NETEVENTS

APAC PRESS & ANALYST SUMMIT

First Draft

Debate II: Protecting the Enterprise Means Protecting the Cloud and the Network - Where's the Opportunity?

Chaired by: Nikhil Batra

Research Manager, Telecom, IDC

Panellists:	
Andy Solterbeck	Regional Director - APAC, Cylance
Ashok Vasan	Vice President, Digital Transformation - Asia Pacific & Japan, CA Technologies
Brendan Leitch	Director of Marketing, Asia Pacific, Ixia
Peter Lunk	VP of Marketing, Menlo Security
Frank Wiener	VP Marketing, Wedge Networks
Sunny Tan	Head of Security, SE Asia, BT Global Services

So we just spoke about the fact that our enterprise is ready for cloud. But in a way trying to talk about is the cloud ready for enterprises? How secure is the cloud today and are the cloud service providers ready to provide enterprises with the safety and security that they are looking for.

So not to get any funny ideas; it's still a security session. But how many of you know about this or know what this is? I see not many people around here because this is one of the most controversial online dating sites. It's banned in Singapore and a lot of countries around the world. So this is the landing page of that website, which says life is short. Have an affair. So this website was hacked last year. So I'm going to talk about a few security breaches last year and then the panel can chip in, saying how enterprises can protect themselves from these things happening.

Now what happened was that this website was hacked. And this is the whole timeline. So around 37 million accounts were hacked. And the hackers then threatened that

they're going to release this information publicly, which they indeed did after a month. And this information included the names of the subscribers, which included the big CEOs, CIOs of all the companies and individuals. And it was all the information was available on the internet, which talked about who these people are messaging, what are they messaging and you know where this is going.

And as a result, a lot of companies, CEOs stepped down. There were a lot of class action law suits against this particular Ashley Madison company, so much so that they rewarded – they announced a reward for $500K, $500,000 dollars for somebody for sharing information on these hackers. But nothing really came out of it.

One interesting stat that came out, one of the security companies, they laid their hands on all of this data on 1st September. And they claimed to have broken down 11.2 million passwords within 10 days. And surprisingly enough that the most popular password was 123456, which was 120,000 accounts in this database had this password. So that just makes us think that how secure is a service and how much should cloud providers emphasise and provide security to the enterprises?

Now there was a time when this was the worst thing that could happen to us. A malicious code or a bug would result in a blue screen of death and we would just restart our PCs and get on with it. But now we are getting into an era of IoT and connected things, where things like the connected car is being hacked. So these two gentlemen, Charlie and Chris, they hacked into a Jeep Cherokee late last year. What they wanted to show was that all of the connected things today that we have, be it a refrigerator, a smart refrigerator or a smart edge-ware controller or an air conditioner controller, they're not secure enough. We have had phishing incidents where the email has been coming from a smart refrigerator, for say. So who would actually have thought that?

So what actually these guys did was, now imagine you're driving down a highway and you see a – so suddenly a blast of cold air, at the maximum temperature throughout your vents, and then the radio switches on to a local hip-hop channel with full volume blaring at you, you try to spin the control left to stop the radio. Nothing works. You try to switch it off. It doesn't work. And suddenly the wipers turn on and the wiper fluid blurs all of your vision.

So in a normal scenario you would think this is a scene out of a horror movie, but this is actually that something happened and then the worst happens, that the transmission and the accelerator stops working. Now the gentleman who was driving this as a part of this experiment had to drive the car into a ditch to avoid an accident on a US highway. So this just takes us back to the question that when we are talking about connected cars, we are talking about relinquishing our control into the hands of technology for the sake of convenience and for the sake of having all parts of our legs connected to each other. Security is a big part of it.

And now there have ben incidents of drones falling out of the sky. For those of you who follow US Open, this was an incident out of the last year's US Open, where a drone fell down during a live match. Now this was dismissed as a, I don't know, it was dismissed as a normal incident, something that wasn't really investigated a lot.

But what could happen with this if these drones are hacked into? This could be a whole new level of insecurity that we are heading to.

