DRAFT

Conference Debate Session III:

Business continuity in the face of current and future challenges

Introduced and Chaired by Paul Hughes, Research Director,

Future of Connectedness, IDC

Featured Speakers:

Analyst chair: Paul Hughes, Research Director, Future of Connectedness, IDC
Hugo Vliegen, Senior Vice President of Product Management, Aryaka Networks
Prakash Mana, Chief Executive Officer, Cloudbrink
Srinivas Rao, AVP & Solution Specialist, Tata Communications
Ken Levine, Chief Executive Officer, Xcitium

Paul Hughes, Research Director, Future of Connectedness, IDC
Great, well, looking forward to this panel discussion, I'd like to discuss a little bit about my role at IDC. I'm an analyst at IDC that focuses specifically on enterprise research. My role is as director of future connectedness, I look very closely at the impact of enterprise connectivity on the enterprise itself. So I spend a lot of my time looking and spending time interviewing enterprises, as well as doing a lot of survey based research. So I'm actually very glad to be here with the esteemed panel to talk about business continuity, and the challenge in the face of current and future challenges. And what I'll do is I'll kick off by some sharing some of some of our some of our framework for the impact of what the future of connecting means for business continuity and resiliency and also then show you some of our recent data from some several surveys that we've done. And then we'll jump into the panel discussion. So you're going to see some common themes that we've been talking about with a lot of the other presentations earlier today. And as we've seen now we're entering in this post pandemic era, we've seen the role of how enterprises have gone through this path of digital transformation in the folk and their focus on adapting to change, dealing with the impact of the hybrid workforce and changing a lot of those internal and critical policies and procedures that help them adapt to that change. Obviously, now as we look towards the next year, over the next year, the winds of change are moving now into what we're calling the storms of disruption, as we see the impact of all kinds of new influences that are impacting the way businesses are able to operate. So we think about skills gaps, we think about the impact of the of the global instability, potentially threatening business continuity, you think about the supply chain constraints, which are hurting certain

organizations as they try and start trying to stay operationally efficient. And that leads to the overall vision that we have for the enterprise as they try and address a lot of these issues around business continuity and reliability. We built what we call the future connectedness framework, which looks at four key principles that are required by an organization to really help address a lot of those issues around staying connected, staying efficient and staying agile. One of the critical areas that we focus on is the impact on business continuity and how organizations need to be thinking about the way that they address networks, applications, the role of the cloud, the role of productivity and collaboration, as a way to bring to maintain & help to maintain, make sure that the organization can stay resilient no matter what the situation can be. This aligns with the requirements that we see as it relates to the impact on digital experiences, the way it relates to the impact on X on secure access to the network and allowing the organizations to stay productive and agile, regardless of the situation that they're in and no matter what kind of impact they may see coming from outside influences or business change or market changes. So, in just setting the stage for where we are in terms of this path towards business continuity and resiliency and reliability what we find is that over half of enterprises today are still in this mid stage in terms of building out a strong strategy around resiliency and business continuity. A lot of this gets tied specifically to the way that they think about their core connectivity strategy and the way that they connect, the way that they're connecting systems, applications and people and processes together, whether it be on site on premise, or whether it be working with applications that reside in the cloud, resolving a lot of these critical issues, I think becomes one of the main challenges for organizations that I think we'll be talking about on the panel today. And it's something that as we think about the impact of everything from security to changing, and business models and the impact on the customer, the partner and the employees, we organizations are clearly trying to address this in the most effective way they can. But what we are finding is that even in the wake of all of these challenges that we see coming from the impact of inflation supply chain, and so forth, the prioritization that's comes that enterprises have around connectivity and digital infrastructure transformation remains remarkably strong. I think you can see from the data on the date on the slide, that over almost 80% of organizations are still prioritizing connectivity and digital infrastructure transformation programs as a way to continue to down that path of ensuring that business continuity and resiliency remains a critical remains a priority for the business going forward. Similarly, when we look specifically at the digital infrastructure perspective, what we also see is that organizations are very much prioritizing this focus on trying to bring greater levels of seamless integration and process to the way that they manage their digital infrastructure. So as you can see, you've got almost 65% of organizations worldwide, they're looking at ways to rationalize and manage a lot of the impact of the way that they look at the rollout of not just managing their internal infrastructure, but how they push a lot of this critical infrastructure to the cloud. All of this becomes part of a core strategy that will help them drive a greater sense of business continuity and resiliency across everything that they do.

