurricane.

I already mentioned to you what the level of devastation that hurricane took on us. I'm going to skip quickly because we already show some of these images yesterday.

What we learned is that normally when people talk about disaster recovery planning, some people tend to think about one disaster, but as you may hear in our case – and I understand that is the case of [inaudible] – is that disasters comes in pairs many times, and sometimes three at a time. And one disaster will lead to another disaster that you will not foresee.

In our case, we got the hurricane, but in the same area in the Latin American region, less than 24 hours before we had an earthquake in Mexico and hundreds of people died there and telecommunications and everything else related to the infrastructure was destroyed in that particular section. Imagine if that would've happened in northern Mexico, God forbid, in Monterey. What would've happened to NIC Mexico then and what would they have done? Patricio, you will share with us that Chile is now no stranger to disaster, tsunamis and so on.

So, our lesson began with Japan. Our lesson began in 2011 when our registrars in Japan approached us and they could not approach us at all. They could not communicate with us. What we did, we felt that it was necessary that we have a responsibility to protect those names. We're talking about Sony, Canon, Nikon, Toyota, Honda and for whatever X amount of dollars, I'm not going to allow those domain names to expire only because they cannot contact me or because I'm sending them renewal messages and they're not responding. Something would've happened. This is not a matter of money.

So, what we did is that we extended the renewal period and protected those names until such time where they can contact us and tell us, "Hey, listen, I don't care for that domain," or, "Yes, please renew it and then we'll take care of the money."

So, in the case of Japan, what we know is that there was a terrible earthquake, a 9.1 I believe, and then right after that, they had a tsunami. Well, the same thing has happened in Puerto Rico. We have earthquakes, and right after that a tsunami. We have seen that in Chile as well. They come in pairs, many times. And that isn't the best-case scenario. Sometimes it can come in many more of those.

In our case, we had terrible problems with water, with electricity. With telecommunications and everything else. In fact, some people are considering doing a case study because an electromagnetic pulse could do the same thing to any particular country and that is when a radioactive device is exploded and that electromagnetic pulse can wipe out anything that is electronic. What would you do then?

We make sure that we looked at our databases and compare what are the domain names … What is the country of origin that would match the particular areas that were affected by the hurricanes Irma and Maria? Once we identified those, and in our case it was about 626 of them, we automatically renew their expiration dates by four months and we continued to wait. So, as registrants or registrars approach us, we renew their domain name upon their command.

What we would like to do is to promote a discussion in which not only ccTLDs but also gTLDs can become aware that the fact that a domain name – that a disaster happens in a particular remote area, from their perspective such as in our case … I mean, what is more remote from us? We would think that what is more remote from us, from us Puerto Rico than Japan?

But, guess what? We had plenty of registrars. We have three registrars in Japan, so immediately we were forced … It was our duty to protect them and to see what can we do. So, what if a disaster happens in Puerto Rico and you are the registry in Thailand, in China, in Japan? Do you have a responsibility to protect our customers? Do you have a responsibility to protect the registrants from this particular area in your registry? That is the kind of discussion that we're looking forward to do, where we can become aware that the fact that a disaster happens in a remote part of the globe from your perspective, you should look into your databases, see who is registering from there and protect them and take the time to protect that cyber real estate and help them out to renew whenever that time comes.

We continue to look at our disaster recovery plan, and after speaking with Dr. [Lisay] not too long ago. He brought something to my attention that is very important. Our CEO died in 2014 and although we had a robust structure to carry on and we were able to carry on [inaudible], that is something to think about, too, and that has nothing to do with a natural disaster. It is a disaster, but it’s not a natural disaster. That is something to think about. It’s not only natural disasters, but what if several of your colleagues died? What if there is an accident? That’s why we see that at ICANN. People are not allowed to … Important roles cannot fly together because if there was an accident, God forbid, they would cripple the operation of the organization.

So, there are a number of things that we need to keep in mind. We need to think about this and take the time to reflect on this and take the necessary measures to protect ourselves, because by protecting ourselves, we will be able to protect our customers, our registrars and our registrants. I strongly believe that is the right thing to do. Thank you very much.

KATRINA SATAKI: Thank you very much, Pablo. Let's hear more experience from Hiro because more time passed since disasters in Japan. Let's hear what dot-JP registry have learned and how they approach their operations. Then, we will take questions together for both Pablo and Hiro. Please, Hiro.

