Deutsche Bank 2023 Technology Conference

Company Participants

- Charlie Bell, Executive Vice President, Microsoft Security

Other Participants

- Brad Zelnick, Deutsche Bank

Presentation

Brad Zelnick {BIO 16211883 <GO>}

All right, well, the room got a little bit quiet. I think this is live. Good morning, everybody. I'm Brad Zelnick with the Deutsche Bank software team. Welcome to the DB Tech Conference. Once again, delighted to have everybody both here in the room and online that's listening in.

For this session, I am truly delighted to welcome none other than Microsoft's EVP of Security, Mr.Charlie Bell. Charlie, thank you so much for being here with us.

Charlie Bell {BIO 22439127 <GO>}

Oh, it's great to be here. What a nice setting.

Brad Zelnick {BIO 16211883 <GO>}

I learned that you're from sunny Irvine, California.

Charlie Bell {BIO 22439127 <GO>}

Yes, I grew up down here, so I know the whole area. And it's kind of nice to get back in the -- out of the smoke and into the sunshine.

Brad Zelnick {BIO 16211883 <GO>}

Well, we're all glad to be here with you. Thank you so much, and really looking to learn a lot about Microsoft and its strategy and security. Thank you so much for joining us. If you don't mind -- maybe some silence. If that's important, you may want to take that.

I always take a call from my mom, even if she calls while I'm not here.

Charlie Bell {BIO 22439127 <GO>}

Not my mom.

Brad Zelnick {BIO 16211883 <GO>}

Okay.

Charlie Bell {BIO 22439127 <GO>}

But I would take that call.

Questions And Answers

Q - Brad Zelnick {BIO 16211883 <GO>}

(Question And Answer)

So maybe if you don't mind, for those that don't know you, could you just take a minute to explain your role at Microsoft and what your mandate actually is?

A - Charlie Bell {BIO 22439127 <GO>}

Sure. Well, maybe the best way to do that is kind of wind the clock back to when I first started thinking about doing something new when I was at Amazon. I was at Amazon for 22 years, for those of you who don't know. And in January of '21, Jeff Bezos said, he was going to step away. And I thought about it, and I thought, wow, this is going to be a different world. I could keep doing what I'm doing. I'm having a good time. We're building a cloud.

But I thought about it and thought, if I'm going to do something new, this is the moment. Because of my age, I thought, I get into things deeply. I can't do the years and out thing. So I thought, well, if I'm going to do something new, I should really analyze it, think about it, and either stick with what I'm doing or do something else.

And the thing that got me right away is something I'd seen over the years with customers in cloud computing, the growth and the problem in security. And it really bothered me because I didn't see an end in sight. It was actually getting far worse. There was this whole shared responsibility model. It was very difficult for customers. And I thought about it a lot. And the more I thought about it, the more it grew on me. And it was funny because I was talking to my wife, and she's, by the way, a brilliant woman. You can look her up someday.

But she said, "You know, you should talk to Satya Nadella." I said, "What?" She said, "No, you should talk to Satya. Microsoft is doing a lot in security. And it's a great company." And at the moment, I said, okay, fine. So within a week or two, she knew Satya, by the way, there's an old story there back in the early 2000s before Satya was

Satya. She had tried to recruit him to Amazon and, of course, he was trying to recruit her to -- I met her at Amazon. She was one of the senior leaders there.

And so she called up over there at Redmond and on a Saturday I was talking to Satya. And the thing that impressed me is first of all, I didn't know it, he'd already formed what Microsoft calls a customer solutions area around security because he saw what a problem this was. And the more I talked to him -- by the way, he didn't try to sell me at all. I wasn't recruited. He wasn't trying to push, "Hey, Charlie, you ought to join Microsoft." He was just listening and asking questions and then answering my questions. And I was mostly interested in how was he thinking about security.

But the result of that conversation, I talked to the two major engineering leaders he has there. Rajesh Shah who runs the productivity and user side of the business; and Scott Guthrie, who runs the Azure cloud side of the business. And it was a really great conversation. What -- I realized a lot of things. I realized one, it was an engineering company. Microsoft was really inventing a lot. But also very thoughtful about how you do that at scale.

And so -- and of course, the security problem, the more I thought about the security problem, I realized it's one, the company was really going to solve this issue was going to be a provider because you see so many things as a provider. And this I knew from running a cloud.

