ICANN Transcription

IDNs EPDP

Thursday, 22 December 2022 at 13:30 UTC

Note: Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. Attendance and recordings of the call are posted on agenda wiki page: https://community.icann.org/x/PYYFDQ

The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page http://gnso.icann.org/en/group-activities/calendar

DEVAN REED: Good morning, good afternoon, good evening. Welcome to the IDNs EPDP call taking place on Thursday 22 December 2022 at 13:30 UTC.

We do have apologies today from Michael Bauland and Nigel Hickson.

All members and participants will be promoted to panelists for today's call. Members and participants, when using the chat, please select everyone in order for everyone to see the chat and so it is captured in the recording. Observers will remain as an attendee and will have view only chat access.

Statements of interest must be kept up to date. If anyone has any updates to share, please raise your hand or speak up now. If you need assistance updating your statements of interest, please email the GNSO Secretariat.

All documentation and information can be found on the IDNs EPDP Wiki space. Recordings will be posted shortly after the end of the call. Please remember to state your name before speaking for the transcript.

As a reminder, those who take part in the ICANN multistakeholder process are to comply with the expected standards of behavior. Thank you and over to our chair, Donna Austin. Please begin.

DONNA AUSTIN: Thanks, Devan, and welcome everybody to our last IDN EPDP call for 2022. I guess first of all, I just want to thank everybody for their work throughout the year. I think we've made some good progress. We've still got a little bit of work to do if we're going to hit that deadline in April. But I sincerely thank everybody for their input and commitment. I don't think we've lost too many participants along the way, which is very encouraging.

We're going to try something that we don't think any other group has tried before. This isn't going to be perfect by any stretch. But we're going to have a look at risk assessment in the context of denial of service and misconnection risks that were identified by the small group for the string similarity review.

I just want people to bear in mind that we acknowledge that this will be a subjective test. We're looking for input and thoughts on people about where they think the risk might be. But we do recognize that this isn't mathematics or there's no defined outcome here.

So we're going to give it a go and see where we land. James Caulfield, who most of you who were in KL might remember, James is on ICANN staff, and he gave us an outline of what risk assessment is and how it could be useful. And James is joining this call as well, mostly to observe. But if there's any technical questions we can't answer as a leadership team, or Ariel, who's done a lot of work to pull this deck together this week, James is here just to provide some guidance.

So I understand we haven't done this before. So it's a little bit novel, I suppose, in that regard. But I'd just ask folks to keep an open mind on what we're doing. We've had a lot of discussion around string similarity. We appreciate there are some risks associated with it. We're trying to determine whether the hybrid model is the best path forward for us, or given recent information from ICANN staff that it will add layers of complexity to the evaluation process and some of the data that was collected by Pitinan and Sarmad on the 20 strings that we reviewed a couple of weeks ago—we've got a little bit more data. So just keep that in mind. And let's work through it and see where we get to.

Obviously, this is the first time that folks have seen this, had an opportunity to think about it. So it's not the last conversation we'll have on this. We'll come back to it early in the year and see how folks think about it. But this is really the big question that's in the way to us getting our initial report done. So let's see how we go today. And hopefully, we'll make a little bit more progress than we were when we started. So with that, I'll hand over to Ariel.

ARIEL LIANG: Thanks, Donna. Hello, everybody. Before we do the risk assessment, this is a quick refresher why we're doing this exercise and remind folks the steps we have taken and brought us to today's exercise.

So the first point everybody should remember is the small group for string similarity recommended the hybrid model. And it was mainly to meet the singular goal of risk mitigation of the two failure modes, according to SSAC.

One is the denial of service. But we realize this term may be kind of misleading in a way, so maybe we can just call it no connection. And then the second type of risk is misconnection. So hybrid model is designed to mitigate these two risks as much as possible.

And the caveat is that the small group did not consider the implementation complexity of the hybrid model. So that's something basically the EPDP team has to request ICANN Org to provide input.

And then when the hybrid model was brought back to the EPDP team for the full discussion, we have heard generous support for the model. But we also heard reservations expressed by representatives of some groups in terms of implementation. So we do know there's a reservation from some members for this model.

And when ICANN Org got back to us regarding the operational inputs, that's something we heard two weeks ago. So basically, the Org team conducted analysis to determine the potential number of comparisons that need to be performed in a string

similarity review. And they calculated these numbers based on four models.

Basically, level one is basically the primary against primary. Level two, primary plus allocatable variants against primary plus allocatable. Level three is everything is being compared against each other, including the blocked ones, and then the hybrid model.

Just to remind you, the numbers that the ICANN Org team provided, they selected 20 gTLD strings in a random fashion and calculated the theoretical limits for the number of comparisons in all these models. So one thing to emphasize here is if you look at the number of comparisons for level two versus the number of comparisons for hybrid model, the theoretical limit increases almost 38 times from level two to hybrid. So definitely a huge jump.

And what we can deduce from this input from ICANN Org is that the hybrid model may introduce more complexity, because in essence, the string similarity review is a manual process that cannot be automated. And if we have this many number of comparisons need to be conducted, the more time and more people will likely be required to complete the work. And that means some more cost for conducting the review will likely occur. And then those costs will be passed on to the applicants due to the cost recovery principle of the new gTLD program.

So that's a refresher of the ICANN Org inputs. And after we reviewed this input, a few members in this team suggested that we revisit the risk assessment exercise to understand the risk of

the denial of service or no connection, and then misconnection risk. So in that way, we can better understand whether the hybrid model is commensurate with the risks and whether the risk level are high enough to justify the complexity and costs for the applicants if the hybrid model is indeed used for the program.

So that's a quick refresher on the background, why we're doing this exercise. And now, this is an overview of the risk assessment before we jump right into it. So, the purpose of this is to assess the risk level of the two failure modes that I just mentioned earlier, and understand whether the mitigation measures are commensurate or appropriate to mitigate the risks.

