NETEVENTS

APAC CLOUD SUMMIT

First Draft

"For Every Cloud an Iron Lining"
Addressing the Security Challenge

Tim Dillon

Research Director Asia, Current Analysis

Panellists:

Amit Sinha Roy	Vice President, Marketing & Strategy, GES, TATA Communications
Jatin Dhawan	Senior Consultant, Professional Services, BT Global Services
Bryce Boland	Vice President/CTO, Asia Pacific, FireEye
Hongwen Zhang	Chief Executive Officer, Wedge Networks

I'm going to invite Jatin from BT, wherever he's disappeared to, Bryce from FireEye and where, is Amit from Tata, ah always down the front. We are going to have a little bit of an open panel discussion in a minute or two. However, yes there we go, right two minutes of blah ladies and gentlemen, a little bit of a scene set before we get to a much more interesting panel, because we've actually got -- this panel was interesting to me because almost, in fact we should have done it side by side so we could have the Telco's and the Security Vendors squaring off against each other, because we have an interesting mix here and I'd like to explore that dynamic a little bit more.

The thing for me though around security is are we actually looking at the right thing. What do I mean by that? What I mean by that that in the last, as I said with our discussion with Hongwen, in the last two years or so the security environment has changed dramatically both through a motivational perspective as well as an information perspective and what hackers and others are now looking for. And I'm not sure if anybody has had the chance to read it, but very late last week PwC released a global security report. And it's actually worth a look. And they looked at various regions so they did a global version, a vertical version, in fact they tried to do every single thing that they could with it. But they really did try to address a number of particular issues.

And the thing that is interesting and we'll get to that say in a minute, but if you try and quantify the cost of a security break, it's very hard to do it's very hard to do. There are some studies that suggest a public disclosure of a breach will knock up to 5% off an organisation's share price. You have others suggesting that Sony's outage back in 2011 I think it was for a month cost them $171m of lost revenue. There are other figures that suggest a breach in a private cloud will cost to remedy depending on the size of the breach around $9m etc., etc. The cost per record, so for an employee record, seems to hover around the $200 per employee mark. The cost of losing a customer record seems to sit around $220 per customer. And there is lot of money to be now in this environment.

Several years ago Verizon did a very interesting security demonstration where they'd actually set up a live honey trap. And it was credit card information and they captured the scene and shortened the sequence somewhat considerably, but actually showed the output of the Visa and the Master and the credit card information which then I as a buyer if I wanted to could segment by country, by age, by sex and by pre-packaged credit card information in that environment absolutely fascinating [the way] it's going.

And the influences have changed significantly, and activism, state-sponsored security activity all of those areas are now, if you talk to government officials around the world and I don't mean to just point a finger at China, but if you look at the activities and the DSD in France for many years has been well-known to be targeting corporate and other governments, the Australian Government is currently in the press for a slight with Indonesia, so for any Indonesian's in the room I will apologise for that. But there are a number of influences now that from a motivational perspective have changed significantly.

That's a bit of a given, so let's have a look at Cloud and we are going to talk a lot more about that, that's the focus of our panel. All I would like to say to you right now is the technology environment that I'm about to walk through up to a certain extent underpinned by Cloud technology and services delivery and that's where I want to go. So we are going to do this, I hope you can read that at the back it's a little [Gilbert] cartoon, but this really is reflecting upon the impact of consumerization of IT.

Dustin talked about shadow IT and the influx of technology from a consumer perspective into the organisation. We did a survey recently that actually looked at mobility and spoke to organisations in Asia Pacific and said do you have a policy around mobile device usage, BYOD and I -- yes, and off the top of my head I can't remember the exact number now I'm getting old, but it was a relatively low number of organisations actually approving of BYOD use. Then we asked the same question [to more] are your employees using their own equipment either mobiles, laptops, tablets whatever they are in the office even though you've said no and the jumped to about 80%.