HIRO HOTTA: Thank you, Katrina. And thank you, Pablo, about the presentation. It's very well-formatted and maybe covers 30% of what I want to say. Thank you. But, 30%.

Where is Japan? We are here and Puerto Rico is on the right-hand side of the globe. This kind of map is usually used in Japan. I use the map today, not only because Japan wants to be the center of the Earth, but also that when there's an earthquake in Japan, and if it causes tsunami, that tsunami reaches the west coast of North America and west coast of South America as well. Of course, vice-versa when a big earthquake happens in Chile, a tsunami reaches [inaudible]. So, that's why I want to use this map here.

We have a lot of natural disasters very frequently. For example, earthquakes large enough to [inaudible] even by me, it's around 20,000 times a year. It's a big number. And typhoons, which are disastrous to our territory, 5-25 typhoons hit each year our land. It's a big island, which collects a lot of natural disasters.

These are pictures taken when the natural disaster happens. The first one is 1995 January. There's a big earthquake in the Kobe area. This is a highway in Kobe. It fell down and we lost 6,500 people.

In 2015 September, it's climate change. Due to climate change, the typhoon is becoming bigger and bigger year by year. In September 2015, 40 dead. In 2016 April, there was an earthquake in [inaudible], which is the west part of Japan and 258 dead and 195,000 houses broken. In July last year, there was a heavy rain and 41 dead.

So, there are many natural disasters in Japan. The Great East Japan earthquake that was mentioned by Pablo in March 2011, which is just seven years ago, it was an anniversary this Sunday. This is the map of Japan. The earthquake center was in the sea. It's around 400 kilometers north of Tokyo.

The earthquake hits the land directly and then 30 minutes to 90 minutes later, [inaudible] hits the land and such earthquake, big earthquake and tsunami broke the nuclear plant in Fukushima. So, there's one, two, three [inaudible].

What happened on March 11? March 11 was the Friday and ICANN San Francisco meeting began on Saturday, next day, so I couldn't fly in time to San Francisco for ICANN meeting. So, [inaudible] scaled 9.0. [inaudible] quakes and buildings slanted by land liquifraction and roads severed, lifelines severed. Lifelines means water, electricity, and so on, and gas.

A tsunami happened, made by the earthquake. The height of the earthquake was nine meters on the sea. When it reaches the land and when it comes up to the land, it can be higher, went higher, and round up land slopes 30-40 meters high. So, even if they live 30 or 40 meters high from the sea level, they were hit, and nearly 20,000 dead or missing. Such [inaudible] tsunami made nuclear power plant disaster happen and they were intensely hit by earthquake and tsunami and plants broken and radiation leaked. Maybe you know.

Of course, power shortage. The [inaudible] nuclear plant [inaudible] to metropolitan Tokyo, so even Tokyo lost their power. No traffic lights even in some parts of Tokyo area. We experienced plant [round robin] blackout several hours a day.

Difficulties experienced first from the people aspect. On the day of earthquake, some facilities [inaudible] in the office, even in our office and machine rooms were broken or fell down by the earthquake. But, fortunately, none of our employees injured. We were fortunate. But, not easy to spot all employees, all of our employees because some … It happened in the daylight time, but some were out of office for business, for a day off or something. But, we have to spot whether they are safe or not.

Phones, including fixed-line, mobile, or Internet were heavily congested and lines, mobile waves, couldn't be grabbed by users so we couldn't communicate for several hours after the earthquake.

Staff safety check services. We have this kind of function, but such function is [inaudible] for this kind of emergency, but it didn't work because of the communication congestion. It's a [inaudible] thing.

Of course, employees couldn't go back home after the earthquake, which happened in daylight time. So, public transportation halted the operation because they had to do thorough safety checkups of the intense earthquake. And road congestion because many people tried to get home by cars or even by bicycles because public transportation systems were inoperable.

We have around 70-80 staff, and among them, 30-40 people – about half of them – stayed overnight with blankets and sleeping bags. You see that we did have blankets and sleeping bags prepared for this kind of disaster. In Japan, 120,000 people couldn't travel home in Tokyo area it is said.

And continued people aspects. On the day of earthquake, food, drinks in the market stores or convenience stores were sold out of course because many people couldn't go back home.

And [inaudible] couldn't sleep well in frequent aftershocks to make their minds of the fear, beer. I'm not kidding. Beer, wine, amusement, DVDs were much of help even in the office because we couldn't sleep at all, so we need alcohol and we have stock for this kind of … Not just for the party. But, I learned that chocolate is better, right?