So with that in mind, I'd just like to highlight that the security solutions over the past decade or so, they have shifted from a reactive to a proactive approach. So it's not about just your end user devices. It's not about having an antivirus on your PC; it's about protecting your own environment. And with cloud and IoT coming into picture, the security is moving away from the perimeter. It's moving into the cloud and now there's a much more, much larger audience of the devices and the networks and the cloud servers that we need to provide.

So with that in mind, if you see here, these are the investments in the four technologies. And the investments in cloud, mobility, big data and social, I'm not sure if you can read the numbers or not, but down below are the largest investments. And all of the investments in these four pillars is into the security, privacy tools or your administrative privileges control. So with that in mind, let's just take a place today that, starting today, all our passwords much contain letters, numbers, doodles, sign language and squirrel noises, just to be safe.

So with that in my mind, let's welcome our panel here. So we have a lot of people from security service providers to service providers, telcos here. And I'll let you gentlemen introduce yourself once we get into the discussion. So we have spoken about cloud services making the whole security complex – security landscape a lot more complex and more vulnerable, in a way. But what you have seen is that some service providers claim that it's for the good. Ultimately this is making the whole environment more secure and enterprises can safely move to a cloud and not be worried about all of those things.

So I'd like to get your thoughts on it. Andy if you will start.

Andy Solterbeck

So thank you. And the session before I think was a really interesting introduction to the topic. By the way, Andy Solterbeck. I run Cylance in the region. Cylance, by the way, is, if you think about us, we're kind of the crazy man that they described before. Three years ago what people, what we were represented as doing, people thought was completely crazy. We now have over 1,000 customers and 4 million endpoints under management. So we're all about doing something fundamentally different.

I do not question for one second that how we are doing security in the cloud is orders of magnitude more sophisticated than an enterprise can do. There is no question. The ability to bring on the right staff at scale with the tools, all that kind of stuff, fantastic. Unfortunately, the approach is fundamentally not working. If you look at any measure right now in relation to the number of attacks, the success of those particular attacks, this approach is not working. So why?

It's not that the cloud is not secure; it's that we've forgotten about a fundamental part of the attack surface. And that's the endpoint. 95% of all attacks start at the endpoint. And today we've forgotten about that and we've forgotten about prevention. So fantastic they were doing work in the cloud. Awesome. Great technology, really

believe in it. But as an industry we've really got to step up to protecting against the entire attack surface to really mitigate the attacks.

Nikhil Batra

Okay. So that makes perfect sense. And Ashok, we spoke about digital transformation during the breakfast, that how cloud is one of the primary ways of driving digital transformation. It's one of the technologies that is powering digital transformation. So do you think that the cloud is secure enough for the enterprises? Or what do you see when enterprises approach you, talking about cloud adoption? And do they feel that it's secure enough?

Ashok Vasan

Yes. My name's Ashok Vasan. I'm from CA Technologies. We have a broad suite of security software, which is designed to enable companies, deliver their goods and services in a more secure environment. So that's the context of who I am and why I'm up here.

But more specifically to the question around digital transformation and how cloud plays into it and whether the security aspect is taken care of, I think the notion of cloud becoming available or usable by enterprises is well proven and documented as the earlier panel talked about, no doubts. There is regulatory restrictions to a large extent. And therefore what we're seeing today is really a hybrid model, which I foresee will continue for a little bit longer, somewhere between on-prem private cloud to public cloud. It's going to be a hybrid model. That's the first point.

The second point is the vulnerabilities and the entry point into all of these areas are multiple. And what therefore becomes important for us to manage, be it cloud or otherwise, is the identity of the people who are coming in. And all those examples that Nikhil talked about, it essentially boiled down to the hacker being an individual, either an employee or contractor or perhaps an outside party.

So the cloud has progressed tremendously in terms of restricting access and control. But there is also a sense of responsibility that falls upon the service providers as well as the users of it to make sure they build in sufficient protection into the kind of services that they're using. Identity becomes very critical. Privacy of public data becomes important. And I think it's really a combination of the cloud service itself being secure as well as the applications that are running on it being coded to make it secure.