I'll close out with the visionary slide of where organizations are looking to get and I think this will be a key point for a lot of the discussion on the panel. And that is as organizations are looking at what are some of the critical business outcomes that they're looking to achieve over the next year. So not surprisingly, you can see that the top priority for organizations is adopting a cloud first approach. And that is, when you consider the impact of moving a lot of these critical applications and systems to the cloud, you help to mitigate a lot of the risk that comes from having you know, centralized or siloed applications siloed data that sits within the organization. And this all contributes to the ability to ensure that the business can stay connected. And business continuity becomes a critical priority going forward. So with that I'm going to open it up to the panel. So, Prakash, I'll start with you.

Prakash Mana, Chief Executive Officer, Cloudbrink
Yes. Thank you so much. Prakash Mana, Co Founder and CEO of Cloudbrink, as I shared before Cloudbrink delivers secure in office experience to the modern hybrid workforce anywhere. So obviously, in this post COVID, the new normal, whatever we want to call it. When we talk about business continuity, how do we deliver the same level of experience productivity for our employees when they are inside the office and when they are working from anywhere becomes critical? So that's where Cloudbrink plays a critical role. You can think of Cloudbrink as a personal SDWAN, or a high performance zero trust ZTE and a kind of solution.

Ken Levine, Chief Executive Officer, Xcitium
I'm Ken Levine, CEO of Xcitium. I've been in and around cybersecurity now 15 ish years or so. Xcitium is in cyber, we are an endpoint security company. And I think endpoint security with a twist, I should say. And I think where we're kind of all cyber has to figure out how to play with business continuity is how do we straddle the line between great security and not impacting productivity? And I think that's the challenge that CISOs have, I think it's a challenge that that vendors have. Because there is one solution to great security, it would just destroy the entire global business, that would be just disconnect. So you can't do that. So the question is how do you get the best the best security you can and we focus just quickly on Xcitium, we focus on the on the notion of the malware is already there.

Sorry, I just gonna just finish and saying that our unique approach to it is we assume the malware is in what our job is, is to prevent it from doing any damage. And that's the way we're trying to trying to work through the continuity.

Srinivas Rao, AVP & Solution Specialist, Tata Communications
Hi, Srini from Tata Communications. So I spent about three decades with this company, particularly whatever we have seen during the COVID disruption, we also had to start a lot of digital transformation as a company for ourselves before we serve our customers, right? So therefore, there is a huge gate of digital transformation that we adopted internally in our own organization, in enabling a lot of digital ecosystem solutions for the customers that is revolving around UCC cloud security. And obviously the network's the largest share of what we do today in the market, so happy to be on this panel.

Hugo Vliegen, Senior Vice President of Product Management, Aryaka Networks
Hello, I'm Hugo Vliegen. For Aryaka. I run product management. Aryaka is basically providing a cloud delivered service for connecting enterprises. So if you talk about the enterprise when connecting your users to the enterprise network, your sites, your any clouds whether a SASE is that is where Aryaka does, and we build it from the ground up because the interesting thing before Aryaka there was no cloud for delivering enterprise where networking, right, you buy a box, you go somewhere they integrate it. And one of the challenges is which we will resolve is that wherever you work, wherever you are, you have this resilient performance, the high performance the same policy. So you talked about siloed data, silo application, I'm still shocked that a lot of the implementations on this planet silent networking, siloed security, siloed for the workers, silent for on prem, silent for different siloed for different clouds, and that is not supported for resilient and business continuity.

Paul Hughes, Research Director, Future of Connectedness, IDC
I think you've almost answered my first question. And that is where does the panel think the biggest shortcoming is, and I think as it relates to building much more out a business continuity strategy. I know a

lot of the research that we see, not surprisingly, security always ranks number one in terms of a top challenge. But you also consider the fact that you think about the impact of, as you said, data silos, service silos becoming a challenge. But as you look and talk to your enterprise customers, is that showing up as the primary shortcoming today?

Hugo Vliegen, Senior Vice President of Product Management, Aryaka Networks
Yeah, yeah, totally. I mean, if we talk about if things go wrong, the CIO gets fired, right? It's literally what it is. And they are struggling with the complexities all the systems which make things very brittle, tight? Because if things go wrong, yes, you can have a nice procedure book. But now you need to do it. Right now you need to change policies people have to make we have to work somewhere else, and how do you adapt to it? And then if you don't have from the ground up systems, which are built for integration, not only technologies, but as people and workflows, right, who do you call and who solves those problems for you so that if somebody's challenges, the legacy, you cannot call anybody, and it's very brittle because of the underlying infrastructure, which is siloed.