You just see how customers are both currently using things, where their problems are. You see where they're going, what they're doing, what their issues are. I was very much attracted to the fact that Microsoft had, really I'd say, the three pillars of -- in addition to the security business, had the three pillars of services in the cloud that we're going to read on this problem. One is providing an infrastructure cloud. That's really important.

The other is the end user and productivity world because bad actors start with people. That's one of the -- we're the weak link in this. And then of course the Identity business that Microsoft had because when you move to a world of Zero Trust, you have to know what you're talking to, who or what you're talking to. And Microsoft had far and away the largest capability in all those areas.

And so yes, I talked to Satya, came over about two years ago. He formed the CSA, but what he hadn't done is taking the products, the engineering products from Scott and Rajesh and united them in one organization. And so I brought those things together and so my mandate is all things security. By the way, he also has a read (inaudible), the CISO report to me. And so I own protecting Microsoft. I own the internal security at Microsoft as well. And there's a lot of first-party equals third-party, there's a lot of learning that goes on there. Microsoft is ground zero for attackers, and so we learn a lot from that. But yes, that's my mandate.

Q - Brad Zelnick {BIO 16211883 <GO>}

Excellent, Thank you very much for that. And you've touched on a bit of my next question, but I'll still ask. I mean, the momentum just in recent years in security has

been nothing short of impressive. At a high level, can you start by giving us a sense for the overarching strategy and the couple of key things that you think really differentiates Microsoft in a security context in what is a highly, highly competitive, even noisy market?

A - Charlie Bell {BIO 22439127 <GO>}

Yes. Well, like I said, one of the things I thought about carefully was the breadth and scale of the problem. I mean, one of the things we have to realize is, this problem is not getting smaller, it's getting larger. The estimates of the take, the negative drain on the world's economy that bad actors represent have gone from $6 trillion, I think it's estimated now to be $10 trillion in 2025, and it's growing faster than the Indian economy, which is, I think, in the top 20 GDPs, it's the fastest growing economy.

So the problem is getting more difficult and you need to solve it with an end-to-end offering. You've got to cover the full spectrum because attackers work, they start with end users, they'll dish somebody, compromise an account, they'll use whatever privilege that person has to lever up to somebody with real privilege or that person, and use that to move laterally through the environment. And they'll use all of the pieces, they'll use the network, the identity, e-mail, productivity applications, main applications, infrastructure, they use all of it.

So end-to-end is really our thinking about what is going to solve this problem and we focus on all those areas. I think the world is moving that direction. I've seen some CISO surveys where there's a pretty radical shift in their thinking, going back like 10 years, generally they piece together solutions by getting best of breed, but literally hundreds of different solutions to read on the security problem and now they're going after consolidation, they're trying to figure out how to get end-to-end. And attackers find the seams between things, that's part of what's driving this.

Q - Brad Zelnick {BIO 16211883 <GO>}

It makes sense. Charlie, I think it was in December that Microsoft had disclosed that security is a $20 billion plus business at the time, growing north of 30% year-over-year versus the broader security market, which I think is growing somewhere in the teens. Obviously, the backdrop has become a bit more challenging since then. Can you talk about what you've seen in terms of customer demand and your ability to take share in this environment, because I mean clearly you have a consolidation play that's quite unique?

A - Charlie Bell {BIO 22439127 <GO>}

Yes. Well, I think we're one of the major beneficiaries of the consolidation move. We see healthy growth. We're now a million organizations protected, and that number grew by 26% last year. Really interesting is that the number of customers who are using more than four workloads, that number has gone up by 33%. So there's an intensity, increase in intensity, I think, that's going on.

I think there was a lot of optimization that people were doing, but typically you see that happen over a short period of time. Over the long period of time, the way I think

about it is what I said like, we're going to a $10 trillion drag on GDPs, and that's going to grow. I've seen some estimates to say it could pass the U.S. economy's GDP by the 2030s if we don't get ahead of this. So that, to me, is the signal of demand. And so I think there's going to be a lot of need for security products going forward.

Q - Brad Zelnick {BIO 16211883 <GO>}

It's a strong signal, and it doesn't seem to be abating. It's been the same story for years. Maybe with that, I think it was in 2021, Satya announced plans to invest $20 billion in security through 2026. Obviously, there's very few, if any, other players out there that can credibly make that kind of statement and have the wherewithal. Can you talk about your R&D prioritization and the criteria that you use, how generative AI might impact the composition and perhaps even the level of overall investment going forward?