And then there are two terms I hope everybody can keep that in mind. One is the inherent risk. So that means the level of natural level of risk without doing anything to reduce the light likelihood or mitigate the severity of the risk. So that's one risk we need to assess. And second is the residual risk. So that means the risk remaining after the inherent risk has been reduced by mitigation measures. So that means once the mitigation measure kicks in, how much risk is left for our consideration. So this is the risk level we need to assess.

And then the specific risks being assessed—there are two. One is denial of service. Also, we can call it no connection. The other is misconnection. And we can go to the description to provide more detail on that.

Another factor we need to assess is called the control effectiveness. So it's basically a fancy way of saying the effectiveness of the mitigation measures. And in our current

context, we have put forward two options on mitigation measure for our consideration. Option one is hybrid model as the obvious option. And then option two is the level two for string similarity review, plus, the string confusion objection using the hybrid model.

So based on the discussion between leadership team and staff, we believe you cannot just look at the string similarity review in isolation, you should also consider other measures in the new gTLD program that can potentially detect confusingly similar strings. So the string confusion objection comes into play. And if we use the hybrid model there, in conjunction with the level two of string similarity review, then it might be also a viable option for consideration. So that's why we're putting two options on the table for the group to assess their effectiveness for mitigating the risks.

Another assumption I want to note here is that, once we have the mitigation measures kicking in, may have the effect of lowering the likelihood of the risks or lowering the severity of the risks or doing both. But if we're looking at our current context, our assumption is that the mitigation measure will mainly impact the likelihood because as a result of these options, fewer strings may be delegated in the zone. So it may lower the likelihood of the user, for example, encounter problematic domain names. So we thought the mitigation measure will mostly impact likelihood, as our assumption.

Another important point is that some to assess the risk, we need to identify a target audience and for simplicity reasons, we tried to do this exercise based on the perspective of individual Internet and users at the micro level, so it's probably more straightforward

and easier to understand in terms of their experience encountering a problematic domain.

Another assumption we have is that an individual's experience can be extrapolated to understand the collective experience by the end users at the macro level so we could potentially generalize an individual's experience to reflect the broader end user population, their experience with domain names.

So these are some assumptions we kind of put in this exercise. So, something to keep in mind. And lastly, this is something where we talked to James, and he also kind of stressed on this point, is that risk assessment is inherently subjective based on the professional judgment of the assessors. So we don't really have rocket science or hard data to support our exercise at this point. So it's a subjective exercise, but at least it provides some kind of framework and structure for us to conduct it. So it doesn't sound too wishy washy based on sticking a thumb in the wind. We at least have some structure to guide our thinking. So these are some general points for this assessment. Maybe I should stop for a moment and see whether there's any questions comments, before we jump into the exercise itself. And I saw Sarmad has his hand up.

SARMAD HUSSAIN: Thank you, Ariel, I just wanted to add to this that as far as risk is concerned, another stakeholder in addition to Internet users is the registrant itself. So I guess taking into consideration that there are two TLDs which are similar, and for some reason, perhaps because of not sufficient analysis, they are both delegated and

they're confusingly similar to each other, then there is a potential that registrant under one TLD, or one gTLD, somebody could potentially phish that site by registering the same domain name under a confusingly similar, basically TLD, gTLD. And this is obviously then applicable to all the domain names which can potentially be registered under one gTLD. If the gTLD is confusingly similar to another gTLD, then all those registrations under the first gTLD can potentially get open as a security risk to the other gTLD. So registrant is certainly another stakeholder in this risk assessment process, as well. Thank you.

ARIEL LIANG: Thanks for the input, Sarmad. Donna, please go ahead.

DONNA AUSTIN: Thanks, Ariel. Sarmad, phishing is a thing that happens on a pretty regular basis. And I think it's—How can I say this? It's something that happens now. So I'm just curious, from your perspective, do you think that this would become potentially more of a problem with IDN gTLDs if the TLD itself was confusingly similar to another TLD?

SARMAD HUSSAIN: Yes, I think the scale of it generally increases. Because currently, there are multiple ways this can be done, but if the phishing is done through creating a confusingly similar domain name, currently, what is done is that you have a TLD and then you try to figure out something similar at the second level under the same

TLD. So I think the phishing is largely focused on second-level registration under the same TLD.

Now If there is a similar gTLD, which is through some process delegated, then the space through which the phishing can actually be done, obviously, increases, because you can or you can not only do phishing under the same gTLD, you could actually go and try to figure out some, quote unquote, ingenious way of having a second level domain name which somehow looks the same, you could actually go to the other gTLD and register exactly the same name, where the TLD is confusingly similar, and the second-level domain is exactly the same.

And that way, people don't need to find, quote unquote, some ingenious way of writing the same thing, you could actually just register the same string. And so it becomes much more probable and also much easier to phish. Because initially, if you're trying to find a similar looking domain name at the second level, you may not find it. But in this other case, you can actually just use the same string. Thank you.

DONNA AUSTIN: Okay, thanks, Sarmad. So I suppose in the context of this exercise, I guess the question for us is what's the mitigation we need at the top level to reduce the potential for confusion by the user with the top level. So the string similarity review itself is one aspect of that. But the question is whether it has to be through the hybrid model to reduce that possibility or whether the option two with string confusion objection would have the same effectiveness in terms of mitigation. Thanks, Ariel, I think we can keep moving.

ARIEL LIANG: Okay, sounds good. And also another point I want to note is that the current exercise, we tried to make it as simple as feasible. So we're only looking at this risk from end user perspective. And we're analyzing the no connection and misconnection risks faced by end users. But if we want to enlarge the audience, to include registrant for example, then we can use a similar model to conduct that exercise. But maybe something to consider later. Not right now, because we do have some kind of an actual exercise we need to do during a call today. But okay, let me just keep going here.

DONNA AUSTIN: Before you do, sorry to interrupt. But I think it's important for us to keep in mind that what we're dealing with here is the top level, we're not getting into the second level, we still have some work to do on the domains at the second level. But in order to keep this pretty clean, let's just remember that what we're talking about here is confusion at the top level. Thanks.