Several days after the earthquake, not all the public transportation services were back to normal and [inaudible] blackout was [inaudible] among designated areas, and employees living in designated areas were directed to work from home. So, we need remote work facility. And employees who need to work in the office were directed to come to the office, but back home early during daylight time. The government directs people to stay home as far as possible to avoid troubles and safe electric power.

From service aspect, on the day of earthquake, all sorts of problem fighting must be done immediately, so safety in the office for staff, for [inaudible]. And country [inaudible] of the service, DNS, WHOIS, registry system, [inaudible] and so on. And service in the office, service in the data centers and [inaudible] function. But, fortunately, dot-JP services were not disrupted, some [inaudible].

During several days after the earthquake, decide how domain names should be handled, should be relieved as Pablo said. People, meaning registrars and/or registrars in the disaster-affected area may not be able to renew their domain names, even if the domain names are about to expire. Such domain names are automatically renewed with no charge, it's decided by our company. And [inaudible] to the public was not done, only through registrars. It's a kind of no good thing, but because we want to say that [inaudible] because we are ready to help you. But, some registrars could not extend this kind of service to relieve their registrants. It's a pity, but this is the reality. This was the reality.

Preparing ourselves for the future, we do have [inaudible] for all employees, how to evacuate, how to safety check and so on. Who, what, how you should report the telephone number, e-mail address, and SMS account. How to [inaudible] lock doors. This is a very important thing because usually our offices are locked electronically. So, if the power is off, we cannot open. Of course, it can be opened manually, but usually we don't know how to unlock it, how to manually unlock it, [inaudible] safety boxes. And brief manual within smartphone or on paper. This manual is on paper and on smartphones.

And survival kit. Food, water, gloves, helmet for every employee, plus more. Plus for the visitors. And sleeping bags for office stayers. And basic dress often done, [inaudible] twice a year and periodical [inaudible] drills. The company has to allow our staff, employees don't come to the office because office is in danger or something, so we have to give SMS or Internet mail to them, but it needs drilled because those [inaudible] are often changed but not reported [inaudible]. So, we do have to give it periodically.

And preparing ourselves for organization, ensure this is [inaudible]. And basic criteria for making employees to go home or something, of course. And emergency communication, too. That second one is important.

For all employees, e-mail accounts under a TLD other than dot-JP. We need this because Japan is hit by natural disaster and maybe dot-JP DNS doesn't work. So, we need another TLD to help us. Three more pages.

Remote work environment, I will skip this.

Disaster recovery sites. We have Tokyo and Osaka 500 kilometers away. [inaudible] systems and staff are in Tokyo and also in Osaka. And periodical drills to switch the active site. [inaudible] DNS servers within regional ISP networks. This is still experimental research. I will talk about this later. Crisis management committee is created in our company, [inaudible].

So, this is a picture. Three-day survival kit is stored under each employees desk. This is my desk. Clear. Under my desk, fully clear to hide my body. I am small enough to be under this. It may not fit, but yes. This is mandatory for all of our employees to clear their desks to hide themselves.

Storage with three days of [inaudible]. It's triangular box here, and inside [inaudible] open the lid, right inside the top. This is the contents of the box. For each employee, I think we used 200 US Dollars for this survival kit. Of course, there's some water and food. We need to change them periodically. Yearly or semi-yearly.

This is the last slide. [inaudible] DNS servers within regional [inaudible] ISP networks. This is the research effort with eight domestic ISPs which covers all over Japan. So, those ISPs are provided by regional electric power companies or their affiliates and the area covers don't overlap and collectively cover the whole Japan.

So, if the DNS servers manage [inaudible] JPRS, the [inaudible], the copy of the DNS server are operated by these eight ISPs, so they can provide [inaudible] to their area. It may help us if some part of Japan – I don't want to use the word, but if some parts of Japan dies, the other part works for dot-JP. This cooperation will make JP DNS survive even when many parts of Japan are in trouble due to natural disaster. Thank you.

KATRINA SATKI: Thank you very, very much. I've learned a lot. I don't know how about you. Actually, this is one of the things I really wanted to focus on. We shouldn't talk only about infrastructure. Of course, it's vital and it's very important, but we need to take care of the people who take care of infrastructure. Therefore, I think that's … For me, it was very educational and something clearly to think about. Eberhard?

