**NETEVENTS GLOBAL IT SUMMIT**

***SAN JOSE, USA***

***OCTOBER 3 & 4, 2019***

**DRAFT**

# *Welcome*

**Manek Dubash, NetEvents**

Welcome, welcome to this event. Welcome to this stunning agenda we have in front of you, in this stunning location. My name's Manek Dubash and for good or evil I'm going to your MC for the next couple of days.

So, what have we got coming up? We've got a packed agenda here; we're going to be talking about 5G. We're going to talk about AI, Cyber Security, Multiple Cloud Management, Edge computing, SD-WAN and host of other topics.

Good to see a lot of friendly, familiar faces down here. Good - even better to see a lot of friendly, not so familiar faces. Welcome, a very special welcome to you, to NetEvents. I hope you come back again having found it a rewarding experience.

I'd like to explain just a little bit about how this event works. Basically, we're having a plenary session this morning when we're going to be talking about all the topics I've mentioned, and more. That will be repeated again tomorrow morning and this afternoon, after lunch and tomorrow afternoon, after lunch, we'll have what arguably I think is probably the most important part of the event, which is the meetings every 40 minutes between the press and the vendors and the analysts. Those meetings will last as I say, about 40 minutes or so and the vendors move on and press stay put and they get a full blast of everything that's new and hot in technology down here in Silicon Valley.

We have here, for your information, over 100 press from some 35 countries. Speaking of the press, you will see on your screens in front of you that we have a Twitter competition. Let's see, we've got three prizes available. Every tweet that you send must include the NetEvents TV name and also the NetEvents hashtag. Every tweet must be relevant to the event and there are three prizes. As you can see, the top one is a Belkin portable charger for your phone. The second one is a Tile Mate, which a key findery [sic] thing, which is one of these little doofers here, don't lose it. The third one is chocolate cookies because, hey, you can't have too much sugar, can you?

Let's see, also we've got, oh yes, an innovation here right at the back there, in that corner there, we have available for the press a suite of jacks, into which you can plug in any

recording device you like. We've RCA jacks, we've got headphone jacks, we've got quarter inch jacks. I think there's some balanced jacks in there as well. So if you want to capture the whole thing in audio and put it on NetEvents CD or use it for your podcasts or whatever it is you want to use it for, that's available for that, right at the back, you'll get the audio for the whole event.

The transcripts will be available online for each of the open sessions, the plenary sessions the next day. So, today's will available tomorrow and tomorrow's will be available on Monday, because I think some people get the weekend off. How does that work? Images will also be online on the NetEvents website and there will be the USB press kit at the end of Friday, which will include all the press releases, presentations and all that sort of stuff.

So, I think that's the housekeeping done. Without further ado we're going to have - we're going to be talking about the network is the business, which is our first keynote speech. I'd like to ask you to give a warm round of applause, please, to Ravi Chandrasekaran from Cisco . Ravi, come on down. Wow.

## *The Network is The Business*

### Opening Keynote presentation by Ravi Chandrasekaran, SVP, Enterprise Networking Business, Cisco

**Ravi Chandrasekaran, SVP, Enterprise Networking Business, Cisco**

Morning everybody. Morning. Welcome to the NetEvents Global IT summit. I am happy to kick it off - 30 minutes. It's kind of a fascinating time in networking. This is - right now I would call again a second coming for networking. Because networking is central to business again. If we look at the 1990s then towards the 2000 timeframe, everybody were going to web, network was super important. It's once again happening. Network is the business. We'll talk about why? What are the implications of it? How do we go around it? As well as along the way I'm going to weave in the whole AI, IoT and security - how it has implications and what we're going to do.

Let's start with - if you look at every one of the industry today, you see that it's - whether bookstore or there is video distribution, taxi, every one of the industries, which are traditional business that have been there for more than 50 years, 100 years are getting disrupted, every one of them, in a fundamentally different way. We don't go and get taxi; we actually ask taxi to come to you. You do not go to theatres to watch the movie, you don't go to rent movie, you actually stream it. Things are changing in every industry. When we talk about customers, every one of the industry, it doesn't matter what industry you are in, every one of them are changing. It's around how do we connect users, things, with the data and application in ways that we have never done before. It's fundamental, it's all around networking.