A - Charlie Bell {BIO 22439127 <GO>}

Yes. Well, that was one of the reasons I came to Microsoft. I looked at the assets that Microsoft had and the leadership, Satya's propensities to bring those to bear on security. The first thing that -- if we're going to turn the corner on all this, the first component is data. We talk about the asymmetry of the attacker, that the attacker can come at you from any point and you have to defend the entire perimeter that you own.

But we have an asymmetry in our favor, it's data. We get to see the entire environment. And one of the beauties of being a cloud provider is you don't just get to see one environment, you get to see lots of environments. And so there's a data asymmetry that works to our advantage. We do 65 trillion signals a day processed within our products.

And the fact that we have all that data, I think is a huge advantage. So bringing that to bear with investments that we're making is super important. We've brought together -- the industry likes to take all the products and break them into these cute four-letter acronyms, everything from SASE, XDR --

Q - Brad Zelnick {BIO 16211883 <GO>}

SIEM, SOAR.

A - Charlie Bell {BIO 22439127 <GO>}

SIEM, SOAR, yes, we'd like to break it all up. And that's -- by the way, you think about the fragmented world we've been in, it's certainly natural to want to talk -- have names for all the fragments that you talk about. We've basically blurred the lines between things like SIEM and XDR and SOAR, and all the things that you have to do, really, if you're going to be end-to-end, you've got to blur those lines, and it starts with data.

And so there's a lot of investment in that, and by the way, that's a prerequisite for probably the biggest change that we're going to see in security, the one that's going

to finally, I think, turn the corner. The big part of -- you can have all the data in the world, but if you can't see it, and act on it, and use it, it doesn't matter, and we haven't been able to do that so far.

It's one of the challenges in the security industry is the siloing of expertise. You think about, there are companies that know how to do network security, there are companies that know how to do e-mail security, and maybe do something in identity, or endpoint. Each of these companies has an expertise, and they all want to branch out from their expertise, but fundamentally, you got to be able to get across all of it, and to do that, it's AI.

You've got to be able to take all of this data, all of the signal, and understand it. And because no expert in your SOC or in your development organization building a proactive defense, nobody really can understand all of it. The AI can't. The AI can both on the, we call it shift right, on the -- just be very good at responding to attacks. The AI can move very fast and see across a whole bunch of variables and take action.

And in the proactive sense, the AI can look at a very broad environment with lots of different technologies and understand across all of it what needs to be done. And so, that was, by the way, some of my thinking when I came over. One of the things I saw was that just astounded me in my old job was GitHub Copilot. It was just amazing because we were thinking, obviously, about the same kind of thing. It was amazing how good it was.

And as I really dug into it, what I realized is the partnership that Microsoft had with OpenAI, it goes way back. That it's an R&D partnership, the understanding that Microsoft has of that LLM technology and what it could do, it was pretty clear that there was a lot to do there in security. And so that's really opened the door. I think, it's even gone faster than I thought. When I saw what GPT-4 could do as a core of building AI capability, that is the other thing that I think gets us around the corner and we can finally have it be an asymmetry of the defender.

Q - Brad Zelnick {BIO 16211883 <GO>}

I mean, they're using AI as well, right?

A - Charlie Bell {BIO 22439127 <GO>}

But the beauty is, they don't have the data that we do. We get to see the whole environment. They get to go -- they still have to go after their thing, but we get to see all -- by the way, we get to aggregate everything that all of them are doing too. And so, I think we have a -- we now finally have an advantage with AI.

Q - Brad Zelnick {BIO 16211883 <GO>}

That maybe leads to my next question, which is back on a theme that we've touched on, which is consolidation, which I feel like, has been a promise of the industry. Any newcomer who stumbles upon the problem and the domain naturally would say, okay, just -- the customer just wants to make it stop, and they're swimming in all

these point products, but it's always -- cybersecurity has always been this arms race, consolidation along the promise.

Why do you think consolidation is finally happening now? What gives you the confidence that the history of fragmentation for which we've seen pockets of consolidation, next-gen firewall, what some of the endpoint players have done, but there's still more vendors on that RSA show floor every year than we can easily count, but what is it that helps to buck that certainty that's always been for quite some time?