EBERHARD LISSE: Eberhard Lisse, dot-NA. You are all aware that we have also been hit by a personal disaster and that one of my business partners suddenly died on Friday. What Pablo said, it's not only natural disasters or personal disasters. Things can happen at the same time. While you can have enough [inaudible]. For example, Steven Deerhake and I have agreed to exchange non-executive directorship positions now, so that if something happens to him, I can look after his [inaudible] who are not involved and the other way around. Then, we [inaudible] company registers. This is all involved and there is no cost involved. Then, we exchange [inaudible] credentials, but not the [second factors]. My things are in a trust. My trustee has full documentation to know exactly what he needs to do in case he needs to have access. We have got already … We had, fortunately, a system in place to deal with this. We had been thinking about it for a year now because we are not getting younger. But, this is something that you need to … [inaudible] is also not the youngest from dot-VI. And the small ccTLDs, if you are a one- or two-man operation, you must be very clear on what is going to happen.

A purely technical question, the survival kits, you are aware of expiry dates. So, do you buy 200 kits? It's just mundane. When I was younger in my Army time, I was dealing with logistics and had to look at [expire dates] of drugs all the time. But, the food, you can't keep the food in there for ten years, so how do you deal with this? Do you buy 200 packets and renew them all at the same time or do you keep track of the expiry dates?

HIRO HOTTA: Thank you for the question, Eberhard. There is a service who delivers the replacement to us. They manage the expiry date. Before that date, they deliver the replacement to us.

KATRINA SATAKI: So, that's a service that's outsourced.

PATRICIO POBLETE: Patricio Poblete from NIC Chile. We're beginning to work on designing and implementing a second location where we could operate in case disaster hits our main offices. We're having trouble deciding what to put there, how much to invest in having things that would be basically on standby until the day, if ever, that we would need it. How do you handle that? Did you already have two locations? What do you put in Osaka, for instance? How do you handle that?

HIRO HOTTA: Okay. Thank you, Patricio. Actually, Osaka site is a secondary site. It is still smaller. Our plan is to make these two sites equal size. For example, we plan to use Tokyo site for one month and even when there's no disaster, we change it to Osaka. Yes, [inaudible]. No, no people. Just a system because there's remote work environment there. For the system, we'd like to have almost the same copy in those two sites. For the people, at this moment, among our 80 employees, 70 are in Tokyo and ten are in Osaka. So, Tokyo is the main site, staff viewpoint. But, maybe it's not easy to move another 30 to Osaka because Tokyo is their basic life space. We have to think about that, how to operate equally in these two sites. But, we are still thinking about that.

KATRINA SATAKI: Thank you very much. Speaking about automatic renewals, Pablo said you extended it by four months. So, you decided just to go with one year. Pablo, any specific calculations? How did you come up with four months?

PABLO RODRIGUEZ: We recognized that the majority of the people that were affected by the hurricanes were in the region. We were doing it by … We were playing this by ear. So, we figure in four months, most of these regions should be at least at a level of operation where they could communicate with us, within four months. If they were not, we would continue to extend the renewal date. We had no intention of allowing those domain names to expire until we would get a definite response from the registrars or registrant. But, we figure that within four months you should be able to contact us. That's why I came up with the four-month period.

KATRINA SATAKI: Okay, thank you. In case of dot-JP, if I understand it correctly, you had a possibility to identify which registrants are from which areas, affected areas.

HIRO HOTTA: Yes. From the registry data [inaudible], we know [inaudible]. For example, if a disaster is designated as a [inaudible] for the law of relief. There's a law of relief from natural disasters in Japan. The government identifies which city, which area, was the most disastrous area. So, we know where the most disastrous area is and we know who lives there, so we can identify which registrants are in disaster. It's a [inaudible], but we use that to identify who [are in danger].

KATRINA SATAKI: Yes. But, how would it be possible for us registries, for example, in other countries? If we want to take care of our registrants in affected areas, we need some effective mechanisms to be able to identify those registrants are from those areas. I'm not saying we can find a solution now. I'm just dropping a question for …

UNIDENTIFIED MALE: Food for thought.

KATRINA SATAKI: Yes, exactly. Any other questions? One thing, actually, very interesting. If I understood it correctly, in JP, you bought some system in order to inform all your employees, right? And it didn't work because of the congested network? Okay, so probably not always a good idea to rely on technologies.