Srinivas Rao, AVP & Solution Specialist, Tata Communications
Yeah, I think like you said, you can change policies, you can set up new direction for your technology, etc. But I think end of the day, we also have to bring in the customer experience as the top priority, right. Second is the employee experience, I think these two things are paramount important, because it is you know, there is a disruption, I just cannot say that I can serve my customers, what if you know your networks are performing because there is a disruption and you're not able to take your customer calls, you are not able to do your trading what you normally do. So therefore, that actually heals that network, whatever becomes red, that is something that we should avoid despite having a disruption. That's number one. Number two is your employees as collaborative as they are? Otherwise, this something that we need to ensure that is equally important. So therefore, I think there's two things, customer experience and employee experience is something that we need to cater to.

Ken Levine, Chief Executive Officer, Xcitium
I would just add that the policies really do become critical, because it does also impact the user experience or the employee experience. And so your policies can't be too restricting yet. So there really is a middle ground, I think that has to be reached, we are one of an ecosystem of dozens of products that are typically found on a network. So, how do you leverage all of the different technologies better when the company in the users want you to be easy? And the security team wants you to be secure? And so yeah, I think it's a challenge that everybody has in enterprises of all sizes. Now integrate.

Prakash Mana, Chief Executive Officer, Cloudbrink
Paul, let me take a slightly different angle. When we talk about some of the shortcomings associated with business continuity plan, when we're having conversations with global CIOs, there is one thing that comes up over and over everybody in some way, shape or form, we'll talk about this notion that we're living through a once in a generational change in terms of where when how we work is fundamentally changing. So if we all understand that this notion of person working from anywhere, if we thought that was a business continuity plan, then we're now living on that plan in perpetuity, we've got business continuity going on in perpetuity. So that's the single most important shortcoming at least what we hear is, CIOs will say that when an end user, people like you and I, when we go to office, it practitioners have invested north of $35 billion in building a stack that is consisted of three things. The first one is connectivity, making sure when we go to office, everything is lightning fast. We can access any application, anything, it can be

MPLS, network or anything. The second one is, once you have the internet connection, you spread that internet connection across different users some kind of a role based access control marketing, people can only do marketing job. In engineering, people can only access engineering stuff. And then the third thing is obviously they've spent incredible amount of investment in building perimeter around this office space, so that everything that you do is secure. So connectivity, access security, this stack that they have built for last several decades, invest in norther $35 billion, is only in use three days a week, when people are inside the office, two days a week when they are working from home, they're on their own. Right. So that's a shortcoming. We hear over and over and over in terms of how do I replicate this entire stack and somehow left shift it to my users so that no matter where they are, they get that in office connectivity, access and security.

Paul Hughes, Research Director, Future of Connectedness, IDC
Yeah. And you bring up a great point, because I think about this, as most organizations now are in this sort of, I'll call it a return to Office approach, but they are looking at all of the critical aspects of the way that their employees are connecting to, to secure systems, the way that partners can come in with using CTA to ensure that there's no they're not encroaching on data that they shouldn't encroach on. But you also think about this, we're seeing this migration towards obviously software defined networks, the move towards, you know, away from some, I'm going to say complementing, where SDWAN is complementing MPLS. But giving that giving greater sense of scale, greater sense of flexibility, which becomes something that is a big part of driving business continuity. So as you sort as we sort of see this kind of emerging, you know, I think about the impact of network connectivity, the data, the infrastructure, you know, as we start thinking about kind of the setting priorities moving forward, security is always going to be number one. But we think about sort of flexibility and scale as well. So I'd love to get your feedback on that as we think about kind of those priorities. And as you're working with a lot of your customers that are looking at this move towards, you know, virtual virtualized networks and the way that that can bring greater flexibility and build a stronger business continuity framework as well.

Prakash Mana, Chief Executive Officer, Cloudbrink
That's right. I could not agree more with you on that point. In fact, somebody was giving a parallel example and they said as we look into this new paradigm, of course, security is top I already, but somewhere along the way, we miss why we stand for, as Ken mentioned, there is a perfect solution to securing everything destroy everything, right? So we talk about this notion of digital equality, right? If we look at the parallel example, we hear so much right? When we all went into the pandemic, every there was just so much focus around masking, isolation, all of that. And we overlook the whole host of problems that we are now seeing around mental health, stuff like that. So similarly, when we look at the digital aspect of our world, I think security is important, but we cannot over look, the user experience, part of security stands there to make sure people get the level of interaction that they need with the application. So driving that and user experience as Shalini, you mentioned as well, is of critical importance here.