So organisations have this influx of consumer technology into their environment, and it's very difficult to deal with, it's very difficult to deal with and there's issues around policy requirements, there's issues around security and governance which brings us somewhat neatly into mobile. I pulled up the Android icon only because everybody

picks on Android its fragmented etc., ra, ra, ra, mobility though is a problem for many organisations.

Do any of you have auto-updates on applications on your Smart device which is always the precursor to don't raise your hand in case I pick on you, but if you do turn it off, turn it off, whether it's an IOS device an Android device or Blackberry or a Windows 8 device is secondary to this discussion. It has been well researched and well proven that even though you may have an auto-update on a legitimate application second, third, fourth update is fine the fifth will contain the vulnerability that's injected onto the phone, it's common there's in-app purchases now that will contain vulnerabilities. In other words the device environment is incredibly open.

We get all fixated upon this from a mobility and a security perspective, yes there are problems. I'd probably suggest to you that when I talk to CIOs around the region most of those problems though are not so much the mobile device security environment it's the fear of the auditors coming in and causing them even greater problems. And the number of companies that are actually ticking the box around MDM and all those sort of things simply though you can go to the auditors and go yes we have an MDM solution in play.

Where it's more interesting is mobility and a SIM in embedded mobile devices, so let's talk about NFC or machine to machine for a minute. If I look at machine to machine grown in Europe and North America and more recently in Asia Pacific it has absolutely accelerated. India is doing a lot, China is doing a lot there are -- Korea already is, Japan already is, Australia is following suite, M2M is a massive, massive environment. And it is an area where organisations kind of forget about security, and that is going to be a big problem is you listen to the numbers of internet of things and them seem to vary depending on the date, the time, the year, the month, the cycle of the moon and what mood I was in this morning, but 30, 40, 50 a trillion devices whatever the number is going to be not many of them are going to be these sort of things, they are going to be machine to machine style devices and NFC and they are not very secure at the moment and that's a major problem for many organisations.

And then the last area is third parties. Now I just want to give you a couple of scenarios to consider about this. The easy one is contractors coming into your organisation, so if you talk to example hospital groups here in Singapore and Australia and elsewhere you have groups that run a number of hospitals. Into those hospitals come consulting surgeons with a mobile device of their own and that contains patient data, it contains notes, it contains information that under health regulations should be secured. The trouble is those consultant surgeons, I'm a consultant surgeon so I'm going to go to Jatin's hospital then I'm going to go on Hongwen's hospital, then I go to Amit's and then into Bryce's each of those groups has a separate security environment. Anybody that's dealt with a consulting surgeon knows that they consider themselves close to god and therefore go I don't care about you people it's my device I'll do what I want, so you have a vulnerability there, third parties coming into the organisation.

Let me give you another example of a third party vulnerability and this is starting to happen a little bit in the regions, certainly in Europe and North America, organisations that have built large Cloud, private Cloud computing environments and let's say they've had a change in their business environment which means they have their little bit of spare capacity within their private Cloud, so the Cloud is within their firewall, are going out to the market and saying you people I have some Cloud capacity spare, do you want to use it. And suddenly you've brought a third party behind your firewall and that is a massive area of pain for many, or potential pain for many organisations.

So these are some of the changing factors that we see when we talk to enterprises around the region, which really begs the question do we need to look at security in a different way. I apologise for the graphics, if I was going to do marketing they would have been a lot better, but I'm not I'm an analyst. But the point about this is activism, state-sponsored yes, social is an interesting one. Israel actually cancelled a particular military operation last year I think, or the year before, because somebody tweeted about it ahead of time and they went oh no we won't do that and backed off. Social is a tremendous area of both threat and opportunity.

Consumerization [inaudible] extended, but Cloud this is where I want to finish because I think we need to start looking at Cloud a little bit differently when it comes to security. Cloud is both a concern and an enabler of security, and Hongwen started to touch on that and that's where I would now like to I guess bring it to the panel. And perhaps Bryce, actually no sorry we did plan on this but I'm going to change it just on a whim, Amit, Tata is a traditional services provider which is a bit unfair because that is loaded with all sorts of negative connectivity and that's not the case. But where do you see Cloud fitting for Tata from a security perspective?