Nikhil Batra

Right. That makes perfect sense. So one of the tenets of digital transformation is the work source transformation or empowering employees to access the enterprise resources and wherever they want, whenever they want, to whatever part of enterprise they want to get into. So as Andy spoke about earlier, managing the end user devices is something that's really important. Securing those end user devices is something really important.

So if, Brendan, you would like to share your thoughts on that. Where are we with that?

Brendan Leitch

My name's Mr Leitch. I look after – Head of Marketing for Ixia and the Asia Pacific region based out of Hong Kong. I've worked out here for quite a while. I'd like to make a very granular, specific comment about are enterprises ready for cloud and the services in the cloud and the security. One of our core businesses is ensuring visibility into what's on the network for performance management and security tools.

We are very clearly seeing that large enterprises, for compliance reasons, security reasons and performance management of their applications reasons are requiring very granular visibility, particularly in compliance of business-critical apps. When you move something into a cloud, you lose the ability to control that visibility. So for business-critical applications that are core to the business, whether it's financial transaction processing or whether it's your core skills, core transaction traffic and e-tailers, no, they're not ready to put those in the common cloud, full stop.

Maybe you outsource HR system to Workday. Maybe a little saleforce.com. But your transaction ledgers, your back-end Oracle computing if you're an e-tailer on your application delivery front end to your back end, your SSL decrypt systems, or you're managing the security of your users into your front-end and your back-end systems, no, I'll take a clear stand out there. Not all of these things are ready for the cloud. For those exact security reasons, you lose visibility. And visibility is the core to being able, for a CIO or a CTI or CTO or a chief digital officer to say to his bosses, the CEO is on the hook, yes I know what's going on in my network or no, I don't know. So I just wanted to come out fairly strident on that point.

Nikhil Batra

Right. I think that nicely explains the point that we, when we always talk about technology, we don't just talk about technology. We talk about people, process, technology, everything together. And this forms a part of it.

Now one of the leading service providers released their data breach investigation report. And to quote it, it shows that the most vulnerable point in any organisation is privileged identities that have [root] or rewrite access privileges. And because of that, implementing – you need to have these in the system because there are people, there are network administrators, they are the CIOs, they are the hands-on CIOs who need to have this access to have the visibility of their network at all the times.

So, Peter, if you would like to share how does this fit into the end user device management and how do you think we are – or are we managing these devices correctly today or successfully?

Peter Lunk

Yes. Sure. Just by way of introduction, my name's Peter Lunk. I'm the VP of Marketing for Menlo Security based out in Silicon Valley. And it's an interesting point. We have customers that actually, when they start, they trial our product, they

start with those privileged systems folks that have access to everything. If there's anyone you want to lock down, it's that team of people. We've seen that again and again.

And if you look at some of the problems on the security side that they run into, it's the same thing. They have two primary threat vectors that are coming in with these people getting infected, whether it's a CEO, whether it's someone way down on the shop floor, they're getting infected through the web and through email. And whether those are hosted in the cloud, whether people run them as cloud service or whether they're running traditional old-fashioned services, it's coming in through the web and through email.

And so having a prevention system in place, I think Andy touched on it around the fact that prevention has been broken over the last years. We've seen people rotate to I need to do more about detection, fast detection and fast response. And I don't want to diminish those efforts. They're helping. But the fundamental problem of people getting compromised and these high-value targets that you talked about getting compromised needs to be fixed through improving the prevention capabilities and keeping those accounts and those people safe.

Nikhil Batra

Okay. So you spoke about fast detection and fast resolution, day zero, day one for vulnerabilities. Now, as we see, there are two kinds of threats out there. One, the known malware that we have that all of the service providers claim to protect the enterprises against. But then there's the unknown out there that we don't really know. The organisations don't really know what's hitting them. So it's imperative for enterprises to know how to go about selecting a service provider, how to know whether this service provider is good for me or how do you differentiate that or how do you say that who to partner with. Frank, if you would share your thoughts on that.

Frank Wiener

So absolutely. My name is Frank Wiener and I lead marketing for Wedge Networks. And Wedge provides a security platform that's fundamentally software-defined and virtualized so that it can run at the cloud layer of the network.