ARIEL LIANG: Thanks, Donna. Good point. Okay, so this slide goes through the method, how to apply the assessment model to analyze the risks. So step one is we need to have a clear description of the risks. And also think of the consequences of the risks occurring. And as a reminder, we'll have two risks to provide a description, and also the consequences.

And then step two is we need to assess both the likelihood and severity of the risks occurring. And in the later part of the slide, you will see we will provide some numbers assigned to the level of likelihood and severity and then also some examples for you to consider when you try to designate the level or the likelihood and severity. So these examples could potentially be helpful, we hope, for you to assign the right number to indicate these level of likelihood and severity.

And then the third step is to assess the effectiveness of the mitigation measures. And again, we have two options on the table here. And then it's a very similar kind of exercise, you provide a number, designate a number for these two options to indicate the level of control effectiveness. And then the last step is you will see a matrix for the risk rating, basically remembering all the numbers you have assigned to these three factors and you pinpoint in the matrix or the grid, where the risk is at. And you will see we have some color coding and there are some parts as low, some part is high. But when we get to that slide, it will become much clearer.

So now we're at step one is to describe the risks and consequences. And then after going through these points, I will stop for a moment and see whether the group has general agreement on these descriptions and consequences. And then if not, what additional input you have here.

So the first risk, denial of service, and let's just call it no connection—these, you probably have already seen in other meetings, is basically we are using what the SSAC advice has already written in terms of the description, is basically a user attempts to visit website X and read it as being the same as the

website Y. For example, the user saw it on an advertisement on a bus. And then after typing website X, the connection does not work because it was not registered. So basically the user mistaken a web address as something else and typed something else, but then it didn't show up in his or her browser because it doesn't exist. So there's no connection being made.

And then the consequences of the risk. So SSAC advice already kind of alluded to this, basically user confusion and frustration. And then the user may conclude that the Internet does not work. But at the same time, it's mostly a nuisance, or an inconvenience, it's not some serious harm was caused, because nothing happened. It's basically a 404 page, nothing appeared. So it's just kind of annoying, but no harm.

But then if you do kind of generalize this experience to the broader Internet end user population, and if a lot of people are encountering this kind of cases, then they may have a loss of confidence in Internet, because it doesn't seem to work for them. So these may be the consequences for the first risk, no connection risk.

And then for the second risk, the description is that a user attempts to visit website X but read it as website Y on the bus, but then the user may receive email or something that contain the website Yes, but still in the user’s mind is website X. So the user clicked on it and then got directed to a website Y which is different from what the user expected. So in this case, a connection has been made. But the user got directed to a different website, which is different from what the user expected. So that's the basically what this connection is about.

And then in terms of consequences. We also noted this in some other meetings, it can be more problematic than no connection, because this kind of misconnection can result in the exploitation of a user confusion. So even the user arrives at a legitimate website, because it's different from what the user expected, it could result in credential compromise and accidental exposure of information. And if such a confusing similarity is maliciously leveraged, it can be a DNS abused vector.

And also as what Sarmad noted earlier, and also what Donna stressed, we're looking at this from a top level domain perspective. And if at the top level, this kind of confusing similarity has been maliciously leveraged, the possibility of DNS abuses could be much greater than at the second level. So if you generalize this individual experience to the broader Internet and user population, it could have the consequence that a lot of people lose confidence in the Internet and also have distrust issues with Internet if they encounter any abuse, for example.

So this is the first step for the exercise, is we described the risks and also provide some examples or explanation about the consequences of the risks. And I will stop here and see whether anybody have reaction to that. And I see Maxim has his hand up.

MAXIM ALZOBA: If you see the situation is that currently, in many advertisement, because people tend to make mistakes when typing in URLs, you can see the QR code, which has to be severely damaged not to extract the proper information from it. So it's a nice example. I'm not sure how long is going to be relevant. And actually, if a person

uses a mobile device, like phone or tablet, or whatsoever, they usually check if Internet works, why some applications and not necessarily typing in some advertisement will give the total feeling of everything is failed. I think it's a hypothetical example. But first of all, you need to find the user which behaves this way. Like typed in something and everything is not working. Because of that. Most probably people will think that oh, it's just lousy advertisement. Thanks.

ARIEL LIANG: Thanks. I think these are good points as the Internet is evolving and the way people accessing websites are evolving too using QR code or apps. So I think what you said may allude to the likelihoods part of the risks. If people don't need to type a domain name anymore, then the likelihood of these risks occurring may be lowered. But at the same time, when you see the risk two analysis, user may still encounter phishing kind of situation, may receive an email that contains a web address, for example. So the likelihood still could exist. But I see Satish has his hand up.

SATISH BABU: Thanks, Ariel. I agree that the first risk of no connection is a nuisance kind of situation. But the second risk, according to me, is very real, and has consequences. So we cannot dismiss the second kind of risk as trivial. It can actually have significant—it can erode trust. But the point is that it is only known later. When you click, nothing unusual happens, you get your site, but you're being phished and that realization only happens later. So the damage can be quite significant. Thank you.

ARIEL LIANG: Thank you, Satish. Well said. And I also saw Zuan Zhang has some comment about people using keywords searching for a web address instead of typing the address directly in a browser. So thanks all for the comment. Donna, please go ahead.

DONNA AUSTIN: Thanks, Ariel. And thanks for the comments, Satish and Maxim. It would be great if we had some—and we don't—data on the prevalence of what happens at the moment. With ASCII TLDs, I know there's not too many IDNs in use. But I just wonder if we think about the misconnection risks that we're talking about, how often does that happen with ASCII TLDs and whether we think it will be exponentially worse when we introduce IDN TLDs. And I guess the complication is IDN TLDs and variants. So that's where the challenge comes for the work that we're doing here. Maxim.

MAXIM ALZOBA: I think it's quite hard to find relevant examples because first of all, variants were prohibited from being used. And not many IDN TLDs use more than one script. So I'm not sure what are we going to find there. Thanks.

DONNA AUSTIN: Yeah. Understood. Thanks, Maxim. It was just kind of a reflection out loud on my part. So that's part of the challenge for us is, as has been the challenge for us all along, is that we don't know what we don't know. Okay, thanks, Ariel.