It has grave implications for networking as an industry. We have an opportunity to become the most important part of the business. What are the challenges the networking industry faces when we talk about this?

We are talking about the priorities are completely changing. If you look at the number of devices that is getting onboarded. If you look at the number of mobility data growth, or if you look at the number of incidents that are happening in security, they're dynamic, they're changing. We're expecting 125 or so devices being connected every second. Twenty-five plus billion new devices coming onboard. Most of the companies are actually going to cloud, it's not anymore, a question of whether they will or not. These change completely how networking has to work. It's dynamic, the threats are all over the place. The implications are pretty profound. The dollar implications are pretty high.

If you look at it, at the same time the way we run the network is quite old. Pretty much most of the changes are manual. If you think about the [unclear] I'm talking about the number of devices getting onboarded are security threat. Most of the policy violations are all human error. Nearly three-fourths of the expense is spent towards running the network and keeping up with all the incidents and the tools that are happening. If we really want to move to a digital world, if you want to help digitise the business, you cannot do what we are doing.

Similarly, if you look at the networking [topology unclear]. The traditional network was very simple. Branches talk to data center, you apply - put a firewall and it go out to the web. Life was very simple. The world has changed dramatically. If you look at it, the [older users are all - they are] things. Branches are popping up all over the places. They could be a mobile branch, could be many different ways of doing things. You now have your data center assets being spread all over the world, between many parts of the cloud [unclear become zooming] service from the cloud. The topology's changing dramatically. You can go to a very different way of running the network. We cannot do what we have been doing before.

It's time for us to reimagine how we do networking. The traditional way of doing manual operation, the traditional way of doing changes are not going to be sufficient. What do I mean by that? We need to change from being hardware-centric to software-driven. This is what we call a software-defined network. We need to move from manual operation to fully automated - I'm going to talk about a certain example software - in order to change how we do networking completely. We cannot [bolt-on] security. I'm going talk a lot about the security threat we're going to face, that we are seeing day to day today. If you want to solve them, you brought out a separate firewall, the traditional way of doing it will not work. We need to have security built-in as part of the network.

You cannot just monitor the network; you really need to understand what is going on. You need to take the insight. You need to really look at the events in a very different way than what we have done before. So, it has dramatically changed from a traditional network to a very new world.

In Cisco, we call this intent-based networking. Starting by looking at a network, have a controller on top of it, have a way to pool data, have a way to communicate with the network in a very concrete basic of programs so the controller finds the complexity.

This is where you do automation. This is where you do policy. This is where you do analytics. It's actually a closed-loop system. In this, the network we are talking about has built-in security. I will talk about what I mean by that.

It's a very different paradigm. They are not bespoke devices. They are here - in this type of network, wired is not different and wireless is not different. It's a complete - you need to think of them as one single thing. We talk of 5G [unclear] Wi-Fi 6 is predominantly coming along all over the place. Look at this new network. You cannot treat wired, wireless and [unclear] to be different. They need to be thought of as a single network with a controller on top of it and how do you do closed loop. That's what we're talking. So, for a new digital world you need to move to this new paradigm.

What can you do with this new paradigm? First of all, you can address this whole manual effort. I talked about how today the network is broader. Day zero, day one, day two, day [end 20], all the operator [unclear] stack a box. how do your box gets to configured? How do you roll out changes? In this new world, you need to be compliant with security all the time. How do you make changes to the network in a way where you're not bringing the network down? How do you do closed-loop? Automation is a key that you can do in this infrastructure. It's fully automated so you don't need to go manually do the work.

In Cisco we have DNA center which is a controller we use, which actually sits on top of our wired, wireless and [unclear] infrastructure, it has ability to do these actions. This is an example of what you need to do to really address the challenge the customers will have, that IT has moving forward.

The next thing, this is again one of those interesting things in network; networking is used to producing a lot of data, they have been doing it for a while. Take the '90s, in 1990s when you started networking, we started using a lot of data. The problem is that we don't use the data fully. We never - they're all bespoke, every different routers and switches [developed] the data, we never made sense out of it. In this new world, what we do is we collect data, they [are recorded] at real-time, we create insights and then we can actually give remediation. We have 1000s of devices coming on every day. There is no way for you do to it manually. When you rely upon wireless, you cannot go one at a time to find out where the problem is. You want the network to be able to tell you what the issue is, so just remediation.