Amit Sinha Roy

So if you look at our current service that we have, which is a public Cloud services to compute that's available clearly the Cloud strategy is inherent in our growth strategy. And from a security perspective we've actually looked at every aspect, every layout of security when we have created that service as well as we deliver that service starting from the basics of physical infrastructure security right, I liked the camera on your first slide. So starting from that through to actually securing the facilities, the employee access so that's one layer. Then the actual infrastructure which we have rolled out in terms of making sure that the [hardened door] is right up to the virtual machines is there and we take of all unnecessary add-on software that could actually become potential threats, through to making sure that the access, the administrative access is secure, because a lot of times that's how you get the vulnerabilities introduced into the system.

Going forward in terms of having the ability of network security through to even offering private NPLs [on-apps] for customers who really don't want to go into the internet to access. So we look at multiple areas and we've tried to address each of these. And where standards exist like IS20, 000 27,000 we have applied those [70] and so on and so forth and we try to adhere to those. So from a service provider perspective these are the various aspects that we've looked at in terms of the basic

Cloud security, Cloud service, public Cloud service that we have. And then there are also other services like DDoS security but I won't touch upon those right now.

Tim Dillon

Jatin, from BT's perspective is Cloud an opportunity or a threat for your customers?

Jatin Dhawan

Definitely an opportunity, definitely an opportunity and moving forward as BT provides infrastructure to services [move on through] the platform and software to other services there are different service components in the different service models. So I think there is a different set of requirements for every -- for different service delivery models that's the first thing. And customers are coming back to negotiate contracts and SLAs to accommodate security to put in requirements as well, so that is the way forward. I think as a service provider well definitely there are always exclusions but it should [inaudible].

Tim Dillon

So does BT pay up on a breach that's my question, the minute you said SLAs on Cloud security are you going to cough up if you have a breach?

Jatin Dhawan

That's [the certain] thing we are moving forward to mature the security space in the Cloud.

Tim Dillon

Yes, doesn't answer my question does it? Sorry Jatin I did say I wouldn't pick on you. Let me come at this a different way then, because if I think about what both of you have said isn't securing the Cloud, let's say if I look at identity management for example, isn't that a bit old school technology isn't that sort of the traditional approach? Amit, what do you think?

Amit Sinha Roy

I think it's getting the basics right as well, so we need to have those building blocks in place before we move forward. So I agree that it may sound old school but it's necessary to have because otherwise anybody could access and change things around and be able to actually get into systems areas where they are not supposed to so from that perspective it matters. And even basic things like if we have a customer setting up an e-commerce site, so making sure that the web server and the data base are two different virtual machines so if it gets compromised you [don't lose] your data, those are basics which have inherent goodness in them and we don't really want to discard them because that just exposes the system.

Tim Dillon

Bryce, Cloud is it -- how does all that sit with you from a service provider perspective considering FireEye perhaps has a slightly different approach. So first question I guess is opportunity or a problem the Cloud from your perspective?

Bryce Boland

So, in my previous role I was responsible for enterprise security strategy in a major global financial services organisation, and I can tell you that we look at Cloud as being the great enabler of security. And it is in many ways but it also requires us to change the way we think about security, and I think that's the fundamental thing.

When we look at the capabilities that we require as an organisation to protect our users, our data, our applications and our infrastructure they are going to be relatively complex. We know that all of the vulnerabilities that exist have been created by people, and these are people who are trying to do their jobs but they are also trying to create code and designing applications that may be flawed that's an area we need to focus on.

We know that they are designing the new generation of infrastructure and the service providers are going to be providing those, but these people will also make mistakes. They are going to be administered by people who are also trying to use social networks and trying to use the latest mobile devices to get their job done more efficiently, so we know that we need to look at the people aspects of the problems as well as the infrastructure components.