And touching on that point and the point raised earlier about are enterprises ready, I think the answer is larger, more sophisticated enterprises are definitely ready. As you go down from the largest enterprises to the more medium and smaller type sized organisations, they lack the skilled resources to really understand and appropriately prepare and manage that. And most of them don't recognise or don't fully understand that.

The threat landscape has changed, and I know Andy mentioned the surface is changing. And most of the security initiatives have been oriented to securing users inside the enterprise. And that's fundamentally – it's much more sound. But the reality is the enterprise, the boundaries have dissolved, right? And they're not just

using their PC; they're using their tablet, their mobile phone. They're borrowing a friend's laptop and they're accessing content in the cloud.

And so what's become apparent is security needs to move from an enterprise orientation and even – we can't limit it to just specific endpoints. We need to move it to a cloud layer as well. Obviously you need endpoint-type security, but there has to be a cloud layer of security for these connections that are happening outside of the enterprise, with devices that aren't under the control and administration of the enterprise.

And when you think about smaller and medium-sized businesses, how do they do that? They don't have their own cloud to implement security at that layer. So what we're seeing is a tremendous initiative with service providers, who are providing connectivity services to offer security at that cloud layer of the network as a service for both large enterprises but primarily small and medium-sized enterprises that lack the sophistication and the resources to do that on their own.

Just last week, a start-up here in Singapore, their CEO unveiled a major cybersecurity initiative and the creation of a cybersecurity centre of excellence, with – part of the objective is to offer those types of services to their customers here in the market.

Nikhil Batra

Okay. So coming to the security service providers, it's a logical extension for them to offer a secure connectivity, partner with a security provider, partner with a tech vendor like you guys, to offer a secure and inherently secure network. So, Sunny, I'd like to get your thoughts on that, that when the enterprise customers approach you, how is the discussion about security? Are they asking for it, because BT is doing a lot. They are partnering with companies around this. Or is BT going out and saying that, okay, these are very secure?

Sunny Tan

Yes. So by way of introduction, I'm Sunny. I take care of the security business for BT Global Services in the region. And you're right, the connectivity customers that BT has typically expect certain amount of security to be built into the connectivity products that we sell to the customers, that we operate for the customers. But increasingly we are also seeing customers approaching us directly for security problems that we have.

So as some of you alluded to earlier, I think the attacks they face is changing. Obviously as a global telco, we see a lot of it in the connectivity parts of it. But inside of the so-called perimeter, below the WAN layers, we are starting to see dissolve – the perimeter's being dissolved and we have mobile devices with convergence of cloud and mobility. IoT is one thing that stood out very strongly as well, customers coming to us, augmented autonomous vehicles, that sort of thing.

So we are also leveraging on our partners. I think half the table here is probably the current partners of BT in our quest to improve security for our customers. And we also built some of our own platforms, to look inside our own network which our

customers' data actually traverse in to see what sort of information that we can get from it using data science and that sort of thing. So definitely we do see a fair bit of security considerations coming through a global service provider like us.

Nikhil Batra

Okay. That's interesting. Do we have any questions from the audience at this point? Okay. So if I just continue. You touched a bit on IoT. So let's move from cloud and mobility to IoT and the connected things, the connected car we spoke about. So when we are at a point when we are relinquishing our control from control into autonomous vehicles and things like that, it's imperative that the security is in place because otherwise it could be disastrous. So do you guys think that we are ready for these technologies or we are ready for these technologies to come into our mainstream lives? Anybody can take this. Okay, Frank?

Frank Wiener

So I'll jump in on this one. The answer is it's a challenging problem. And when you think about these IoT devices, they're very limited on compute power and memory and those types of things. And they're infinite in variation. So right now it's a growing concern across the enterprise markets. We're actually working with some of the service providers. If you think about IoT, it's either connecting to your mobile device or your LAN via a wireless connection, or it's connecting to the cellular-type connection and connectivity.