That's where we are going with this whole intent-based network which is automated data. It allows us to understand and be smarter. It understands about application, users and things, alerts you. Whenever there is a problem, it has the ability to give you remediation that what you need to fix. It frees up IT from being reactive, to being proactive. It's a fundamental shift you need to do in networking if you want to be part of the digital journey the business are going through.

When you look at security in this new world, it's completely different. The traditional threats are not what we're facing today. The threats are completely different. If you look at it, you see again and again many breaches. There is credit card of many different industries. It happens all the time.

For example, one of the financial report - one of the confectionary big company had a malware, and they lost $188 million in one single incident, one incident. A big logistics company, a transportation company, got impact by malware. Lost $300 million. Completely came to a grounding halt. It took them months to get back on track. A pharmaceutical company, similar incidents.

If you look at the industry today, the malware attack happens in [unclear]. Most of the time it's not fully public. It's happening every day. The interesting thing is these threats happen real fast. It took only four minutes to bring down the whole network, bring the whole company down. The implications are profound. If you're really planning to move to a digital world, we're trying to digitise where everything is connected. The business is running in a very different model. The security source are different. The implications are very different.

If you look at it, how this happened, is very simple. Doesn't matter. Everybody has the phones, laptops. They go into coffee shop, they click the wrong link. You get infected. That laptop comes into a building, in an office. Somebody plugs in. That's when the threat starts moving laterally. The networks today are flat. They move from one to other part of the network. For instance, move from IoT part of the network to point of sale system network where they are able to take critical information. Once they're in, they look for vulnerable spot, then many different threats gets introduced. This is happening every day, and every - many parts of industry.

The reason is very simple. The targets are very - a lot of money is involved here. There are national state activists out there. They also trying to find ways to undermine the infrastructure. The threats of this also have changed because we have devices. We have things. We are going to cloud. We let people bring their own device. It fundamentally changes what is happening in the network. The threat for software are changed dramatically, as well as the threats are also very different. There are many different threats are happening. They perhaps are often not trying to steal data. They are trying to encrypt and prevent you from getting access to data. Then they can ask for ransom.

It's a very different world we live in, this digital world. Look at that, the scale of attack, the complexity, and how sophisticated they are, and how we react [seems to be] very different. But when we look at it, the network is not prepared for that.

We see in every instance we have gone through, nearly 100 per cent do not have segmentation, keeping things in separate lanes. People, things, guests, separate lane. The flexibility you need, [unclear].

It takes nearly 200 days to find, on average, that you have a threat inside infrastructure. Even worse, it takes 60 days to fix it because things are done manual. These are very sophisticated attacks. It takes a long time to react. The implication [unclear] millions of dollars per incident.

This is the world we live in. When you talk about cyber security, cyber threat, this is what every industry is going through today. We talk about digitising every business, every one of them are exposed to this.

What we need to do is very simple. Three steps. First of all, you need to segment the network. Segment and reduce the attack surface and keep them in their own lane. Rules and policies which says what is in which lane. Segmented. Second, you need to get full visibility. You need to know about things, people, applications, cloud instances, what is happening. Last, but not the least, you need to have a way - an infrastructure that allows you to react fast. Real time. As soon as the threat is found, instead of waiting for hours and days, how do you go and shut it down? How do you quarantine it? How do you stop it? That is what we need go.

Unfortunately, we are very far off that traditional model. Things are done manual. You've got to go, enter one at a time. As we talked about, humans make mistakes too. They don't know the context. They don't know everything that's happening. The traditional segmentation of using VXLAN, or VRF, or ACL and all those, doesn't work.

More interestingly, people don't even know what is their network. They don't know who's connected. What things are connected. They don't even know what is the right segmentation. They don't even know who's allowed to talk to whom. They don't what policies they give for them. The traditional network is not prepared to deal with the situation we are talking. What you really need is something else. You should really be able to create the spin lanes. Have employees, I have things, I have guests, I have contractors. I have high value assets. I'm building management systems. They need to be kept separate.