PABLO RODRIGUEZ: Yeah. In our case, it's different because we were not affected by an earthquake which is so sudden. It's unexpected. In our case, because it's a hurricane, we know in advance. We have several days. We can track it. Normally, hurricanes begin in the west coast of Africa. We track it from the moment there is a storm. We can track them. So, we know where. We're counting days. Once they reach a particular area of the Caribbean … They travel as a storm until a particular point in the Caribbean where the waters are really hot and that's when they become a hurricane. At that moment, we start counting. There are so many days before it reaches us, so we start moving very quickly.

Most people in Puerto Rico and in this Caribbean region already are storing food and water. For example, we're talking about this. We're less than 90 days from the hurricane season again in Puerto Rico. Hurricane season starts in June and it's March now, so it's less than 90 days. Boom. Hurricane season all over again.

So, most people already in their houses have food. They have water. They have non-perishable goods and we preparing and storing things, so food and water and that type of thing, it's not unheard of to have it. And in our offices, pretty much like you do in JP, we also use them as storage because right after a natural disaster, we use them to give them away to different communities that were affected. So, we store lots of cases of food, water, Pampers, baby food, powdered milk, that type of thing. At least we have the head's up.

On the other hand, what we do or what we have done is that we make sure that we have redundant systems throughout the entire process to ensure that our customers are taken care of and that our registrars and registrants are taken care of.

But, unlike having … The majority of the cases of a natural disaster, the proximity of the different island states are so close. So, Puerto Rico is very close. The Dominican Republic is very close to Cuba and on and on. We are literally in a chain. Normally, we all get hit at the same time. So, we have to be able to be ready to take care of those that are not affected.

In the case of Irma, we were not hit by Irma as hard as Antigo and [Bermuda] was, dot-AG. So, we were taking in people from Antigo and [Bermuda] flying them to Puerto Rico and taking care of that and Virgin Islands.

Then, after that, we got hit, so other islands further south in the chain who were not hit attempt to help us. And of course, from the mainland US. That's something that we tend to do. Something that we found that was really difficult was the fact that you're an island, you need to bring fuel, gasoline, and diesel and that's really complicated.

So, in our case, we tend to look to the mainland, US, to look for facilities where we can contract and have mirror images there that can also or we outsource our backend, not because we cannot do it, not because we don't have the know-how, but only because it's so much easier that if something were to happen in that particular area, we can always drop food, water, fuel, and everything from other parts of the mainland US. So, that is another advantage that we consider in order to maintain and sustain our services.

KATRINA SATAKI: Thank you very much. If there are no more questions to Hiro and Pablo, then I'll give the floor to our regional organizations. They ran a survey to see how ccTLDs, registries, around the world are prepared. Do they think about disasters? Yes, please.

MIGUEL IGNACIO ESTRADA: Hello, my name is Miguel Ignacio Estrada. I'm the general manager of LAC TLD. Here's Barrack Otieno from AFTLD. I think we have Leonid on the phone, Leonid Todorov, from APTLD.

This presentation is about disaster and emergency preparedness in ccTLD registries. Barrack and I will speak on behalf of the [inaudible], APTLD, AFTLD, CENTR, and LACTLD.

The following slides shows the result of a joint survey we conducted to our member ccTLDs during January and February of this year after receiving a request from Javier Rua from ALAC regarding the preparedness of our ccTLDs in case of disasters and emergencies.

We had 50 unique responses from ccTLDs around the globe regarding the word disaster. For the purpose of this survey, we defined disaster as any event that costs business or operations to cease. They could be natural disasters, as earthquakes or hurricanes, server attacks, [inaudible] failures, software or hardware or human failures.

This slide, we can see that incidents are on the rise. 44% of ccTLDs have been impacted by some sort of disaster or emergency over the past 15 years. As you can see on the chart, the most recent incidents were in 2017. We had disasters … I'm sorry, next slide.

The most frequent are cyber attacks or security compromise. We have natural disasters, [inaudible] failures, network failures, software failures, and human errors.

The most recent disasters were hurricane [inaudible], the Christchurch earthquake, Hurricane Maria. We had DDoS attacks politically motivated and some power outages due to, for example, track crashing into power lines and [inaudible]. Barrack?

BARRACK OTIENO: Thank you. In the survey, we sought to understand some of the areas that were most impacted when disasters occurred. From the survey, it weakness clear that breakdown of machinery or system was reported as having the biggest impact to registries. There are, of course, other areas that were impacted, as you can see on the slides. Utility outages. That is, power outages. Damage to IT systems. Staff unable to access the workplace, interruption of supply chain, physical damage. But, most of this, the most of the [inaudible] had systems that they were able to mitigate some of these challenges. But, breakdown of machinery and systems affected them in a very big way.