Hugo Vliegen, Senior Vice President of Product Management, Aryaka Networks
Yeah, so you use the word MPLS. Right. So I think if you still using MPLS, which was invented in the long line time ago, in the Dark Ages, when everybody worked in the office, right. So if you have MPLS, you will not have the agility and you will not have the performance for the user at home. Now, what HIPAA happens with as the LAN, right, is that as the UN, as what is the older in traditional as UN as the implementation, they said, Okay, use more internet because the internet is becoming great. But still you need some MPLS. If you need high performance, that model is over. So the Aryaka approach is that we have built a private core

where we basically can provide an application performance, which is equivalent of better than MPLS. Right, we can talk about the technology of that. But what is very important, all that hair pinning that in flexibility is gone. The other thing is as well, you can deliver the same performance and agility, whether you are in the office, which is the traditional world where people live, or people can live everywhere at home, because you need not second class citizens, right in terms of if you're at home, you need to same experience. And the other point is that with these traditional models, that if you connect to the cloud, they maybe have one aggregation point or two aggregation point, but that's the wrong model, you need to have a cloud delivered service where you can have endless numbers of aggregation points, because if a disaster strikes, you may have one or two you may have a failover, but that aggregation point is gone. And these are very complex. So aggregation delivered as a service is another aspect, from our point of view is people really need to be resilient and get rid of MPLS. Because that is a that is an old model if you want to have flexible and business continuity. So from that point of view.

Srinivas Rao, AVP & Solution Specialist, Tata Communications
Yeah, I think that's a good point to what you mentioned, replace MPLS maybe for cost saving, maybe because now we have got SDWAN, which can really get you know, multiple internet working together. But then the biggest challenge today is that do I have an intranet which can really perform like MPLS not compromising an SLA is not performed, you know, not compromising on the performance as well right. So therefore, I think that is one part which we need to address. The second part and most important part if you asked me is that IT managers always felt there is a shadow it because they don't know what sort of it they're bringing in, somebody does get some obligation and all that I was talking to one of the CIOs. He said, Okay, my banking guy, he just got one FinTech application, because that application works well for him for his business. But the problem is that, while that is a SaaS application, they really don't know what sort of consumption that is happening on what sort of users are actually accessing on that. So, therefore, that means there is something like a shadow it now had become shadow network as well. So therefore, you lost the visibility in the world scheme of things. Therefore, what is most important is that get your internet fit for business, get your visibility right across whether it is MPLS or internet or even you have to use some the private 5g or whatever, but you should have a single pane of view into your network

Paul Hughes, Research Director, Future of Connectedness, IDC
Yeah, yeah. That makes a lot of sense. We'd love to hear from you guys as well as we talk about this move towards driving business continuity into the enterprise, would love to get some customer examples or use cases that really stand out where there have been some specific successes that have addressed either, eliminating those data silos or addressing security concerns or that have really helped to bring that bring In that enterprise level up to kind of that truly a much more robust level of resiliency. So any examples you could provide or any use cases that really sort of stand out

Ken Levine, Chief Executive Officer, Xcitium
You know, we again, coming from specifically that that cyber point of view, I think that right now the challenge is also exasperated, not only do we have work from home now, which is a given but we also have the mobile device that impacts even when you're in the office, if you're on your, your, you can do almost everything on the mobile device. So that just adds another layer of complexity. But I think what we've started to see and I'd be interested in these guys perspective, too, because it may be more in their (inaudible). But you know, there's this whole notion of micro segmentation and segmenting your networks a little bit. And we've started to see I worked at with a company that did that a couple of years ago. So, but it was kind of emerging and, and so one of the things that we found some enterprises doing is they're

starting to look at, the more granularity you can get with what you have to secure the narrower you can get it, the better your security without really implicating things. So, you know, I think one of the things that I've seen them deploy, it's not necessarily relevant to obsidian, but it is to cyber is just trying to do this micro segmentation, which is sort of, you know, in a way, it's building perimeters around smaller silos without impacting the usage of it. So we've seen that starting to gain a little steam in the security world.