In terms of security and the Cloud though I think the Cloud creates some great opportunities to enable better security. If we can put the appropriate security controls and detection the right sensors everywhere in the environment, everywhere where it's going to matter to give us detection of new threats and enable us to push controls out in a dynamic real time manner, that's going to give us much more effective security. Being able to detect new threats and use that information and share that intelligence dynamically and in real time will enable us to secure the Cloud much more than we can today where desperate enterprises implement different controls and don't share that information in a real time manner.

Tim Dillon

So I want to pick up on a couple of phrases that you use there one is more effectively and the other is better, and Hongwen was suggesting that there is a place for third parties effectively in the Telco network. So does that mean that the service providers have it wrong or they are not robust enough or where do you fit within that approach?

Bryce Boland

Well I believe that today there is a number of security capabilities that are quite difficult for service providers to roll out. FireEye is a provider of one particular technology that provides detection of zero-day attacks and [connect into five threat actors] trying to attack your network. But today most service providers actually make

more money selling lots of other band-aid solutions, traditional legacy solutions like Firewalls, IPS and these produce a lot of false positives and unfortunately enable them to then spend -- acquire even more money by providing investigation and breach clean-up services.

So I think that actually a partnership between the best of breed technologies in the security space with service providers and leverage information about breaches that happen anywhere in the globe with all of the service providers enables us to provide better security for all organisations.

Tim Dillon

Amit, I have to ask you on the basis of what Bryce has just said is it the case that Tata is making more money cobbling together a bunch of solutions and a bit of consulting and is focused more on the dollars than on effective security solutions? Is that what Bryce just said to me, I'm not sure he was suggesting that?

Amit Sinha Roy

No, no not at all, so in terms of our Cloud offering we've secured it like I mentioned across the various layers. But having said that I must also put this on the table that the customer who actually creates an application and puts it onto that Cloud and then puts its onto devices and takes it out in the market would also require to secure that application or the roll-out of that, because that is not an area where we control at this point in time.

So from that perspective I think what Bryce is saying across and using Cloud as something that touches every aspect of security is -- well there is a value proposition there, but from an infrastructure perspective that's where I was coming from we've secured that, but once you create the application and take it out then that's a different point.

Tim Dillon

So the pair of you are going to get together and charge me more is that what you're now saying to me this is going to cost me even more now?

Amit Sinha Roy

I thought his software was shareware.

Tim Dillon

Its open source you can probably copy it from somewhere, it's not a problem. Hongwen where do you, or where do you as a third party come into BT or Tata and help them make more money, because at the end of the day we are doing this to commercialise. And it's not always easy to make money out of security, and perhaps we you've addressed that after Hongwen, Jatin if you could give your thoughts on that, but can you help the service providers make more money?

Hongwen Zhang

Absolutely, I think that if you look at it and these two gentlemen from the good service providers already outlined the issues.

Tim Dillon

Hang on; are you selling to these guys already?

Hongwen Zhang

They already outlined the issues we face every day. They already got so [many] work to do, they still had to do the work and maybe that becomes just another added task for them to do. So when we talk about Cloud as opportunities, opportunity of what, we've got ask this question. So you go to talk with any of the CEOs of the tier one service providers and your service providers they face two challenges. One that they got to keep their customer, so they [could] reduce the charge, the other is that they need to increase the [RAM] [inaudible] which will increase ARPU. Those are the two key fundamental goals of the service providers. And if security is not working on that direction I don't think that's an opportunity and hence it has to be a particular breed of security that works in this direction that can bring the opportunity to the service providers. You guys can correct me if I'm wrong on this.

Tim Dillon

Jatin you're deep in BT's security group.

Jatin Dhawan

Yes, I think it's very right it might be a little --

Tim Dillon

Sorry, just a bit closer to that mike, yes perfect.