ARIEL LIANG: Yep. Thanks, Donna. Thanks, everybody. So I guess we can move on to the second step, is to assess the likelihood and severity of the two risks. So this current table you see is about the likelihood rating, and we have the rating from one to five, so minimum to maximum.

So we probably need to—we definitely need to assess the likelihoods for both the risks. So the goal here is, hopefully the group can agree on a number to pick for both risks in terms of likelihood. And I will just quickly go through the table here. And I will stop and see whether folks have thoughts on what number to pick.

So level one, minimum. So it means the risk almost never occurs. And then we try to provide some examples to supplement the description to help guide your thinking. So we're talking about misleading domain names at the top level. So for level one is a user almost never gets misled by domains. And then, also, if you look at this from a scale perspective, almost no user around the world gets misled by domains, and such incidences are rarely found anywhere in the world. So that's just some examples to try to supplement the description. Then I think we probably won't pick that up. Because we do know those cases exist.

And then for level two is likelihood for risk is low. So in the description, we say such risk occurs occasionally and in an isolated manner. And then to supplement that, from a frequency perspective, one example is that a user gets misled by domain

names only a couple of times in his or her lifetime. And then such incidents rarely repeat. It's basically a very isolated incident.

And then also from scale perspective, it will look at users around the world. For low perspective, it could mean that users only in certain demographics get misled by domain names, and such incidences are still very much scattered and isolated. So maybe we can explain it by saying for example, people get phished by certain domain names, but they're mostly isolated to really senior folks that have very little understanding or experience with Internet and only they get phished. That's something kind of we try to convey in this scale example to explain the level two, low.

And then for level three, medium, in our description, we say such risk occurs several times and in a considerable manner. To supplement that, as example, a user may get misled by domains more than a few times in his or her lifetime. And then the incidences sometimes repeat. So it's not really isolated incidents anymore. That definitely has a pattern, but still, it's not terribly bad. It's only a few times but it's still bad enough for a user to notice it.

And then from a scale perspective, for medium level, it could be that such incidences could happen among users across several demographics, and such incidents can happen many times. So it's not just isolated to specific population, but it could be a little bit more popular, more widespread than the level two low. So that's how we attempt to define medium.

And then for level four, high likelihood, so that means such risk occurs often and in extensive manner. And as example, we could say a user gets messed misled by domains many times and

incidences often repeat. So it's much more than a few times and it's probably much more noticeable, it happens many times.

And then also from a scale perspective, it's basically users around the world, such incidences could happen across a diverse demographics. And then it happens in large scale, so many more people are impacted by such risks.

And then for maximum, that's the most extreme level. So it means the risk occurs regularly and in a widespread manner. And then in terms of a frequency example, a user could get misled by domain name constantly. And incidents repeat regularly. So it's just become part of the life kind of thing for the user. And then from scale perspective, it could mean that users all around the world get misled by domain names regularly and the incidents are ubiquitous. So it's everywhere affecting everybody. So that's the maximum level. And it's probably not something we would select either. But this is just the way we try to describe the levels of likelihood. And hopefully, the examples are helpful to guide your thinking.

And now the task here is for the group to designate the level of likelihood for the no connection risk and the misconnection risk. Which number is appropriate based on your professional judgment? So I will stop here and see whether there's any comments, hand raised. Feel free to provide your guesstimates. Dennis, please go ahead.

DENNIS TAN: Thank you. Yeah, I think this is very useful. But I'm also thinking, this matrix or level of likelihood, I think it depends—I don't know, maybe I'm way ahead of where you're driving our [inaudible] to. This likelihood, whether it's minimal or going all the way to maximal depends on the gTLD itself. And of course, we don't know, for example, it's more likely that a TLD is more used for confusion purposes than other because of the size of it or the meaning of the TLD itself. For example, a bank, I'm using as an example, where maybe bank is more likely to be confused in parts than church. Of course, we don't know this prior the fact of the TLD being used, but I thought that was also another layer that contributes whether a TLD is more likelihood to be confused or not. Just some thoughts on that. Thank you.

ARIEL LIANG: Yeah, thanks, Dennis. Definitely differ from TLD to TLD, the it's probably going to be difficult to analyze it from that perspective. And this is basically a kind of generalized way we're analyzing it across board, but I'm happy to hear others' comments. Donna and Sarmad have their hand up.

DONNA AUSTIN: Thanks, Ariel. So Dennis, to your point, I understand your point. But if we can, just for the purpose of this exercise, just think about this from the perspective of new IDN gTLDs that will apply in the next gTLD round, and the consequences of that. I understand that people might get confused by .com or .co. And if there were serious concerns with either of those two TLDs, it could have serious consequences.

But I think we're looking at this very much from this is more or less a—what do you call it? A green something. we're on a level playing field for most of the new IDNs that will be coming on board. So if we can just think about it in that context, and not take it to what exists today. I think we just need to kind of contain this to the IDNs and their variants that we're trying to develop policy for. Sarmad.

SARMAD HUSSAIN: Thank you, Donna. I was actually thinking that another factor which can potentially also contribute to this discussion is that whether those two gTLDs, which are found confusing, or can potentially be confusing come from the same script or from different scripts. So if there are two gTLDs which are potentially confusing within Latin script, they can have more implications than, for example, two TLDs which are confusing, but one of them is coming from Latin script, and maybe the other one from let's say Cyrillic script or Armenian script. Because that may actually then also have implications because there may or may not be as much overlap under them for second level registrations. Just a thought. Thank you.

DONNA AUSTIN: Thanks, Sarmad. I need to think about that a little bit. But I think Ariel, are we good to move on?

ARIEL LIANG: I am hoping the group can give us a number to assign to the likelihood because to pinpoint where the risks are in the matrix, we

will need a number. So I just wonder whether there's any thoughts about what the likelihood level are for these two risks. And I see Dennis has his hand up.