A - Charlie Bell {BIO 22439127 <GO>}

Well, it's like many other things. You have ideas about something that should happen, and you look at the technology and it's just not mature enough to do it, and then you finally reach a point where you get technological maturity.

It's why I came to a provider, because you look at the capability you have at Microsoft in data, like just being able to process huge amounts of data, we're talking about 65 trillion signals a day.

Q - Brad Zelnick {BIO 16211883 <GO>}

Sure.

A - Charlie Bell {BIO 22439127 <GO>}

You talk about massive inputs of data that come from customers as they're building their unique environments, you've got to be able to process huge amounts of data, you've got to be able to do it in real time, and we finally have that ability. We can handle huge volumes, petabyte scale logs coming in, the ability to issue queries across all of that, being able to do it in real time and respond, all the messaging systems, a lot of the cloud technology has really begun to enable this.

I think the other one is the AI side. I think the fact that you can now bring AI to bear and look across some of these signal silos, if you will. I mean, we've always had the seats to it. We've talked for a long time about Zero Trust. Well, the aggregator of Zero Trust has been Microsoft's conditional access. I saw that from the other side. You have Identity system.

It basically went through a whole kind of maturation of that. We protected ourselves with passwords, and we figured out that we needed MFA. We needed multi-factor authentication. We needed something else that we had that said, yeah, I'm Charlie. You can trust me. And then those things started to get intercepted.

So now you need an AI that can look across the infrastructure and say, "Well, I'm looking at your end user variables. I'm looking at your system variables. I'm looking at your IP address, the system you're on, identifiers. I think you're Charlie. You're not Charlie, you're not going in." So there's been a lot of capabilities that have been built over the years. And that's kind of how technology works, you can tend to layer things up. But I think we finally have enough technology to do it.

And I also think, I go back to Satya, his understanding of this being kind of fundamental to the human progress on technology. One of the reasons I wanted to do it, and he shares this view, is that, if you're a technology company, you win if people can confidently move forward. They can adopt new technologies. Like what's going on with AI right now, GenAI? I've got to be able to just use it. I can do tremendous things with it, if I feel I can do it safely.

But if I'm afraid because I'm seeing bad things happen out there, I don't want to use it. I won't buy it. And so security, that goes all the way back to Bill, all like around 2001 or 2002 when he did the trusted computing memo. Microsoft figured out that it really doesn't have a business if people don't feel confident moving forward.

And so I think we're in a spot where it's in everybody's interest, it's Microsoft's interest, we're going to continue to invest in it and make it easy for people. Move it into the background, security by default. Eventually, if we really get over the hump, you guys won't even be talking about it.

Q - Brad Zelnick {BIO 16211883 <GO>}

One day. It's all about trust. That resonates with me quite a bit. If I go back to March, just several months ago, the response that Microsoft proclaimed to the world, to all the things that we're talking about, the trillions in loss to our economy, the shortage of talent that really understand cyber, the fragmentation that customers are forced to deal with.

The answer was Security Copilot, which I believe combines the capabilities of GPT-4 with proprietary Microsoft security models. Can you remind us what the product is, maybe some of the feedback that you're getting in preview, even potential monetization structure, and what milestones should we be looking to as investors going forward on the progress of Security Copilot?

A - Charlie Bell {BIO 22439127 <GO>}

Well, first, this isn't just, ChatGPT looking at a vulnerability and kind of telling you about it. Like this is -- in order to do the security side, hopefully, maybe you guys have played with Microsoft 365's ability to summarize an e-mail or something. But to do the security side, you've got to -- you get down into a lot of very technical analysis of signals, looking at logs coming off of machine.

We think about it, this is a kind of a little different application of generative AI. And it's -- we often say security is a team sport. Well, within the AI world, building a copilot is a team sport. It's not just the LLM, it's specially trained models. For example, one thing that the LLM has to be able to do is query data. Well, how is it going to do that? Well, you have to have separate capabilities that know how to do that. And so it's a systems problem.

And what was exciting to me is, I came to Microsoft in -- well, it was two years ago. It was end of August '21. And we were just getting started on LLMs and security. And now when we look at all the things that we can do across the board to stitch this

together, you've got to be able to go after, not just the data that we have, the signals that we have, you got to be able to let the customer bring signals, it has to be done safely.