Simple rules. You're not talking about IT [unclear] here. You're talking about identity. We're talking about understanding what it is, and then deciding how I segment. The reality is this. You know who your employees are. You know some of their … assets, but everything else is a swamp. You don't know what is happening there.

What you really need to do is you have to start with one. First identifying what is the infrastructure. You … data. You use network to classify what is available. What are the different assets that is connected?

Second you need to understand who's talking to whom. It's surprising for you to hear most of the companies do not know. They only know what is leaving their infrastructure, what is coming into the infrastructure, because they have firewalls.

We'll talk about [unclear] laptops within the infrastructure. They have no idea who's talking to whom. We do not know the [unclear] policy so you have to learn that. That's the next thing you are to do. Third you need a [author] the policy.

Last, but not the least, when you enforce a policy, you need to make sure it is being executed properly. This is a journey we talk about. When we talk about our customers, we talk about software defined access. This is what we mean by that. It is about how do you move from having thousands and thousands lines of CLI, but you have no idea using IP address what's happening in infrastructure. You hope and pray things are working for very different model. When you got IoT based, we understand what it is, who it is, and the same policy. Make it secure, simple, and easy to implement. That's what we talk about. That's what we will insist on, software defined access. That is being done right in my view for the access network. This is common for wired, wireless

it doesn't matter. It doesn't matter where you're connected. It doesn't matter globally where you are. You can set policy to say you know what, I'm am not supposed to - employees are not supposed to talk to each other. That means potentially a wireless is moving, and malware is moving. You can set this policy. It's very simple. It's auditable.

Now we have moved from IP address and things which are not scalable for identity. When you talk about cyber security in the digital world that's what we need to have. This allows you to create a very fundamental part. I talked about how we need to create a fast reacting system. It which allows you to create closed loop infrastructure. For example, you have a security infrastructure where you identify a threat, you identify a malware. For example, CISCO's infrastructure, you can talk to DNA centre. You can tell hey this is a user. I see that user's laptop is infected. We have ability to talk to your IPS systems. This is why the policies are there. It could be serviced now. Different users and different threats might require different responses. A policy decision.

Sometimes you may say you know what, this is an exec's laptop. I don't want to completely shut it down, I want to put it in a quarantine zone. It's a guest officially down as a thing, I want to stop it. You may have different rules based upon that this threat is happening. The IPS system those rules can communicate back to DNA centre using the API. DNA centre being a controller for the infrastructure, it implements the rule. It goes and shuts it down or creates a quarantine zone. What are you all to do? It communicates back to the IPS system [closing the gate]. This happens in minutes. When we talk about threats that we are facing, this is what you need. You need a closed group security system which understands who you are, where you are and reacts to the threat in real time.

Let me go to the last leg of my presentation. When you talk about all these things, I'm going to talk a little bit now about the use of AI in networking. I use specific term AI [unclear] alone. I will talk about MR as well [unclear] reason. When I talk about having DNA centre and having the ability to collect data, analytics, produce the information, that's awesome. Still there's too many things that's going on. You got cloud, you got application, your business rules you're trying to do. You're having experience for the users. All sort of different things are going on.

The ability for IT to do these still is very hard. The alerts per week, the events that are happening, and the number of people they are having, it's not feasible to really still do these with just controller alone. Just doing analytics alone is not sufficient. You need some other tool.

To look at the early '90s and the industry, the revolution, helped humans to get help from machines to do things which is not easy for humans to do. It's time again. The threats we are facing, the complexity you're facing in networking is not sufficient for humans alone to do it. Brains cannot sufficiently do it. You need help. This is where we have MO and [AA] comes in.

What we do, what example in CISCO, they collect all the date. I talked about what we do in analytics. We analyse it. We send globally to a single place in a global - what we call a privacy policy. We take all the knowledge we have got in CISCO at our internal support organisations and engineering and everywhere we have got, we convert

them into models. We combine them. They have the ability to do very interesting things. Let me talk about what we have. Three examples I'm going to talk about.

Number 1, the [unclear] is very interesting. Generally, you look at network, we always have anything you take you always have some thresholds. If it's above that give me alert, if it's below that give me alert [unclear] see how much time it take to connect. Anything you take if you have these things.