Jatin Dhawan

I think it's absolutely right that security is a matter of concern today and many, many organisations are not moving to the Cloud for the reasons because of the security regulations and the requirements come from the compliance etc. So it becomes very important and vital for the service providers to establish practices and capabilities to ensure that the security is also well taken care of at the same time while we are providing you these services. So I think it's very important going forward and it could be embedded I think into the overall process.

Tim Dillon

So if we stay on the topic now, specifically around the Cloud, a lot of discussion this morning that hybrid seems to our end point for Cloud but I suggest that's probably true, doesn't that make it both from a service provider perspective and an enterprise customer perspective a much more complex and difficult security environment?

Jatin Dhawan

Well, with the Cloud computing I think for organisations it's very important to understand the network boundaries, to understand where the data is and enforce the security controls accordingly at the provider side as well as the organisation side both. So for example when I am outsourcing as an organisation I'm outsourcing or moving one of my businesses process to the Cloud provider I must understand what are the implications of that in terms of regulatory requirements etc., and what are the data security requirements and what is the responsibility of an organisation and what are the security responsibilities of the service provider. And I think these must well negotiated in the contract with the service [inaudible] manager.

Tim Dillon

So are we starting to butt up against the argument around on-prem or off-prem?

Jatin Dhawan

Yes, well I said all different kinds of service deliver models require different security requirements, demand different security controls. Definitely a private Cloud hosted in my own premises would definitely not need that much security controls which -- if hosted in that different public -- in a private premises.

Tim Dillon

True. Amit, we've had these sorts of discussions before what are your thoughts?

Amit Sinha Roy

I think to answer the question that you put up first in terms of hybrid I think it's a matter of choice and the choice is led by cost and scalability, the ability to scale typically what --. And the decision that needs to be taken is what is the information that is completely -- has to be completely kept within the enterprise and what can be shared or put outside. So those are some of the decision factors it's not something that we do with data that can be residing anywhere, so that decision in terms of the data policy and information policy is critical in terms of what's going to be private and what's going to be public.

But having said that one of the points that Jatin just mentioned in terms of if we take our applications and -- if an enterprise takes its application and hosts it in a service provider environment is it necessarily less safe, I wouldn’t agree because in many cases the service providers have far more sophisticated controls be it all the various elements I talked about so I won't repeat it, than enterprises because enterprises may not actually be looking at their data centre with the kind of secure practices that service providers have been doing naturally over a period of time. So from that perspective certainly I would say that the data is as safe or probably more safe with a service provider. But let me talk about the other aspects. When you open it to the public then what happens?

Tim Dillon

Bryce [inaudible].

Bryce Boland

Can I just -- I just -- I would champion there with -- I think any point of aggregation of data of something of value is going to be of greater interest to people that want to take advantage of that information or that value. People don't break into banks unless there is money there. If they do break into a bank and there is no money there they obviously haven't done their due diligence. But in general we see attacks taking place against organisations and data centre's repositories that provide real value. And that means that a service provider becomes a natural aggregation point.

And as people move their processes, their business value chains, their most important data and even in the case of a bank the information is the money and I think you all understand that. As that information is sort of aggregated under a single point of control in a major service provider that service provider becomes subject to all of the interesting interest of the baddies who would be otherwise going for the individual organisations.

So instead of it being the potential value of corrupting a single bank or a single law firm which might have M&A information or breaking information about a legal case it becomes all of those organisations together. And for that reason I think as a service provider you have yes a greater investment in security but your threat profile is significantly greater and requires a real level of attention to detail, and continual maintenance in terms of the evolution of the threat which is extremely difficult to continue to provide.

Tim Dillon

Hongwen, what are your --?

Hongwen Zhang

Yes, I think that to answer the question is that hybrid Cloud solutions is here to stay and that's actually in the very spirit of Cloud [elastic] computing is the key thing of hybrid Cloud to actually stay there. Now certainly that creates tremendous challenge in many levels and one is that you are currently the service provider providing service to one of your customers, you have customer go to the hybrid Cloud it actually means that business goes to someone else, the other thing is that really the privacy issues that we all pointed out.