Other impacts that the affected registries encountered included loss in customer confidence. This was rated as one of the most impacted areas as a result of the disasters and the emergencies. Data loss was also rated as the least impacted aspect. From the presentations you've had, you can see that a number of registries have deployed their [anycast] systems that make sure that at least the registries are available even after disasters take place.

In terms of response time, whenever disasters occurred, 50% of the respondents were able to recover essential operations and services in under six hours. Again, when you look at the presentation, you can see from the response how the 50 registries address this issue and you can see that at least 50% of the registries that were surveyed were able to respond in under six hours.

UNIDENTIFIED MALE: So, in terms of [inaudible] response, regarding tools and teams, we see that 86% of organizations have [inaudible] text or [inaudible] messaging services for communication during the disasters. It's a good thing, but as we saw, it's not always effective. And 75% of organizations have a dedicated incident response team. We see that [inaudible].

BARRACK OTIENO: 43% of the respondents estimated that their staff are partially set up to perform remote recovery. From the survey, again we established that organizations with large domain counts – that is more than 50,000 domains – are better prepared to recover the operations remotely.

In terms of overall preparedness for a disaster or emergency, 78% of the ccTLDs that responded consider the organizations either prepared or very prepared for disaster or emergency.

You can see across the regions how prepared the country code top-level domain registries are for disaster or emergency. Again, from the respondents, a number of registries say they are very prepared, as you can see, and they're willing to talk to any of their counterparts that is interested in knowing or learning how to put in place contingency measures for disaster recovery. You can see the list of registries that say they are very prepared on the lower line there.

In terms of the lessons learned, the respondents highlighted the need to prepare a disaster recovery plan, a documented disaster recovery plan for that matter, not just a talk show. Regular testing of the disaster recovery plan. It's one thing to have a disaster recovery plan and it's another thing to know that it is functional. You've seen some questions being asked here. Sometimes the water can be expired or the food can be expired, meaning it leads to another disaster.

Communication is critical during disasters and data backup is also very critical.

Some other key points that we picked from the survey, half of the ccTLDs globally have faced some sort of disaster or emergency. So, if you haven't encountered it, it's on the way coming.

Again, most incidents relate to cyber security. Breakdown of machinery is the most common immediate impact. Loss of customer confidence, rated as having a high impact to the organizations. Again, incidence response times are mostly under six hours. Most registries have response teams and instant message communications in place. Larger registries are even better prepared from the survey. Again, 78% of country code top-level domain registries globally consider the organizations either prepared or very prepared for disaster or emergency.

We got some resources from the respondents that they felt worth sharing with colleagues. Most organizations provided some details on their current disaster recovery plans in the survey. This report will be shared in coming weeks. We will circulate it with those that responded to the survey, but again we want to encourage most of the ccTLDs to be responding to these kinds of surveys in the future.

So, the TLDs that are listed there are able to share their current plans if you wish to contact that. So, you can see dot-AU, dot-CA. You can see the list. This presentation will be available on the ccNSO website as well. You can have a look at it.

One of the resources that was recommended was disaster recovery and business continuity, the act of service suggested by dot-BR. We also have a suggestion by dot-DE that is listed there.

Again, we have the [ISOR 27,001] series of standards proposed by [dot-LA] and [ISOR 22,301] proposed by dot-UK. So, most of this, especially the last one, looks at societal security and business continuity management.

That’s it. Thank you for your attention.

KATRINA SATAKI: Thank you very much. Yes, please, [inaudible].

UNIDENTIFIED MALE: I would like to thank CENTR for sending us [Patrick Miles] in conducting this survey and then given the final analysis.

KATRINA SATAKI: Eberhard, please.

EBERHARD LISSE: I just wondered, it was a CENTR survey sent to CENTR members, not to ccNSO members, because I don’t recall having gotten it.

KATRINA SATAKI: It wasn’t ccNSO survey and it wasn’t CENTR survey. It was a survey distributed by regional organizations to their members.

EBERHARD LISSE: Oh, okay.

KATRINA SATAKI: Yeah. That was an initiative taken by [Ros].

EBERHARD LISSE: [inaudible] have been better to distribute it, to send the surveys, to all ccNSO members? I wonder why the report is only made available to the respondents and not to all.