DENNIS TAN: Yeah, thank you. That's the million-dollar question, I guess, what's the number? And I think Sarmad gave us a better example than I was trying to convey here. It depends. So if we are trying to determine a rating for likelihood for confusion overall, we can say if we are pointing to data of cybersecurity research, whether people are misled on domain names, yes, that happens every day, maybe hundreds of times a day. But is that the right way to look at it?

I think that's where the challenge lies. I'm not saying this is wrong, but it's just more complex than trying to put all the potential IDN gTLDs in the same bag and for lack of additional layers of that account these complex factors, we just put higher a bit, right, because that would be the collective likelihood of what we're trying to assess here. And maybe that's not the right way to look at it. This one, I think I'm just going in circles. But what I'm saying is putting a number here collectively to account for all confusions, that might lead us to the wrong conclusions. And I'm still processing my thoughts here. But that's my initial reaction.

DONNA AUSTIN: Dennis, if I may. I understand that this is a very difficult exercise for us to do, but perhaps if we can just try to constrain it to the purpose that we're doing this for. So this is about the string

similarity review. And what we're trying to assess here is given that we have variants for IDN gTLDs, and only some may be applied for along with the gTLD, do we need to factor in all the allocatable variants and the blocked variants? So does they have to be a visual string similarity review of all those strings?

And then what we're trying to do is more related to, if a lot of those strings look alike, then it would seem that perhaps we have more confusion that is going to come out of that if we don't try to mitigate it in some way. So does it make more sense to load the evaluation process at the front end? So we do accept the complexity with the evaluation and the potential cost to the applicant of being more thorough in that evaluation? Or do we think that it's reasonable that option two and the objection will give us a similar mitigation outcome?

So I know this is a lot to take in, and we will come back to it, but perhaps if we can try to constrain it to this is about the evaluation of the IDN gTLDs in an application process and what we're trying to mitigate against here is the confusion for the end user. So maybe if we can try to think about it in that context and not go too far beyond it.

But I do accept that what you're saying is that perhaps we could have come at this from another direction. But I guess what we're trying to understand here is misconnection seems to be—it's more likely for misconnection to be a problem than the no connection risk. So how do we factor that into the evaluation process? So I know this is really hard to wrap your head around. And James Caulfield, I know you're on the call, if you have any thoughts or

words of wisdom here to help us through it, that would be appreciated. So Maxim and then Sarmad.

MAXIM ALZOBA: I think we need to approach from some different perspective, because likelihood is probability. And to understand probability of something, you need some statistics, like how many occasions were and how many were successful or unsuccessful. Without it, it's going to be uneducated guess. And as far as I know, GNSO is about factual-based approach for policymaking. So if we, for example, say numbers now, it's going to be just wild guess without any ground. So I do not think we're able to say numbers now, to say which numbers we should assign here and there now, because we literally don't have data.

DONNA AUSTIN: Yeah, Maxim, I think the problem is that it's going to be difficult to get the data that we need. We do have some that was provided by Pitinan and Sarmad a few weeks ago, but it is going to be difficult for us to get data on this. So Sarmad, Ariel, and then James.

SARMAD HUSSAIN: Thank you, Donna. I'd like to make a couple of comments, two comments. First of all, I think one thing which though generally I guess I've been presenting arguments in the context of the conservative perspective, but I also wanted to highlight that since the previous round, another thing which has actually happened is that communities actually have looked at data and I guess reduced the string similarity confusion space by actually

identifying things which are obviously confusable as variants. So some of that confusion could have potentially reduced because some of those cases are now part of the variant sets and therefore already blocked off. So that's also something to consider in this analysis.

The second point which I wanted to, I guess, ask or clarify, is that in the second option, where we have level two comparisons plus string objection, I guess the question is—and please excuse me, if I'm not too clear on it—that can somebody, for example, in option two, or would somebody in option two be able to make a successful case based on blocked variants? Or could an argument be used against the objection saying that since string similarity review is only level two, which is focused only on allocatable variants, therefore, if somebody is raising an objection on a blocked variant case, then it becomes weaker? If that's the case, if the latter is the case, then of course, I think maybe we need to clarify that since we are trying to mitigate the blocked variant analysis for objection cases, those are still good options to consider. Thank you.

DONNA AUSTIN: Thanks, Sarmad. Steve, if I may, I'll have you respond to Sarmad's question about the objection. But I'll go to James first, and then we'll go to Ariel.

JAMES CAULFIELD: I just wanted to address the issue around the probabilities and—we didn't—I don't think we used the word probability. We used the

word likelihood. And I think Ariel laid it out very well at the beginning, where she said that it's really a matter of—there isn't good data, much of what we do in risk management around the Internet is subjective. But that doesn't mean it's not without good inputs. And she referred to it as professional judgment.

So while you can't necessarily get your hard statistics, and it's actually one of the things we warn about, is you if we assign a number like one through five, it makes it sound very scientific or numeric. But in fact, it's really more around the description. So in this case, the policy team has developed the description with some examples. So rather than saying it's a 50% chance, or 75.2% chance, it's, here's kind of what we describe those probabilities at, and it's then using judgment. And it's a group of smart people who are very familiar with the Internet and can make those kinds of judgments. And are there some leaps, perhaps, because there isn't the hard data, which would always be better? But we all very often make decisions with imperfect or information with a lot of ambiguity. So I think it's really a matter of kind of looking at the descriptions and what feels right, or what is kind of sensible. And I'll just stop there.

DONNA AUSTIN: Thanks, James. Ariel.

ARIEL LIANG: Thanks, James. And he said what I intended to say much better. And I just sensed a little bit of—I don't know whether fear is the word, maybe reservation from the group to provide a number. But

I am encouraging folks to take a leap of faith and just pick a number because it may not be as bad as you thought, because you have to look at that together with severity, which is the next slide I will go through and then when we put in the matrix, it isn't really going to be as bad as you thought. So I'm really hoping folks can take a leap of faith based on your professional judgment.