And so what we're doing is we're working with service providers to provide IoT security again at the cloud layer because those devices are either coming through the broadband connection or the mobile connection. And the service provider is in an ideal position to have visibility to be able to inspect the packets that are flowing to and from those devices, inspect the kind of communication and ask is this a databased communication that should be occurring to this mechanically oriented type device or is it uncharacteristic and does it represent any threat.

So there's a lot of work going on obviously in the industry around IoT. But we're seeing a lot of interest in the service provider community to offer security as a service for IoT to augment and try to address some of those gaps that are going to exist in most enterprises.

Andy Solterbeck

Totally agree. And I think that's a valid approach. But just consider this again. Once a piece of IoT hardware has been compromised, the fact that you're doing monitoring up and back, it's too late. So the challenge in IoT is exactly as you said, Frank. Limited resources, very – almost consumer-scale construction, so not a lot of memory, not a lot of CPU, not a lot of those environments. And also an environment where, quite often, they're disconnected. So how do you manage an environment and secure an environment that looks like that? And in the end, we have to actually construct technology that allows us to be embedded in those endpoints that actually can mitigate against the attack of malware. It's the only way we're going to get there holistically.

Once again, we need to protect the platforms that support them. We need to protect the networks. But we also need to actually specifically create protection mechanisms on those devices themselves. And I think that's the big challenge for the industry. Do we really have detection techniques that are effective and efficient, because they have to be incredibly efficient? Can you imagine downloading a 400-megabyte DAT file to an IoT device? That's just not going to happen. We have to have a fundamentally different approach. So I think it's a big challenge for the industry, but one I think we're starting to see some early signs of good adoption.

Ashok Vasan

I actually think that we're a ways away because the definition of IoT is not yet – we haven't comprehended it in its entirety. Case in point being a television today is an IoT, which is actually running its own version of an operating system as an example, just purely as an example. And the connectivity to those kinds of devices are through traditional means, which were just discussed earlier. So the point of vulnerability extends right into the operating system in certain cases, which we've not yet fully comprehended.

And this is happening because the traditional owners of either these devices, networks or operating systems are changing rapidly. Android didn't exist very many years ago. Now it's all over the place. TV operating systems are now in every home. Large organisations like General Electric are now coming out with their own operating systems and stuff. So we've got a ways to go before we get a full handle on it. And I think the vulnerabilities will exist as long as some sort of critical mass is not established and adoption reaches some stage where we can then build that layer on top of it. But we have to keep working towards it.

The other fundamental point that's happening is enterprises are opening up. There's this whole API culture, which is what is driving a lot of this digital disruption. And that's another entry point which is opening up third parties, external developers, where somebody within an enterprise has to decide what they are exposing to. And it's voluntary because it's a new business model that they do want to embrace. And in that whole process they could inadvertently open up their enterprise, whether it's through the cloud or whether it's through other points of entry. But APIs are going to become another point which needs to be very, very securely managed and governed because it's both a necessity as well as a point of vulnerability.

Brendan Leitch

I'd like to unravel your question into two discrete questions. You mixed up a couple of things here. You said IoT and cloud. Let me pull those two apart first. We as a test and security test company, as one of our core competences, are absolutely seeing certain verticals take on IoT fairly aggressively. Specifically those are medical device verticals in the hospitals, in Japan, in Germany and other developed countries. And what they are doing from a security vulnerability perspective is because there's big money in that, they are taking on the testing of the endpoints. They're taking on the testing of the services, driving the connectivity. They're taking on the testing of that.

We're also seeing a couple of big airports in Asia which are doing that to control airport departures, aircraft departures, baggage and stuff. And they're investing heavily in literally when the plane backs away from the gate, it's a thing in the airport's intranet infrastructure and it records that it's left the gate, things like that. These kind of verticals are heavily testing that stuff. And they extend into heavy testing.

The other one is we're also involved in the car testing. I'm just bringing that up because you mentioned it. And they're very cautious and conservative. If you talk to BMW and Toyota, they're going on to only the audio system in the car first and making sure that's not vulnerable before they get into anything beyond that, let alone car telemetry. So audio bridging is being tested first, so we're seeing that going on.

