NETEVENTS

2016 GLOBAL PRESS SUMMIT

Conference Debate IX - Analysing the Analysts: What They Heard, What You think

Chair: Manek Dubash

Editorial Director NetEvents

Panel:

Erin Dunne	***Director of Research Services, Vertical Systems Group***
Andrew Braunberg	***Research Vice President, NSS Labs***
John Fruehe	***Senior Analyst, Moor Insights & Strategy***
Paul Jackson	***Principal Analyst, Digital Media, Ovum***

MANEK DUBASH

We're going to talk about what we've talked about. Interestingly - let me just very briefly run through the agenda, the stuff that we've talked about over the last couple of days. We started off by talking about artificial intelligence. We discussed that in the context of security amongst a number of other things. We talked about the Internet of Things, will there be enough bandwidth, can you make any money out of it.

Talking of money, there was a lot of focus at the end of the sessions, the last couple of sessions of yesterday morning, talking about - obviously we had the shark tank so entrepreneurs, can they make any money out of their start-up ideas. We talked about unicorns and today we've talked about - we had the presentation from Dell, talking about Dell reinventing itself from a - if you remember the start-up just being a company that sold PCs.

We've talked about who's going to win the cloud wars. We talked about who's going to make money in the carrier space. Which of these things, which of any of these things, all the things that people have talked about, have really stuck in your mind and

resonated do you think will carry weight in the future. Erin, since you've been on your feet for the last…

ERIN DUNNE

Do you want me to start or do you want me to end?

MANEK DUBASH

You can start.

ERIN DUNNE

I'll start. So I come away with this with two very, very simple topics, one which I just discussed, which is as every minute we take an application or a process that used to sit in the wiring closet over there and stick it up there, that network, whether it's wireline or wireless becomes so critical. And we as an industry have to do everything that we can to make sure that those networks are resilient, flexible, affordable and ubiquitous. That's my first.

My second one, which might be a little more humorous, which may or may not, which is I feel like I'm under attack by something at all times. From the entire first day all it was was security; everything is being hacked all the time and we have to be vigilant. That's what I got from it.

MANEK DUBASH

Yeah, of course. They're all trying to scare you [laughs].

ERIN DUNNE

They're all trying to scare me and I think I need to go secure stuff.

MANEK DUBASH

Andrew, why are you trying to scare us?

ANDREW BRAUNBERG

Do you really want me to answer that?

MANEK DUBASH

Go ahead.

ERIN DUNNE

Go right ahead.

ANDREW BRAUNBERG

I wish I wasn't here to scare you, honestly. It sounds very whiny but the security guys are always the last ones to come in, right. It's making money - there's been a lot of conversation about making money on some of these new technologies. The leading question isn't: 'let's make sure these are secure technologies and then figure to how to make money out of them', it's always: 'let's figure out what the revenue stream is and then see what kind of hit we take on the backend trying to secure them'.

I think we've had a fair amount of conversations about things that look very promising from the ability to be more cost effective for a couple of years, but the further you get into them, the more troublesome they start to look. So I think the Internet of Things is one of those topics. It's probably the one that resonated most with me. The Internet of Things is to me the internet of doing things, so it's that ability with all this instrumentation and monitoring and controls out here in the world to not just monitor and collect information but to take action on that.

I think the internet up to now when we think about security around the internet, it's mostly around confidentiality, right. It's this idea that we're protecting our privacy and we're protecting the confidentiality of our intellectual property. But the two other main legs of the stool for security folks are the integrity of the information, to make sure no one monkeys with it, and the availability of the information.

Yesterday, it's interesting, we talked mostly about ransomware in the conversation we had, and that's about availability; that's someone coming in and keeping you from actually getting access to your data, which is troubling. But when we move to Internet of Things it's really the integrity piece that everybody's got to be thinking about.

When we think about - well, I should say it's the integrity and it is the availability too and I'll gave a couple of examples. Certainly availability of medical device information becomes, and not in a ransomware sense, but in effect if you could actually block the flow of information from a very critical medical device that's being used in a hospital. But the bigger problem is this idea, and it came up quite a bit in the…

[Interruption]

ANDREW BRAUNBERG

Keep going? Okay, yeah, good. I might have lost my thought there. I was talking about integrity; I was talking about the availability. I had a great point that I was getting to there.

[Laughter]

MANEK DUBASH

Take a break in your head for a sec and let's move to John.