The interesting thing in networking is that you cannot have a single min or max for anything in your network, because every environment is different. This conference facility is different from the entrance that people are coming in and signing in. Is different from the rooms where people stay. It is different in hotels. Every part of the infrastructure, every environment has different behaviour, different days, seasonality.

In the morning people come and go. That's very much difference. Having a single reference point for infrastructure is not sufficient because there are too many alerts and most of them are not useful. What we do in CISCO, we take the data, we create this green band. This green band is the normal, which is dynamically calculated in the cloud for each facility, each instance, each part of the building. Now it allows us to be lot more smarter in when we alarm. Since our alarm [unclear]… above a static threshold now it is very dynamic. The dynamicity is per building, per day, morning evening. We take all in [unclear]. It's fascinating when you see the results.

We just did a study for 10 customers for three months. There was 8000 anomalies they are getting. The go through DNA Centre [unclear]. It came to roughly 1000 - 1200 issues. They are applying ML. When they do dynamic baselining, it dramatically changes.

When they talk about AI ML in networking, it is not about changing dramatically things. It's about using these as a tool to actually make a strong network in a lot more smarter way. [Unclear] efficiently with lot - fewer people. It's pretty fundamental.

We thought the next examples were interesting. We are moving through - traffic is getting encrypted everywhere. Encryption is a must, privacy is important, but then again when you look at cyber threat they're all using encryption as way to hide their malware.

How do you balance identifying a malware, and how to you satisfy the privacy concerns of company? What we do is we actually do mission learning as way to identify threats that is hidden [unclear] the traffic. We can do it in a way without violating, without [unclear] the traffic. We can understand what is inside with very high fidelity we can understand and say what the threat in cyber is. It works by collecting data, sending into the cloud with a threat intelligent infrastructure where we analyse.

Let me talk about what type of a data we are talking here. There are basically three type of data used to do this work. We take things which are unencrypted – there's enough information that we send that out per packet. Second, we look at how the data packing is working. How long the flow is happening. The gap between the packet, the size of the packet, the distribution. We collect all those data. These are all fingerprint.

These are all signatures for different interactions. We send it to the cloud. We combine that with all the threat interventions and all the different work we do in the cloud.

What this [unclear] is very fascinating. It allows us to, without [unclear] traffic. We can identify what is inside. We can say, oh it's a Google search, it's somebody's trying to update their browser. We can also understand the threat inside. When they look at MO, we absolutely need MO for security in this new world. You need security to understand. You need the MO to understand the different patterns. This is just one example of applying MO for security. Without this, it's very difficult to do.

We go to the third instance of how we use AI. This where mission reasoning come into play. We talk about mission learning. Everybody talk about mission learning all the time when they talk about AI. It's one of those branches of AI which gets talked less which is mission reasoning. In CISCO we use mission reasoning. This is where we come to automation. This is where we talk about how we capture human knowledge, and how we use it to run the network. We look at the network has all the information we need. We had the visibility. We also have knowledge. It's about how to deal with the problem.

There is an issue how do I find out humans know how to do [unclear] it's a workflow. There is a way you debug in IT. It capture all of them. They have a mission reasoning engine that runs inside DNA centre. It allows us to capture all this knowledge as rules, as [anthology]. We have these rules created by CISCO. We have in the cloud DNA centre you can download. Now you can apply them in the infrastructure. You can do two things. You can do guided remediation or you can [unclear] issues. It's very powerful because it's very hard otherwise to replicate the knowledge base that's there in every organisation.

In CISCO our rule is to find ways to capture that. We have tools internally we use. There's an editor which allows you to tell what you're trying to do when you deal with the problem. You have the ability to convert that into anthology. You have the ability to download from the cloud, so it can be [unclear] by all of our customers.

When I talk about the need for digital network, you cannot do what we need to do without these kind of tools. In another way, business is digitising everywhere. It's fundamentally changing the role of network. It is becoming one more time a critical part of the infrastructure. It's part of the business. It is the business.

Within the network that [unclear], we need to be data driven. It need to be automation driven because the need for built-in security. It's time for us to re-imagine networking.

Thank you.

**Manek Dubash**

Thank you, Ravi. Now I'd like to invite Jerry Caron from GlobalData and his panel to come down and talk with Ravi about where we're going next with this. Jerry Caron and the other two members of the panel.