To get to the second question about the cloud, do we see these said people, like these specific verticals, like medical and car and airport operations, which is logistic ultimately, outsourcing that to a cloud, relying on the security in the cloud? Those CIOs aren't signing onto that. Not a hospital CIO and not a medical device, x-ray or iPad guy in a hospital doing medical records, putting that on the cloud yet. So I just wanted to separate those two mixed-up things there because I think they were a bit mixed up.

Nikhil Batra

You spoke about BMW and going into the audio systems first. But that's exactly where these Jeep guys got into. The whole electrical or the electronic components of the system is they are interconnected. So even from a manufacturer's perspective and from a user's perspective, they are two separate systems, but when you talk about electronic transmission and this running on the same platform or basically running on the same infrastructure, that's where these hackers are getting into it. So that is an entry point for hackers and that's how they have been doing this. So I think from what you mentioned, having a visibility of whatever's going on and having a visibility of all the connected endpoints is really very important in this case.

Just when we are on the topic of IoT, let's get some other views on how important is testing for IoT, security testing for IoT, because again, if it was a normal system that we are talking about, if it was like a server that dies and it just affects the uptime of an organisation, there might be revenue impacts. But when you're again talking about connected things and autonomous vehicles, you're talking about potentially fatal accidents that could happen. You're talking about human lives that could be affected.

So then it takes a different shift. The conversation goes in a different way. You cannot go in a cycle and say that, okay, let's try this first, and then when a vulnerability is exposed then we'll work on it and then we'll go like this. So what are your thoughts on this, Frank?

Frank Wiener

We've actually been working with some of the folks who are managing power grid and water control systems and things that – if somebody takes over a dam and opens a

dam through an IoT-controlled system, there's a lot of implications, as you're saying. And so definitely there's been a lot of scrutiny around that.

As Brendan mentioned, they're very focused on testing and validating the individual devices and the security and robustness of them. But we've definitely seen a lot of focus on trying to address those critical infrastructure things as well as those, like automobiles and those types of things. We've been involved in tests with that as well. And they're looking both for the traditional vulnerabilities of is malware coming in through the IoT to go infect other systems, but also is somebody hijacking the control of that IoT?

And so what we're seeing is a focus not just on the traditional security vulnerabilities, the traditional malware, but actually they're looking at what are the communications that are occurring to that device. Are they consistent with the set of actions that they want to authorise that device to take on? So there is a lot of growing focus on this and there's some industry initiatives around this more broadly. But it's definitely an area of – it's evolving. It's growing. It's not mature. But people are jumping in. And they're doing a lot of testing of the systems in advance. But the answer is welcome to security; it's constantly changing, right?

Andy Solterbeck

So all I've got to say though is fundamentally, whatever processes and systems were used to set up the current critical infrastructure approaches is not working. We've just released a report called Dust Storm, which was a low and slow hack of the critical infrastructure in Japan. So that entire infrastructure was compromised. So while I fundamentally agree, we have to test, we have to be conservative, we have to take it step by step here, we do have to fundamentally shift the approach that we're using from a security perspective.

To rely on the historic mechanisms and approaches we've been using for the last 10 or 15 years, for all the reason we've talked about, attack surface, different vulnerability assessments, we do radically have to shift the approach we're taking to security as an industry because at this stage, to a large extent, the approaches we're taking, historic approaches we've taken have failed. They don't work. So we do need to reinvent and reinvigorate the entire industry, from the cloud all the way through to stack.

Ashok Vasan

Just a quick comment and I'll pass it on to Brendan. The physical limitation to testing, it's very important, but there is a challenge. And the reason why it's not doable is two reasons. One is we're not able to conceptualise what kinds of testing needs to be done. So it's a matter of test coverage and figuring out whether it's – the second thing is the physical cost in some instances, like the example that you talked about. In the early days the analogy I would give is aeroplane testing. You had to build expensive wind tunnels, which itself was expensive, but the alternative to it was actually physically flying the aeroplane every single time to test it, which is just not practical or business-feasible.