ANDREW BRAUNBERG

And move it down and I'll come back.

MANEK DUBASH

Come back to that, yep. John.

JOHN FRUEHE

I think the best phrase that I heard over the two days happened this morning when somebody said, IoT is going to become a world of one-cent devices and you can't secure a one-cent device. That ultimately says all the security is moving over to the network. At the same time that that happened - I think, Erin, you just said that as more networking moves up into the cloud it becomes more important - but I believe as more networking moves into the cloud, the physical networks that we deal with can become stupider. They can become less important because I'm going to rely on software to drive this and my hardware doesn't have to be as robust, and that changes the dynamic pretty dynamically.

ERIN DUNNE

It changes the entire paradigm because you have service providers generating billions of dollars a year and they don't want to be commodity [unclear] players, they just want to jump over you.

JOHN FRUEHE

Exactly. Those service providers - and it ties back to security. Some people when public cloud first came out they said well, I don't know if I trust somebody like Amazon to protect all my data, and instead of the three guys that I have in my shop who are actually in charge of security, I can deal with Amazon where there's 80 or 90 people that think about security all day long. So suddenly, as they become more viable for security and can provide a more secure environment, can they also provide a better networking environment?

MANEK DUBASH

Paul.

PAUL JACKSON

Well, unsurprisingly as the AI guy I liked the conversations we had yesterday morning around AI, the security aspects of AI but also some of those wider questions of where's that going to go. I think some of the other topics, particularly IoT, is both going to be an application for AI with autonomous vehicles, smart cities, but also thinking about all those one-cent devices, a massive source of those training datasets for AI that we're just going to feed into neural nets and get things out the other end that we're not anticipating, some that we might like, some that we might not like, but something that will definitely change how we think about our interactions with cities, roads, medical professionals, things like that. That was probably the highlight for me. Also, I thought the unicorns discussion was fascinating, because who doesn't like a nice fairy tale.

MANEK DUBASH

Absolutely. Any particular technologies you think that we're going to be talking about over the next - let's say foreseeable future, maybe three or four years - that we've touched on today? Any thoughts?

ERIN DUNNE

I'll toss that down if someone else wants to start, or I can.

MANEK DUBASH

Andrew?

ANDREW BRAUNBERG

I'll jump on. It was actually yesterday, but to follow on from Paul, the AI bit I think is just going to become a huge benefit. We could get into whether some of the downside potential as we move down that road, I think we did a little bit yesterday. But I think short term it's got huge application and security is just one aspect of that.

MANEK DUBASH

Yes, it's really, really exciting that we're actually going to discover stuff from data that we didn't know was there. John?

JOHN FRUEHE

I think the AI was very interesting, but as always, I want to take a different perspective, which is massive datasets for AI are very interesting and will get us some great

breakthroughs, but think about smaller datasets and smaller AI and think about your phone and some of the things that you can do there. So AI becomes part of personal life; AI becomes part of everything that you do and devices have the ability to get smarter about how you engage with them.

MANEK DUBASH

Have you got any examples in mind? Do you have any examples in mind?

JOHN FRUEHE

Well, no, I haven't patented them yet so I can't say anything.

[Laughter]

JOHN FRUEHE

But I think the phone, the phone is a great example right off the bat. I have a Chicago accent and when I start talking it starts to sound a little funny, but my phone can understand. Now, down the road my phone should be able to understand when I'm saying you've got to close the garage door and then close the garage door, where my wife or somebody else who has a different accent won't be able to walk in and be able to do those same things.

MANEK DUBASH

Well, as a Brit using mostly American-made devices, I have a similar problem.

ERIN DUNNE

I'm sure.

MANEK DUBASH

Paul?

PAUL JACKSON

I kicked off with AI, so I can't say AI. I think some of the stuff we talked around drones was very interesting. It's a space that I've looked at from a consumer side as something which down the road becomes very engaging. And I think one of the other areas that we haven't talked about in terms of content flowing across these networks is going to be the spaces like AR and VR where we're now getting the devices which will very quickly be ramping up to 4K resolutions and we're already seeing a bunch of the

infrastructure providers say wow, that's great, we can upsell people Fibre Connect, we can upsell people better bandwidth and more reliable bandwidth. So I think that's something that will become an application and usage of a lot of the technology and security we're talking about.