One of the challenges I think in the AI space, when you start systematizing large language models, is that, oh my gosh, this thing is going to be looking at a lot of data, how do I protect the data that I'm accessing? How do I make sure that this customer can take their stuff and not have customers be able to see it or do something, or it gets into the model in some way? That all has to be guaranteed through separation.

And then the other thing is, you got to make sure these models cannot be manipulated. One of the challenges is that large language models operate off of prompts, and people can manipulate what the answer is going to be by doing things with them. So it's a lot of -- we do a lot of red teaming, understanding both the base model and all of the separate models and the combination of the system, how it's going to behave. And so that's actually taken quite a while. That's been a long journey for us.

And it's something where I think being part of the R&D for development of GPT-4 has given us a lot of understanding of the problems and how to go solve, and also let us work with OpenAI and what kind of things have to be done at their level, but also our own capabilities. So the way I'd say it is, it's a journey.

We've got private preview with a few customers. We're working with them. I think the first reaction a customer has to this is they're astounded, like the fact that they were able to have this thing tell them not only, here's the problem that you have, but here's what you should do to stop it right now, and I think it's the same reaction I had the first time I saw the capabilities that we were producing. It will change security forever.

But it's -- so it's a fundamentally new way of doing things. It's also pretty, I'll call it R&D and resource intensive. As I said, it's not just taking ChatGPT and saying, summarize an e-mail. It's really a whole bunch of things that you've got to go do at a systems level to make things work. And it's back and forth between us and the core teams that own the models at Microsoft and OpenAI, and so we're on a long journey.

It's going to be -- we're going to begin introducing things to customers, I think a little more broadly later this year, and we'll roll it from there. I think, as far as monetization, the only thing I can say, it's going to -- it's a lot of investment on our part. It's a lot of GPUs to go spend.

By the way, the other thing about these security models is, you guys go to the web and you start playing with ChatGPT or Bing and you start going back and forth, well, each time you do it, you're doing an inference. But you do security models, you're doing a lot of inferences. Like in order to do the systems level job we do, it's

resource intensive. So this is going to be a -- it's going to have to be a separate important business for Microsoft.

Q - Brad Zelnick {BIO 16211883 <GO>}

How do you maybe, on the topic of monetization, balance the interests of direct monetization versus indirect monetization and creating trust and therefore just better sell through of the rest of the security portfolio and Azure and Office and other copilots and everything else? I mean, at Microsoft I know Amy's not going to let you spend money on spending all these GPUs without a return, but there's a big picture here, right?

A - Charlie Bell {BIO 22439127 <GO>}

We do that. Again, one of the reasons I was excited about working at a provider is that there's a flywheel between a paid security business and a free security business. So the provider is going to provide security by default embedded in the -- we just did a bunch of stuff with -- we continually launch all kinds of new things with Windows for example.

We've done a tremendous number of things with our Identity offering, Entra, and it just comes in, it just -- customers get it. And that part of the business gives customers the confidence to move forward with products. So there is indirect monetization, it's in the interest of the provider to make sure that people are safe from the get go.

But there's a flywheel because you learn, you get to build on top, you get to find the unique needs of customers who say, banks, for example, have some very severe regulatory requirements for segmentation of duties. And so, okay, they're going to need very special functionality to be able to do that.

The analogy I use is, you've got a car, everybody buys a car, some of you buy snow tires for your car. So you're going to buy extra stuff that you need. So there's always going to be monetization here and this is an incredibly important area, I think, but there will be things we provide as part of the products themselves as well.

Q - Brad Zelnick {BIO 16211883 <GO>}

That's helpful context. I want to be respectful of the time and there's so much to talk about, Charlie, such a broad topic, but maybe pivoting to another acronym. I think it was big news just a couple few months ago. Microsoft announced its entry into the SASE market with Microsoft Entra.

Why is this an area where you feel you can really win and how should we think about Microsoft's value prop as you get further away from securing Windows Core and Microsoft 365 apps and Azure services?

A - Charlie Bell {BIO 22439127 <GO>}

Well, so first of all, I want to say, one of the parts of the conversation with Satya that got me at Microsoft was, I was probing him to understand, is this about protecting

Microsoft products? Or how do we think about securing things? Because back of my head, my thought was, one of the things I've observed is, you can't say it's my cloud or no cloud. It's going to be a multi-cloud world.