So the approach that people are taking now from a testing perspective, not just for security purposes but even for overall functionality of an application, is virtualise those environments so that you are simulating, like a wind tunnel would simulate actual flying conditions, you would simulate the environment, whether it's a medical device, whether it's a water regulation device, whether it's semiconductor testing and so forth.

So virtualisation becomes a very critical element in how this testing could be taking place. But then you've got to then back it up with actual test scenarios that are going to mimic the kinds of security breaches or the kind of functionality you were expecting out of the application. So those are just a little bit of insight on how people are – the challenges people are facing and how they're overcoming it.

Nikhil Batra

I think Brendan will have a couple of points when he says that we can conceptualise.

Brendan Leitch

Well, as a test company, I have more than a few points.

Nikhil Batra

Go ahead.

Brendan Leitch

The short answer to your question is do you actually test? The answer is absolutely, yes. Okay? And those in our traditional customer base which we've evolved from, which make devices, don't ship anything without testing. Every security device maker in the world tests, not with us, but they test before they ship. That's the same thing that's going on with enterprises and IoT. Enterprises that care about their business test.

But let's not leave it as a platitude. Let me break that down into three discrete components for everybody. And two of them are obvious. One of them is quite often missed though. Devices under test, that's where you take whatever you've got in your architecture and you test the device, is it a firewall, is it intrusion detection, is it layer two, layer three switches at a WiFi access point? You test the device. But no network or no business runs on a single device; it runs on a whole collection of devices, from load balancers to WiFi access points, to firewalls, to intrusion detection things, to everything in the mix. You test the architecture as well. So you start with device under test and then you have a systems which is your architecture. And you test the overall architecture. That's number two.

But we preach that that's not enough because, with all due respect to somebody on this panel who's going to dispute my point, you will still end up having a breach. Even if you have device under test properly done, as best you can do it, and you have system under test, especially if you're a nice rosy target, you're still – somebody's going to invent a day zero vulnerability to go after you. And that's going to happen.

So how do you address that? You put people under test. And that's one of the things that we actually do as a company. We call them cyber range services, cyber testing services. But we go out and we say, okay, it's going to happen. How is your team? How is your security team? How are the people in your security operations centre going to respond when it happens? How are they going to figure out what's really going on? What are the plans they're going to have in place? And how are they going to execute against those plans? How quickly do they identify it's a fault attack or not a fault attack? How quickly do they figure out what it is? How competent is their team in responding and how quickly?

I'll give you an example of a major financial institution just to put a point on that. We're doing cyber range training services for a major financial institution in Asia. And all we did is we spoofed their website to make it look like it had been hacked. It had actually not been hacked. Okay? Just put up a screen to show them that it had been hacked, just to see how the CIO responded. They panicked. They said we have to shut down our internet banking. We have to shut down our processing systems. We have to shut down. We've been hacked. Hadn't been hacked. It was just a test of the people to see how they responded to it.

And so that's how you – that's the last level, not the last level, but certainly it's a level of protection you need to put into your people and your systems and how they're going to deal with it when it happens. And that's the ultimate thing in testing.

Andy Solterbeck

I've got a really quick one. Apologies for taking so much of the airtime. I totally agree. A breach will occur. Here's the question for most enterprises though. What you just described was a very sophisticated customer. And we call it the 1%/99% problem. 1% of customers have certs, have SOCs, have response teams, have sophisticated approaches to actually mitigating these attacks. Fantastic. Awesome. What happens to the 99% that's out there that don't have the ability to respond on those kinds of ways?

So I think what we, as said, once again, as an industry what we've got to start doing is arming those people with tools that actually allow them to get back to the preventative posture that we used to have before. It won't be perfect. Nobody's perfect. What we're trying to do is get away from the point where we are now where the approaches to malware, they're lucky to be 50% effective right now. And we've got to get back to the point of actually being preventative. That's the major shift I talk about.

Nikhil Batra

So I think Andy very rightly mentioned, and it summarises the session that saying security concerns are always going to be there. It's always evolving. The landscape is always evolving, so it's just about partnering with the right guys and making sure that they care of you.

But thanks a lot, all of you, for your discussion, and thank you.

[End]