Srinivas Rao, AVP & Solution Specialist, Tata Communications
Yeah, I think since you talked about customer examples, I do it for living, because that's why I got excited and then press the button first. Yeah, I think essentially, the transformation when we say people all know that, okay, they went on to the clouds, and there is a cloud transformation that has taken a leap, right. But then, people now realize all the CEOs, now they're realizing that we have to also do some sort of a network transformation, that to it is a secure network transformation. Otherwise, you're in for a failure, because you really don't know what sort of security posture you are managing, what sort of experience that you are giving it to your customers and your own employees and all that stuff, right. So therefore, there is something like a, you know, methodical approach something like Day Zero, day one, day two, you need to follow whenever you want to deploy an SDWAN. day zero is where, look what you have, what is the as is what are the current, you know, assets that you have? What is the CMDB that you are really having? And you have to segregate your applications for different user experiences as well. Right. So that's what you need to do in Day Zero Day one is like you have got a cluster of OEMs talking about SDVAN, therefore, you need to know which is the right one, do you have an experience of someone who could really understand what those challenges are, because they have to live with your existing environment as well, it cannot be that you know, you're creating a greenfield all the time, you have an existing Cisco pix firewall or Palo Alto, next generation firewall, you have got a Z scalar system, whatever, right? So therefore, you have to have a good experience a player who can give you that brownfield (inaudible) investment protection, that's what is most important. And last but not least, day two, how are you managing this whole fulcrum of you know, the environment, which is including private 5G, IoT is the (inaudible) MPLS internet, there's like normal things that end of the day, they all get culminated in creating this enterprise, so to speak the renewed environment. So therefore, you required a very revised or renewed attention in terms of managing this complexity. So you need to give a thought to how are you going to manage the day zero, day one, day two, to have a right esteem and posture for you?

Hugo Vliegen, Senior Vice President of Product Management, Aryaka Networks
Yeah, maybe I can give you an example of a company in the in the airline service industry, which we have been working with was ten thousands of engineers who are working on the airlines for repairs and updates etc. And for them, it's that they had a traditional model. You know, where they had outsourced to manage it to traditional MSP with multiple technologies under the hood will mention the names but for networking for firewall for cloud, etc and what they realize the complexity of this, even though it was outsourced to a managed service provider to make a change one week, two weeks, and as a result of fact, not that many service providers are unwilling but the stacks and the flows and the integration of all these other technologies honors is very complex. And so when we got to interact with them, we talked about that we have a software model as a cloud delivery provider, where we can have the software stacks on prem and in the cloud, and integrate not only on the single pane of glass, because that's often the makeup, right, so you have to go under it to control planes and data planes is integrated, because if you, if you don't do that you can do whatever you do, you can stitch and it becomes overlay, right? And you still are struggling a visit. And if you go back to this customer in this airline service industry, for them, it was like, we can never go down. Never ever. And if we go down, if it risks what do we do, right? How we

do get out of it? And if you want to make changes, for example, you talked about micro segmentation and segmenting. If I'm dealing with a segment definition, MPLS, segmentation and networking, segment definition and security. And I have to coordinate all of this stuff. Even if you outsource it to an MSP within the MSP, you have silos again. Right. So that's a huge problem, which we believe we have resolved, right, from an architectural point of view, which is very essential if you talk about these heavy topic topics like business continuity, right.

Prakash Mana, Chief Executive Officer, Cloudbrink
Thank you, Paul. I think examples, as everybody has talked about are countless in different industries, let me just touch on one or two. We're working with a content provider. In the old world, in order to build a creative documentary, that content team needs to fly into LA Los Angeles into Hollywood or some studio where you record your movies, you do your programs, and all of that stuff. In the post pandemic world because that thought process has already changed. Once you find creativity in in a in a place that is nowhere close to any studio or someplace in the real life example is in this particular case, they found a team in Cambodia, right. So instead of having that team of 17, go fundraise and find money to fly in and do all the recordings, everything. In the future of work world, we can deliver enterprise grade, reliable and secure connection all the way to wherever they are. And they have got digital Dolby sound system in the cloud, they can do all their creative recording, designing all of that right then and there. So that's one example. Similarly, in telehealth, all of a sudden the health care system, at least here in United States was under stress, because of all the COVID and all that other pandemic related issues. But at the same time, there was a population of medical healthcare practitioners who did not want to come to hospital because they would be putting their own family members at risk. So they so that put additional strain on the system. Fast forward. Today, what was supposed to be deemed as one of the toughest regulatory challenges in the world is to deliver eHealth or telehealth is now a commonplace thing. We because we've been able to deliver a highly reliable secure network all the way to wherever that healthcare practitioner is, using digital technologies. Now they can do all of those things, wherever they're similar cases are in call center industries in hedge fund is another use case that we see quite a bit as well.