UNIDENTIFIED MALE: Normally, it's a reward for those who take their time to respond. So, it's a lot of work responding to some of these surveys. So, from time to time, we do it as a reward. But, of course the presentation will be publicly available to members of the ccNSO.

UNIDENTIFIED MALE: Of such an important thing, you will only send it to the people to report and not the ones who didn't, are not aware of it, and the ones who might be affected. Are you seriously suggesting this?

KATRINA SATAKI: Thank you. It was an initiative taken by [ROs]. Thank you very much [ROs] for this initiative and for summarizing all the response. It doesn't mean that we cannot do that, some lessons learned from this survey. Maybe we could add new questions, taking into account presentations that we heard today, some new aspect. We could extend the survey and then again ask – maybe this time we can do it and ask all ccTLDs. Not only ccNSO members, but all ccTLDs that are interested in answering the survey to provide their responses and share their experience and ideas. Yes, please, Bart?

BART BOSWINKEL: May I suggest that maybe … I don't know if somebody from TLD Ops is in the room, that TLD Ops context [inaudible] see if they can push this forward because then you have an outreach to probably the most populated group and this is something …

KATRINA SATAKI: Yes, thank you. And I think we have a question from Leonid who is on audio. Leonid?

LEONID TODOROV: Yes. Katrina, thank you. Can I have a couple of minutes? I just want to fill up on what was already [inaudible].

KATRINA SATAKI: Absolutely. I just want to ask if it's possible to make it louder because it's very difficult.

LEONID TODOROV: Oh, yes.

KATRINA SATAKI: Yes, good. Excellent.

LEONID TODOROV: I'm good now?

KATRINA SATAKI: Perfect.

LEONID TODOROV: Okay. So, first of all, hi. I'm sorry that I couldn't be with you in person and I just want to commend the dot-TR team for raising this very important issue and my colleagues and all those who responded to the survey because that was very interesting. To the best of my knowledge, it's probably the first truly collaborative effort for all the regional organizations, although Barrack may prove me wrong. I don't know.

Anyway, I think that one of the most interesting aspects of the survey was the one which was not basically made available to the audience and to us as well, and that is the question of those ccTLDs which were left out, or rather, preferred to stay out of that survey. I think that they're the least prepared ccTLDs, and probably – this is just my guess – one of the challenges is that once we have most ccTLDs quoted in the survey more or less prepared for any kind of natural disaster, there is quite a number of those again not covered by this survey, which are the least prepared for any kind of disasters because of a number of factors, such as, for example, limited communication with the external world [inaudible] the ccNSO community. They have very few registrants and very limited resources, [inaudible] of stuff, and they are prone to not only natural calamities, but all kinds of social challenges including political unrest and war and [inaudible], whatever.

Of course, the level of their observants of the ISOs is very minimum. So, I think that we should also focus on those ccTLDs because they are the most vulnerable link in our chain.

So, I believe that the time has come and I fully support dot-[DR]'s idea to come up with comprehensive guidelines or a manual, if you will, or handbook for all ccTLDs in which we should probably put in every detail all the findings of the survey and all the best practices to date. And of course these manuals should be updated regularly and we will try to collect as much information from each individual ccTLD.

We also, as Bart already started telling you, probably have the best platform to do that because TLD Ops, it seems to me, is most suitable platform – the most suitable platform for such kind of work as there might be created a special dedicated subgroup to address the matter and to draft this holy book of preparedness, if you will.

Then, considering some further steps. I believe that we should also be very practical and think, for example, of some capacity building project which might be funded by regional organizations, so whether on the bilateral or multilateral level. We have that perfect example recently when dot-SE stuff was sent to CIRA for a week-long training. Why wouldn't we consider something like that, sending those officers, customer relations officers or security or whatever officers, technical officers, from those smaller, vulnerable ccTLDs to the most advanced ones to get that firsthand practice.

Of course, we should also not underestimate the quite extensive experience cumulated by some other platforms and organizations, whether it's ITU or, for example, for Asia-Pacific it's APEC, Asia-Pacific Economic Corporation that have already addressed the issue and developed certain guidelines and recommendations on the matter, so we can build on the existing good practices. It's just a matter of our goodwill to get in touch with them and ensure some credible input, for the benefit of end users, of course.

So, that is it. I just want to thank Hiro. I would echo Katrina. I think that every minor detail matters and sometimes we are too focused on the critical infrastructure and things which are supposed to ensure business continuity in the technical terms, but we tend to forget about those people behind those machines and software. Thank you very much.