And then another point I want to emphasize is that this is our multiple calls about string similarity. And we do have a hard deadline or goal to publish an initial report. So gathering hard data to do this exercise is definitely going to take time and then I'm not sure we can keep punting the question and then not make a call in some way.

As you know, the initial report includes preliminary recommendations, it's not final. We still have the opportunity for the broader community to provide input. So I'd just try to encourage folks to do this exercise as much as you feel comfortable and at least we can see how it may look like in the matrix. And then if we need to go back to this and think a bit more, it's definitely feasible, but we just don't have a lot of time. So that's just something I want you to note.

DONNA AUSTIN: Yeah, thanks, Ariel. I think let's look at this, this is about likelihood. Ariel will take us through severity. Perhaps what we should have done was done and run through the whole slides and then come back to this point by point. And it is a bit of a leap of faith here to give a best guess. But I also appreciated the way that we have presented this may not—maybe we could have done it differently.

But as a first pass, I think this is a reasonable way for us to think about this.

The other thing is that we may, in the initial report, if we still have differences of opinion among the team about what's the best approach for string similarity, is that we could seek specific feedback from the community on this string similarity in particular.

And the other thing that I'm mindful of as well is that we did ask Steve and Ariel to talk to Karen's team about the input that they provided, which said that the hybrid model will increase complexities and cost. So we did ask them, what does that mean? Do you have more information that you can base that on?

And really, there isn't much underlying that, except for the fact that the numbers will be more that need to be reviewed. And if there's more numbers to be reviewed, then they may need more people to do that string similarity review, because it is a manual process. And I think we spoke about that a couple of weeks ago, is that this is a manual process. And that's why it becomes complex. And obviously, with allocatable and blocked variants, if you have both of those that are being considered in the review, then that's where the extra numbers come in.

So I think we have a lot of the information. We don't have absolute data. But we do know a fair amount about what we're discussing here. So I think let's just take a stab at it and see where we get. Steve.

STEVE CHAN: Thanks, Donna. You asked me to try to provide a bit of a response regarding objections to Sarmad's comment, and I'll try to do that. So I guess the way I'd respond is that objections are based on a set of criteria. And so if this group is to determine that the scope for allowable objections is to be the hybrid, presumably the panel that is performing objections, they shouldn't be influenced by other elements unless they're explicitly told her to keep that in mind.

So if this group were to take into account the string similarity evaluations when performing the objection review, then they would do so. But otherwise, the outcome of the string similarity shouldn't be a negative influence on the outcome of an objection, unless that's part of the criteria. And presumably, that is not what this group is saying. So that's my attempt at providing an answer. And while I have the mic, I would actually just say that for this exercise, recognizing that there's a lack of data, I'd also note that the solution that is at least preliminarily on the table, I think it's safe to say it's near the higher end of the mitigation strategy. There is also a level three above it, but the hybrid model is just under that.

So that assessment of this group to lean towards that potential solution, it's also made without the presence of specific data. So I guess another way to look at it is what was relied upon to get to that assessment that that is seemingly the appropriate solution. So presumably, it was professional judgment of this group. So the idea for this exercise is, given what this group knows and their professional knowledge of the situation, which I think what Donna said is quite right, it's not nothing, this group definitely understands

the topic, at least decently well enough, and well enough to get to an assessment that the hybrid model seems to make sense.

This exercise is really just to help make sure that the risk being mitigated, there's a common understanding of it. And like was said repeatedly, I think it's not scientific, but this group definitely has professional judgment to help inform its decision making.

So I guess I would just echo Ariel's comment. Maybe it's good to just take a leap of faith and talk it out. I think James would agree that a lot of the risk assessments, it's sort of crowd sourced. As people talk about it, there is often just a coalescing around a number, and it helps talk it through just to see where people end up on the numbers. Thanks.

DONNA AUSTIN: Thanks, Steve. So we'll go to Maxim. And then I think what we'll do, Ariel, is we'll go through the severity slide, and then maybe we can look at the table and whether the two axes meet and see how people feel about it. But I do appreciate that this is a lot of information to take into account. And I think we did recognize that risk assessment is a tool for us. It's not an absolute. It's just to enable us to have a discussion about whether we think the conservative approach, which would be the hybrid model, is the right way to go, or from a policy perspective, is a good recommendation, or would the hybrid model plus the objection actually serve the same purpose? So that's what we're trying to get to. So Maxim, and then we'll move on with Ariel.

MAXIM ALZOBA: I think here, we shouldn't use this approach, because it's like writing, “We believe,” instead of facts, which somehow grouped and related. Because in some letters of [SSAC,] for example, “We believe” replaced basis for some evaluations of numbers. And I'm not sure we need to do this. We may use it as example. Like some people say that the probability is like this, but it's not necessarily this way. But giving numbers now, it's just like tossing a coin. We shouldn't do this. Because what are we g an write in the report? We just guessed some numbers and because of that, you have to change policy this way? I'm not sure it's just factually based approach. Thanks.

DONNA AUSTIN: Thanks, Maxim. And I think whatever goes in the report is going to be based on our analysis and consideration of the question. And the string similarity review, there's been a lot of work done on that. And this is just the last piece of that work. So we don't have hard data. And as Steve said, the string similarity small group when they did their work, they didn't really have hard data to deal with. And that's why some of this is a challenge for us.

But I think in the report, it's not going to be a belief or whatever, it's going to be a recommendation based on our analysis and consideration of the charter question that we had in front of us. And what we're doing now is just an extra part of that analysis and consideration. And again, this is just a tool to help our thinking about whether the hybrid model is too conservative, or it's the right approach given that variants haven't been used before. So let's try to keep that in mind. So Ariel, let's keep rolling.

ARIEL LIANG: Yep. Thanks, Donna. And in the interest of time, I will try to go through the rest of the slides. So you can at least see the model in its full picture. And I just want you to note that we were requested by the team members to do this exercise. That's why we're doing this right now. And then this is the model that James taught us in ICANN 75 and that's the only tool we have at this point. And if you have better suggestions for approaches we can use for assessing risk, we're definitely open to input and suggestions. But we're doing it because we were asked to do it. So that's just something I want to quickly note.