And if I can draw another analogue anyone heard about organ transplant, you all know that it's a tremendous [standard] your body will kill those [internal] things right, and we want to from a security perspective, we want to make sure that if the hybrid Cloud is being adopted by any organisation they are really two issues. One is make sure that we actually have the security measures to make sure they work together not cause any privacy data leakaging issues. The other is really make sure that [there is a] standard together to allow them to work together so you don't have the antibodies

killing the other part, which is typically happens when you have an over-strung security and your business continuity got impacted so that's our view.

Tim Dillon

I'm starting to feel nauseous about this now. Ladies and gentlemen we have a few minutes left, does anybody have a question. Can you wait until the mike comes please? I know you can yell but --.

David Heath, IT Wire

Hi, David Heath from IT Wire. With the focus we are having on moving security into the Cloud are you suggesting that endpoint security is doing it too late?

Hongwen Zhang

Can I take on this one?

Tim Dillon

Absolute yes.

Hongwen Zhang

So basically that I think that as a -- typically as a technologist I find myself sometimes insensitive to the real needs so I have to rely on statistics to actually to demonstrate real need.

Tim Dillon

I wouldn't [go with these] analyst firms.

Hongwen Zhang

And so here are the statistics we read, there is according to all of the prominent research organisations basically point out 53% of mobile users to not like to have security software installed on their devices. And you know that it drains your battery and you also know that when the signature updates start happening, I'm not talking like FireEye had a different approach, but if the signature based update happening it drains your band rates so that's the laws of physics that go against the [only] device management. There are certain areas certainly it can be done in a -- on the device management but I believe that really the only way to be effectively doing it is at the network level.

Bryce Boland

Just to add to that I think putting controls in place at the network level gives you a level of coverage that is very difficult to achieve on the end point, with building any kind of security control to work on all of the mobile devices, Mac OS, Windows all of the various variants of Chrome OS now that is extremely challenging. What we do see though is organisations focusing on the things that actually matter to them in terms of

business impact. This is things like the theft of data, the loss of intellectual property and how that impacts on their bottom line and their competitiveness in the market. From that perspective I think we are going to continue to see a focus on mechanisms to protect data and most of that data has to flow to an end point through a network. If it's coming from a corporate network that's probably where you are going to provide most of your security controls.

Amit Sinha Roy

I would like to just comment on that, that it's not either or it's got to be both right, because if the end point is compromised however good the network security is the data can bleed out right, so I think it's got to be both.

Tim Dillon

Jatin, do you wish to --?

Jatin Dhawan

Yes, I think apart from the controls as you mentioned in terms of the network security controls and the -- and controls at the end point security device itself another important aspect I think is the awareness of the various risks and these must be explained to the user community as a part of the ongoing security program this is quite important I think.

Tim Dillon

That answer it for you David?

David Heath

[It's a start].

Tim Dillon

A start, alright grab them afterwards. Anybody else got a question for our panel? Oh two at once, stop that. Sorry so the gentleman from Verizon we will get to you I promise but if we can come down the front first.

Mr Mohammed Kamil, Telekom Malaysia Berhad

Hi, my name is Kamil from Telekom Malaysia Berhad. I have been asked by my colleague do we know what we don't know. In other words we need to know what we don't know i.e. looking beyond firewalls or IPS and stuff like that. From a Windows perspective why is your -- what you can offer on this.

Tim Dillon

There's an extra 10 points for anybody that can do a Donald Rumsfeld impression and do the whole known knows and unknown known's. Do we know what we don't know?

Hongwen Zhang

In 2010 I made a speech in the IT [inaudible] so I could use that analogy because actually we don't know what we don't know. But there is some advantage we can refer into, and there is very good, in the scientific community there is the very good little book called the networking and the breaking science of networking I think that's the name of the book which draws strong analogy of all the networks in the world and the typical situation they face.