KATRINA SATAKI: Thank you very much, Leonid. I see Byron has comments. Byron?

BYRON HOLLAND: Byron Holland, dot-CA, for the record. First off, I just want to thank everybody here. I know that the two of you in particular have gone through great hardship and I appreciate you sharing what obviously was an extremely difficult situation with the broader community to stimulate our own thinking. As Leonid just said, it's not the big systems necessarily, which often we are relatively prepared. It's the little things that you don't forget about – that you sometimes forget about – which are extremely valuable lessons. So, thank you for sharing that with us.

I also do want to say thanks to the regional organizations who did the heavy lifting and undertook the surveys and did the work to come here and also present it to us and make us think about it. I think that what we've heard here is a real opportunity. Never let a crisis be a wasted opportunity, so for that. But, also, all the work that you have done and the presentations that you've given. I just want to say thank you for that.

I think it has stimulated, actually, a really good dialogue here because while the [ROs] have kicked us off and done good work in their respective regions, I think this is a real opportunity for us as a community to get together a little more holistically, and with it's TLD Ops or the ccNSO, build on the work that you've done so we can share that work more widely. I just want to say I think this is a great opportunity to really do that and we should take it up ourselves as council to see how can we foster this even more so than has been done already? Thanks.

KATRINA SATAKI: Thank you very much, Byron. Patricio?

PATRICIO POBLETE: A number of years ago, I participated in a workshop held together with an ICANN meeting, what was called ACRP. [inaudible] contingency response plan was given by a couple of fellows from a company called Delta Risk.

I learned a number of very valuable lessons there. Just like people were saying, it's not only the technical part that we have to worry about. It's of course all the people that are involved. Also, that sometimes when disaster strikes, you also have not only a technical problem, but also a political one or a public relations one. If your registry is failing for some reason, you'll come under heavy criticism if you [inaudible] not have been prepared for that. Suppose it only hits you and not the whole country. When it's the whole country [inaudible], you have an excuse. But, what if it's not?

Then, you need the whole network of people that you should know, have been on good terms with, and be able to access and tell them what's really going on. You have to be transparent. You have to have a communication plan and so on.

I find it really good that we have this renewed interest in the matter, and perhaps we should organize that kind of a workshop again, roll up our sleeves and really work on this and bring all our experiences together and try to come up with plans or ideas that are up to date and learn from all the experience of people who know how to do this and people who have suffered this kind of thing.

KATRINA SATAKI: Thank you very much. Eberhard?

EBERHARD LISSE: It was in Mexico where that presentation was given. We also had a shorter version of that on Tech Day. The Tech Day committee, the Technical Working Group, has discussed this on Sunday in the face-to-face and we are looking at doing something in Barcelona about this. We will be, of course, inclusive.

KATRINA SATAKI: Thank you very much. Useful information. [inaudible]?

UNIDENTIFIED MALE: [inaudible], dot-FR for the record. Thanks, all of you, for that very interesting information. We don't use in France to be a face of this kind of problem for the moment. I will take the role of TLD Ops [inaudible] community member. One of the goals of the TLD Ops group is to produce materials to help ccTLDs [inaudible]. We will [inaudible]. We will enjoy to work on this kind of problematics with these kind of materials you can give us. Thank you.

KATRINA SATAKI: Thank you very much. Thank you. I hope that you found this session valuable. I heard some feedback from you saying that, yes, this is something we need to think about. Yes, even though

… Personally, I feel privileged to live in a country that hasn't been hit by any such disaster. The worst thing we could get is to be attacked by a hungry mosquito.

PATRICIO POBLETO: Or [inaudible].

KATRINA SATAKI: That's true. Absolutely. Yes. You're right, Patricio. That's why I really learned a lot from this session. The fact that currently we're not affected doesn't meant that it will last forever. Something can happen at any time. Yes, as Patricio puts it, if it's whole country, it's one thing. If it's just you, you have no excuse.

Thank you very much to everyone who shared their experience, regional organizations who prepared – came up with this initiative and prepared a presentation, thus giving us more food for thought and some ideas how we could proceed further. I hope nothing bad will ever happen to any of you, any of us. But, if it does, then we can always rely on our fellows from other ccTLDs. So, thank you very much for this session. We break for coffee.

LEONID TODOROV: Thank you, bye-bye.

KATRINA SATAKI: Thank you, Leonid. Bye.

[END OF TRANSCRIPTION]