So in terms of the severity rating, it's very similar to what you saw earlier for likelihood from level one to level five. So that's assessing the severity of the two risks. So for level one, our description is that it's minimum, the meaning that when the user encountered that risk, they may encounter some negligible inconveniences. So we're talking about misleading domains at the top level. And based on the consequences we said earlier, it could result in credential compromises, or accidental exposure of information.

So when we tried to supplement this description, we thought of some examples to showcase the consequences. So for example, for privacy perspective, if it's level one, at a minimum, it may be that a user got to a website and then it has a potential in revealing the user's personal identifying information because it could have for example a pop up window for the user to click and type the birthday, for example. But the user may elect not to do that at all and quickly detect that, so no harm was caused. But it still has the

potential to cause breach in the user's privacy. So that's one example where thought of.

And then another example, it's a typical kind of category we need to analyze in terms of risk, is the financial consequences or financial severity, financial harm severity. So at the minimum level, it may also have the potential in revealing, for example, the user's banking or financial information. So that's some of the example we thought could try to help explain what minimum means in severity level.

And then for the one level up, level two, it's a low severity. So that means the user may encounter few inconveniences, which may be overcome without any problem. So to supplement that from a privacy perspective, for example, a user got to a misleading website and then it leaked the user's email address and phone number and then as a result, the user started receiving spam and phishing messages. So that's kind of a privacy breach. But still, it's not terribly harmful yet, but definitely caused harm to the user. So we thought this may be appropriate to explain what low means here.

And then in terms of the financial perspective, it could be that the user went to a misleading website and got tricked to purchase unwanted goods or services, or even fraud, or counterfeit goods, for example. So it didn't escalate to the point the user, for example, lose control of his or her bank account, but the user got click baited and bought something the user doesn't want. So that could be an example to explain what low means here.

And then for the medium level, it means that a user may encounter significant inconveniences, which may be overcome despite a few difficulties. So it's a little bit worse than level two now. So as an example, to show what it means, a user's online credentials can be leaked because they clicked on a phishing website. So then the bad actor got access to the user's email accounts and got control of the user's social media accounts. And then that may also result in reputational damage because the bad actor may impersonate the user on Facebook, for example, to try to phish other people. So that could be a medium level of the privacy breached. And then from perspective of finance, it could be that the user got tricked and provided his or her debit card, credit card information on the malicious website. And then also, some people use that information—

UNIDENTIFIED PARTICIPANT: [inaudible]

ARIEL LIANG: Sorry, I'm hearing some noises. Okay, thank you. So yeah, for these financial consequences, these are maybe at the medium level, because it seems much more harmful, and some real damage was done. But still, you could, for example, cancel your credit card, and then recover your lost funds by talking with your bank, and then maybe freeze your social media account or freeze your email account to control the damage. So still be overcome, despite a few difficulties.

And for level four, the high severity, our description is a user may encounter significant consequences which may be overcome albeit with serious difficulty difficulties. So this is much worse than medium level. And then some examples from privacy breach perspective is that there's theft of your bank account information or theft of your biometric ID, and then so some of your critical personal data were stolen. And that's definitely much worse than just stealing your credit card number, because now your bank account is being stolen, that's much worse. And then that could result in some financial consequences such as misappropriation of funds. And then also your property got damaged, for example, and then even could cause a loss of employment. For example, if your credit got really bad or you got into some financial trouble that your employer was flagged, and then it could have that kind of consequences too.

It's just some examples we think of, trying to explain what high severity means here. And then for the maximum level of severity, that means the user encounter significant or even irreversible consequences which may not be overcome. So that means from privacy perspective, it could be that your social security number got stolen, and your key personal data got stolen. So some people can just open up a whole bank account or get into a loan situation using your identity. And that's much worse than just getting a hold of one of your bank account information. That's much worse.

And then for a financial perspective, it could mean that you're bankrupt as a result of this breach. And then you got into life ruining debt or you lost your property, lost your house, for

example. So that's much worse than just getting your bank account information stolen.

So that's some examples. We try to complement the description and help folks think through it. And I know this is not a perfect exercise, and a lot of it is based on your professional judgment. But we hope that at least gets folks thinking and can try to assign a number by taking a leap of faith.

But I think I want to quickly go through the rest of the slideshow, at least you get to see the matrix and then get a whole picture of this risk assessment matrix, how it looks like. [Staff's theory,] as noted earlier, we also want to assess the control effectiveness of the mitigation measures. So we have two options at hand.

One is the hybrid model for string similarity review, to mitigate any confusing similarity among top-level domain names. So that's option one. And option two is that we use level two for string similarity review. So that means only taking into account the applied for a string plus all allocatable variants. And then combined with the string confusion objection, which can use the hybrid model to detect confusing similarity among strings that may not be caught by the string similarity review panel.

So that's the two options we have. And we hope the group can also assign numbers to try to assess their effectiveness. So it's also level from one to five from minimum to maximum. And I won't go through everything here. So minimum means effectively no mitigation in place. So basically, no effect. And maximum means mitigation measure is considered fully effective, was near negligible chance of control failure. Meaning if we use one of the

two options, basically, there is no confusing similarity ever existing on the Internet anymore, which I don't think is the case for our current situation, it's probably something in between. So you see two through four, these are these are the level in-between.

And then lastly, I just want to show everybody the matrix table. So once you assign the number, in accordance with the likelihood and severity, we can move this little circle here. So risk one is the inherent risk. And risk two is the inherent risk for misconnection. So we can try to pinpoint where the risks will be in this table. So if you say, for no connection, the likelihood is three but the severity is one for example, then basically, we'll move this first square to low here, and then for like misconnection, we say the likelihood is three but severity is also three, you will see this little round button will be moved to the middle of the script.