Paul Hughes, Research Director, Future of Connectedness, IDC
Those are all great, It also makes me think of one that I just I had I was doing, I did an interview with a mining company up in Canada. And you think about the country, think about even in this as organizations become is they're adopting smart mining, you know, they're out there, so remote out where they are, and any type of network interruption or outage, put them in, they will shut down for three months because of all of the automation within their systems. You know, you've got autonomous vehicles, all the health and safety requirements, all of again, all those disjointed data silos, the issue of trying to bring all that together. And this became such a big priority to make sure that from a from a network redundancy perspective, and from a backup and obviously the traditional sort of BC and DR perspective, but that became such a critical component for them as they you know, adopted more and more smart technologies because it becomes something that just is so critical in order for them just to keep their business going.

Angus Robertson, MC
I think we have time for one or two questions from the audience

Antony Savvas, IT Europa, IoT Now and Vanilla Plus
Anthony Savvas. It Europa, IoT Now and Vanilla Plus. Aryaka said that, you know, the CEO gets fired if they don't like do their job. I think that's part of the problem they never do. No one gets fired when something

goes wrong with business continuity or security. I mean, look at T-Mobile, they've lost over a quarter of the population of the US. In two security incidents, the CEO still there, no one's been fired for it, and the government doesn't seem to care. So what's the point?

Paul Hughes, Research Director, Future of Connectedness, IDC
Yeah, that is a great point, at least from my perspective, particularly as you start dealing with industries, and obviously telco is a big one particularly T Mobile, the data breaches, but I think there definitely needs to be as you start looking up within a lot of those organizations, that if not there needs to be someone's throat to choke otherwise these problems don't ever get addressed. Part of my view is as I look out at this whole space, I look out at what a lot of the enterprises that I've talked to are saying is that really, the big focus is to have a specific set of folks that actually manage this whole process, so that if something does happen, whether it's managed internally, or it's managed through a third party that's a managed service provider, there is much more responsibility. There's someone who can take full responsibility for it.

Prakash Mana, Chief Executive Officer, Cloudbrink
Paul, if I may add there one more thing, I think while we're all tied to the digitization, and digital transformation, infrastructure, all of that, when we speak with the boardroom, CXOs and stuff like that, the most successful ones, we've noticed a pattern now are starting to look beyond the digital assets into human assets, right. And when you go into these board conversations, all of a sudden, it's not so much about just putting a gun on CIOs head or throating. Joking, CISOs. throat and all of that, I think the conversation is very well rounded. You've got the CFO who cares deeply about people productivity, how we can get the most out of our workforce. You've got CHRO or chief people officer who is focused on employee morale, and retention and stuff like that, you got the CEO and boardroom that is focused on top line, employee happiness, all of that. So if we start looking beyond just the digital assets here, and there is a real opportunity for IT leaders to become heroes here and drive the entire 360 degree organizational push towards all of these angles, not just on the digital aspect of it.

Guy Hervier, Informatique News
Yeah, just a very simple question. Simple question about terminology. How do you compare a business continuity and resilience?

Hugo Vliegen, Senior Vice President of Product Management, Aryaka Networks
Yeah, it's a continuity on the same scale, right? So business continuity is if it if things stop, you know, how fast can you recover? Resilience is actually that you reduce the probability that it happens. And if it happens, maybe you don't experience it, because it's all automated failover? Right. So for example, you had an in October and France, you had an undersea cable cut. Right? And there's every other day isn't underseas cable cut, but it was so bad that a large part of the country could not function anymore. That day, and even a cloud security provider was down in the sense that the sale function, there was business continuity, but the experience was very, very bad in terms of latencies etc right. And there is an aspect was called security provider, you have to go under the hood, what they do, how do they think is undersea cable cuts? Right? So that's one of the things we do in Aryaka that we can guarantee the bandwidth because in that event on that day, we basically everything failed over because we control the overlay in terms of the undersea cables, which we are using as a cloud provider. So some of that is very deep. If you go into resiliency and business continuity, there's a difference between a very good question. Thank you.

Angus Robertson, MC
Thank you very much, Paul. Thank you to the panel.