And so we are not the only ones that had build the network, network had built the network for longer, very, very long time so we can draw a lot of inspiration from that. And the other thing is that if we focus on the fundamentals and the fundamental is really we all have our business to run and we have to make profit and we have to take care of sales. And that will provide a way to look at things not from the hackers point of view but look at what you -- the organisations true need is and then put the difference there that's the answer I can give to you there.

Tim Dillon

Anybody else want to take that in terms of where security is going?

Bryce Boland

I would add that there is a fantastic network effect from sharing intelligence, and the first time an attack happens the first time we see a new threat that's the opportunity to share that information and make it available to others so that they can then act against that new kind of threat.

One of the things that we know from the FireEye labs is that more than 90% of the malware that goes into organisations is unique, it's only ever seen one time. But that malware is unique because it's been encrypted with a unique key for that particular attack. The actual code itself is usually -- had it been compiled specifically for that attack but its underlying it's the same technologies the same code.

So having seen that first attack, having identified the exploit, being able to share that information in real time to many organisations is the way to be able to protect them in real time from those new threats. The intelligence that's out there is enormous, we just need to find better ways to leverage it and share it so that we can protect everybody.

Tim Dillon

Sir?

Mandeshpal Singh Banvet, Verizon

Good afternoon, Mandeshpal Singh Banvet from Verizon. So my questions is maybe two-pronged one is what do you think the market size between on-prem and [inaudible] security and the second part is how big a movement do you see [in security] moving from on-prem to Cloud-based? Thank you.

Tim Dillon

Why are you all looking at me, I do qualitative analysis I don't do market stats Dustin Kehoe from IDC does that.

Hongwen Zhang

Definitely that's a question for analysts for sure, but I want to just --.

Tim Dillon

Massive is the answer how is that?

Hongwen Zhang

So we read reports and we are seeing that depending on where do you draw the boundary, because if you look at it security and the networking on the Cloud patch is everything. And for the particular industry that Wedge Networks is looking at is still called the Cloud managed security and it also touches -- and devices all those things, and I real fairly conservative information talking about I think the Infonetics talking about $18b by 2016or something so it was a fairly big amount. But consider that Cloud secure -- the Cloud initiative I read that statistic this morning is about $200b and that's a proper percentage you should spend on security for sure.

Tim Dillon

Was there a second part with that question or was that the totality?

Mandeshpal Singh Banvet, Verizon

The second part was how big a movement do you see -- the second part was do you see a big movement of [expanding] security from on-prem into Cloud-based?

Bryce Boland

Let me just quickly touch on that. I think in the organisations that we are selling to we are increasingly finding organisations moving some of their processes into the Cloud just as normal part of business process outsourcing. And one of the things that we've certainly seen from a security perspective the email service providers are starting to become much more popular, so a lot of people moving to Office 365 for example and that creates some new challenges for security. As well as the bandwidth issue it actually makes it very challenging, you're relying now on one particular vendor to provide your security capabilities for that. So I think we are starting to see that shift happen. And no doubt that's going to accelerate.

Tim Dillon

I think at this point ladies and gentlemen we might draw a line under the session. Let me leave you with perhaps an almost not answer to your question about market sizing. The PwC study which I referred to which came out last week suggested that in Asia Pacific 4% or just under 4% of the organisations spend on IT is devoted to security.

That seems a little bit low in terms of perhaps they are not spending enough. And the second comment is around, specifically around Cloud security policies. Only 18% of the organisations in Asia Pacific actually have policies in place around Cloud security according to that research.

So I'm going to take a leaf out of my previous mobile service provider's approach and blame the customer and say that they are not doing enough and they are not spending enough at this point, and there is a tremendous upside if they were to raise that number a little bit and start spending more on security.

If you could please show your appreciation to the panel for giving up their --.

[End]