MANEK DUBASH

Yes, I bet the telcos are really looking forward to four times the data.

ERIN DUNNE

Right, yeah. I guess I'll sound like a broken record again, but the technologies that - the question was what are we still going to be talking about. We're still going to be talking about the virtualisation of the network and there's tonnes of technologies that are out there, there's lots of forums and associations that are designed to make that easier and more seamless. So I'm not even going to talk the regular technologies, but it's the virtualisation and the software defining of those networks to make them more agile to handle all of these new technologies that we're talking about, whether it's AI or drones or whatever it might be.

ANDREW BRAUNBERG

I would jump in on the back of that one. After being at VMworld a week or two ago, I really - NSX is really the micro-segmentation use case for NSX right now is just driving a tremendous amount of interest for security practitioners, that idea of really being able to segment east-west traffic is a huge problem that needs solving right now. This year I think was the first year where they really - VMworld really had a really representative set of customers, reference customers that could really talk through how they're using it and the advantages [unclear]. So I think it's really made a lot of progress in the last 12 or 18 months.

Audience Q&A

MANEK DUBASH

Questions from the floor? You've got some brains here you can tap and some copy you might want to write.

Yes, there's one.

GUY HERVIER, INFORMATIQUE NEWS

Guy Hervier from Informatiquenews in Paris. It's more a comment than a question. You just said that - it seems that we're becoming a little bit paranoiac about security and we talked a lot about security yesterday and AI applied to security, but there is no single day where there is a big story that come up with something about security. It has been confirmed today in several magazines that 500 million accounts, of Yahoo accounts, has been hacked by someone with a state behind it. So this is another story and tomorrow there will be something new. So we'd better be a little bit paranoiac and do what we have to do about that.

MANEK DUBASH

Anyone want to comment on that?

ANDREW BRAUNBERG

I can't argue with that.

ERIN DUNNE

It's not my space.

MANEK DUBASH

As long as a computer is connected, it's going to be, you know.

ANDREW BRAUNBERG

I guess I could - one thing I could say. I totally agree with that, but you did see some folks here this week and it was an interesting mix of security guys. This idea that we shouldn't give up on trying to do protection but we really need this detection, fast detection and remediation, quarantine, limit the damage, assume breach, I think is where everybody had moved to.

You're right, no one is safe, there's just these monster breaches that become really commonplace. It's just a matter of locating them, identifying them and trying to shut them down. That idea of once you land and expand and there's this lateral movement within an organisation which goes back to the micro-segmentation and why that's so critical right now to try to limit the amount of movement folks can make once they get a [unclear] [hold] in your network, so that's important.

MANEK DUBASH

Well, just a thought as well. We've all said that it's the wetware that's the problem when it comes to security. So automation has a role to play here and it seems to me that AI also has a role to play in automation. Are we seeing any of that yet?

PAUL JACKSON

You're seeing AI automate a lot of very, very dull jobs. Arguably, some of those dull jobs are the very ones that can lead to those wetware breaches, because it's security guards or it's factory-floor workers who if somebody says here's a USB pen, why don't you just go and plug this in and they'll go oh, okay, yeah. So in that way it will, but it also means that all that stuff that was previously in people's heads that may have been secure, working knowledge of systems, security systems, is now in the AI; if the AI is breached then the door is wide open. Given that that this, as we were discussion yesterday, it is a black box, you may not even know that the AI is compromised for some way down the line.

MANEK DUBASH

Scary stuff.

PAUL JACKSON

Again.

[Laughter]

MANEK DUBASH

Any more questions? Look, you're terrifying Erin.

ERIN DUNNE

[Laughs].

MANEK DUBASH

Any more questions? No? Okay. Well, if that's all the questions, any final points any of the panel wants to make before we close up?

ERIN DUNNE

No. Thank you. Thank you for a lovely conference, it gave us a lot of great information. Thanks to the audience.

MANEK DUBASH

Thanks to the audience and thanks to the panellists and everyone for making it a great event. So thank you, one and all. That I guess marks the end of the panel of the plenary session. I think we're probably going to get a slide up that says next event, stuff like that, obviously breaking for lunch. Here we are. We've got Hong Kong in April, Portugal in June and back here next September I guess. Yeah.

Okay. Now we move to lunch and then scheduled briefing this afternoon. So it's been great, it's been real; thank you very much for coming along, lovely to see everyone. Bye.

[Applause]

[end]