So that's why I was trying to say it may not be as bad as you thought. So you have to take into account both severity and likelihood. And another, a little bit more complicated thing is, if you factor in the control effectiveness of the mitigation measures, the risk level will move. So if you say option one, the hybrid model, then mitigation measure is high, means most of the string similarity or the string confusion risks will be eliminated as a result of the hybrid model, then basically, the likelihoods of these two risks occurring should be lowered, and then the buttons will move towards the green part of this grid as a result. So that's why I want the group to take a leap of faith and pick a number so that we can see how it may be reflected in this table. And I will stop here. This is the full picture of this model.

DONNA AUSTIN: Thanks, Ariel, and thanks for the work that you've done on this. So I'll go to Dennis first, and then I'll come back and do a wrap. Dennis.

DENNIS TAN: Thank you, Donna. Can we go back? I think it was one slide. A couple of slides, the severity ratings. Yeah, thank you. So I think we're starting to develop the building blocks for our thought process. So I appreciate this. I would like us to consider some other factors here. I see this table—sorry, is this likelihood or severity?

ARIEL LIANG: Sorry, this is severity. If you look at the top here, it's the severity rating.

DENNIS TAN: Thank you. And I appreciate this is a first pass, but I think what I read here when talking about okay, what's the severity, the range, the spectrum of things that we can find or we the range of possibilities in terms of consequences of a misconnection or denial service.

So the first thing, I think, on no connection or denial of service, these examples do not convey that because in terms of no connection, maybe the examples are not focused on that. But on the misconnection side, I think we are leaning towards the most severe consequences of it even in the most minimal severity rating on one. And I would argue that if I have a severity of one,

nothing happens. Because again, I think we are [inaudible] too much to malicious use of domain names and I can tell you that the vast majority of domain names are used in a good faith manner. And we can for example use the domain activity abuse report in order to support that data point. Less than half a percent of domain names are used in security threats nowadays. The latest November report points to that.

So we're leaning too much on the severe possibilities. But in terms of misconnection, if a user goes to the site that they intended to go to one site but arrived to another one, nothing could happen, right? I mean, just, oh, I arrived to the wrong site, clearly is different than what I expected to do. I check my source again, yes, I made a mistake. And I go to another site. And that's possible. And I would argue that's the most common thing that happens in terms of misconnection.

And yes, I agree, a very severe thing can happen if a domain name is used for malicious intent. Then yes, leaking information, phishing, banking, user password, you name it, all of the things in the severe, most severe extreme range. So again, I think we need—or at least my thinking is that if we're going through this exercise, list the range of possibilities, from the most benign to the most severe, and assign those examples or range of, again, possibilities in the right—rearrange these in different boxes, accounting for the possibility of nothing happens. Because again, I would argue that that's the most likely outcome when we look at the aggregate numbers of security threats. And that's it. Thank you.

DONNA AUSTIN: So Dennis, if I understand you correctly, what we've developed here is probably something that is appropriate, if you consider Sarmad's earlier example about the possibility of phishing. So that's a different mechanism, right? So that's not somebody on the Internet is trying to go to a website. There's no real harm done with that, because it's, the user that is in control of that. But Sarmad's example, I suppose, about the registrant who registered the second-level domain, or somebody who just is unfortunate enough to get a phishing email, which happens now a lot, then there's differences in how we should kind of slice and dice this.

DENNIS TAN: Yeah, maybe I didn't fully understand. So in the context of variants, where the SSAC 060 focus on, variant sets, not outside variants as we are using, the misconnection and denial of service, we are taking that out of context from SSAC 060. Because SSAC 60 focuses on variants, failure modes on the variant sets.

And one way to minimize it is to assign, allocate the different variant labels to the same entity basically. And that way, there's only one registrant and one sponsoring registrar likely to manage all the sets and potentially manage the user experience as well. So that way you minimize those risks. But we're taking that outside to talking about in the context of the string similarity, processes and evaluations and string objection and whatnot. And that's where we're building this framework to understand the likelihood and severity. And all I'm saying here is reacting to this table that I see, and we are leaning too much on the wrong uses of domain names and clearly malicious actors trying to use this domain name, but we are neglecting to look at the other side of

the range which is the vast majority of domain names are used in good faith.

DONNA AUSTIN: Okay. Thanks, Dennis. Justine.

JUSTINE CHEW: Just very quickly to Dennis's point, I think the way I see it is my understanding of risk is always, in terms of mathematical or formulaic, is that risk equals likelihood times severity. Right? So if you look at both sides of the coin of what Dennis was talking about, if you just look at likelihood, likelihood is the likelihood that something would happen. So if you think that something is not likely to happen, then obviously, the harm may be minimal. But if you think that the likelihood of something happening is high, and the severity or the harm caused is low, then the outcome of the risk still could be could be low, and it could be still acceptable. But if you think that something is not likely to happen, but when it happens, it causes severe harm, meaning severity is high, then your risk ends up being high. So I think it boils down to what Dennis was talking about, but you've got to look at it from four different angles, kind of thing. I hope that makes sense. Thanks.

DONNA AUSTIN: Thanks, Justine. And thanks, everyone, for sticking around the extra few minutes. And I appreciate this has been difficult to walk through. But hopefully, folks can see the applicability to the problem we're trying to solve, and that is, what is the right option

for string similarity review? Is that the hybrid model? Or is it the option two with the objection?

So we will come back to this in the new year. Maybe we could have done a better job of targeting some of the examples that we had to the problem we're trying to solve, but I think just as a theoretical exercise to try to wrap our heads around these things, it was helpful. And I do really thank Ariel for the work that she's put in this with guidance for James as well. So we're giving you some stuff to think about during the break. I believe we're back on the 6th of January. Is that right, Devan?

DEVAN REED: It is going to be Thursday the 5th.

DONNA AUSTIN: Okay. So we will see you back here on the 5th of January. We will be starting half an hour earlier. Just to accommodate my move back to Australia. So with that, thanks, everybody. And again, thanks for the work during the year. And just a special call out to Emily, Steve, Ariel and Devan for the work that they do in supporting us every week. So thanks very much for that. I think we can end the recording there, Devan.

DEVAN REED: Perfect. Thank you all so much for joining. Have a happy holiday break.

[END OF TRANSCRIPTION]