People are going to use many things. That's historically, you go look at technology. Everybody's always used a polygon of technologies. If nothing else, they get them through acquisition or they've been using them for a long time, but they'll adopt new ones. And the thing that resonated with me is he was all over protecting everything. And that ding, ding, ding, that's end-to-end. That's how you become end-to-end.

You say, look, I don't care whether it's -- and we do, we launched the security world that we have at Microsoft, we protect AWS, we protect GCP, we protect other people's technologies. And we're very committed to the whole end-to-end idea. And so when you think about SASE, maybe it's best to kind of wind back a little bit and really think about what does Zero Trust really mean?

Zero Trust is about, I don't trust anything. Like, I have a system, the moment the system starts to default trust something and say, yeah, you're okay, without checking, well, that's an entry point. It doesn't have to be the network. Like, we've often talked about Zero Trust like it was some kind of networking thing. Well, Zero Trust is a very broad concept. But we've been doing the core of that for a while, so conditional access in Entra.

So the ability, as I said, to take a whole bunch of variables, network variables, a lot of mark, and say from an AI perspective, you should have access. No, you shouldn't have access. That ability, a natural extension of that, is to do the things that we just announced with Entra, but I think the idea is if we're going to be end-to-end, we've got to be able to do all of those things for customers. And they tell us. This isn't us just saying, hey, what do we think we ought to go do. This is customers saying, hey, you guys really need to be giving us this capability.

Q - Brad Zelnick {BIO 16211883 <GO>}

Got it. Makes sense. If we look back in five years, what metrics should we think about to know if you've been successful? And what security-related objectives and measures are all of Microsoft's business units held accountable to? I mean, I remember many years ago, before you had arrived, I had heard of, actually related to Azure AD, where there was a metric by which many of the businesses were measured.

It was one of the many criterias or objective of how many identities did you bring into Azure AD? What's over a multi-year horizon, how do we know that you really crushed it? And you achieved your goal, and how do we think about measuring that?

A - Charlie Bell {BIO 22439127 <GO>}

Well, I mean, I do think revenue is a good one because it means customers see value in what you're doing. That's sort of an obvious one. And we're really proud of

crossing the $20 billion mark, so that was kind of a big milestone.

But actually, one of the things that would make me super happy is if we stopped talking about that GDP loss being bigger than the U.S. economy in the 2030s, like suddenly the whole trajectory is changing, and we look at '25, and we say, hey, maybe that $10 trillion loss didn't come true or to see some tilt in that trajectory. That would be a really big milestone, I think, for us.

But yes, I mean, we'll continue to the number of organizations protected. We track all kinds of very detailed metrics on protected users and everything else, but yes, I would say the big one is that we've changed the trajectory on that growth and what's happening out there.

Q - Brad Zelnick {BIO 16211883 <GO>}

Cool. Charlie, we are just about out of time. Is there anything we didn't get to that you wished I had asked that you want to impress upon folks? I mean, the work that you're doing is obviously incredibly important to Microsoft's success, but it's important to the world. Any final thoughts?

A - Charlie Bell {BIO 22439127 <GO>}

Well, just sometimes we talk about this kind of loss, and you guys see headlines all the time, and I want everybody to be optimistic about this. One of the things that got me here was I really love the idea that human progress is all about technology. You apply technology to new problems, you get to solve new problems.

And I think we're going to be able to do that. I think, the key is the asymmetry I talked about, the fact that we're going to be able to aggregate across a large volume of data using AI, we're going to be able to turn the corner on this thing.

And so, yes, I mean, look, you look at what nation states are doing with, what Russia's doing to attack and what China's doing to attack, and North Korea and Iran, we have a whole unit that spends a lot of time in those areas understanding those adversaries. And it can be kind of depressing sometimes.

But I think, look, I don't think human nature is going to change. I think there's going to be some bad people out there, and they continue to do things. So I think this industry is going to be pretty healthy. But I wouldn't want anybody to think, oh, my gosh, I've got to run for the hills and hide. I think we're making some real progress on this, and I'm excited to do it.

Q - Brad Zelnick {BIO 16211883 <GO>}

Cool. Well, we're all counting on you. Charlie, thank you so much for being here at the Deutsche Bank Tech Conference. This was really, really great.

A - Charlie Bell {BIO 22439127 <GO>}

Thanks for having me.

Q - Brad Zelnick {BIO 16211883 <GO>}

Cheers.