NETEVENTS

GLOBAL PRESS & ANALYST SUMMIT

First Draft

Conference Debate Session 9:
The Next five Years
Strategic Planning for CIOs and CISOs

Vikram Phatak,

Chief Executive Officer, NSS Labs

Panellists:	
Alan Kessler	CEO of Vormetric
Andrew Lee	CEO, ESET
Brian Smith	CTO & Co-Founder, Click Security
Ian Foo	Director, Data Center Products & Solutions, Huawei
Jason Brevnik	Vice President Security Strategy, Sourcefire
Manish Gupta	SVP Products, FireEye

Hi everybody. So the topic here is 'The next five years - strategic planning for CIOs and CISOs. I've got a pretty good panel here, we'll get to them in a second.

Just quickly about NSS, we're an advisory firm similar to Gartner or 451, the difference being that we actually test products. So our core competency is, we started out as a testing lab and we've grown into an advisory firm. So in terms of what do we do? I'll just keep this really simple, we basically our rating products, rating technology based upon results in the lab and all of our analysis is fact-based.

So having said that we'll move on to the topic in hand. So Einstein said that 'The definition of insanity is doing the same thing over and over again and expecting different results.' So the bottom line here is that compromise at a company nowadays is no longer, it may make news if it's a big company but it's sort of a (inaudible) right? Everybody's been compromised and we all know that, so what are going to change? We've got a group of panellists here to talk about that and talk about where CIOs should be making their investments and so on. So Alan Kessler form Vormetric,

Andrew Lee from ESET, Brian Smith from Click, Ian Foo from Huawei, Jason Brevnik from Sourcefire and Manish Gupta from FireEye.

So one of the questions is, there's a lot of new technologies that are, you've been hearing about this is in conference and elsewhere, everything from cloud computing, SDN, virtualization and so on. So how is this all going to play out? So let's dive right into it here. What are the game-changer technologies for the next three to five years? We're wanting to hear some thought here. Anybody want to go first? Alan.

Alan Kessler

I'd comment that virtualization, cloud and even the conversation earlier today, software defined networking, the whole idea that the physical concept of the network is dramatically changing, those are a few.

Unidentified Participant

I think that one of the most exciting new types of technology we'll see is [IDEF] combining things like the internet and things with real-world networks as they exist now and typical infrastructures that we have, so things like implants for medical devices for diagnosis which send information on body biometrics or body metrics to a wireless device which can then inform your doctor or a hospital of your current state and those things. I think those are going to be some of the technologies that we'll start to think that will change things.

Unidentified Participant

I would also add the convergence of communications technologies with information technologies that we're seeing. When people are using information to run their business it's either access to the information to make a decision or exchange of information and collaboration that is driving the business. So I think that convergence is starting to change, some of the way we look at datacentres, support infrastructure and even information systems to support those. And I think we'll also see quite a bit of change driven across different parts of the network by consumerisation of devices and I think most IT managers and CIOs are beginning to feel that pressure today. I think that will only increase over the next three to five years.

Unidentified Participant

So I'll jump in right here real quick. SDN, virtualization, cloud, big data, they're all interesting technologies but the fundamentally enable analytics and real-time decision-making with context about your consumer or your partner, and enable our organisation to make decisions in near real-time about the changes they should be doing for both efficiencies and cost structures and stabilisations in prices and that kind of stuff. I think analytics will ultimately be the game-changer tech that applies to and wraps up all of these different pieces that enable real-time change.

Vikram Phatak

So from a bigger picture perspective there's lots of pieces that are coming together but the summary is it's about big data and analytics number one. Number two is that it's the Internet of Things, so you've got more places that data is coming from. Does that pretty much summarize? Okay.

Brian Smith - Click Security

Yes I think one additional comment on that is I think we're seeing the combination, security always comes in almost as an afterthought after utility and environments, and so what we're seeing is the combination of virtualization technologies, both network and compute virtualization, along with an explosion of devices coming into the network. Friends of mine that run university networks say that they're seeing 7 to 10 IP addresses associated with each student at this point between their Pandora radio alarm clocks and their cell phones and all the devices they bring.

The combination of all this is going to make traditional security controls very, very difficult to deal with because all our security controls are associated with IP addresses and physical devices and with the explosion of those things and the mobility of those things it becomes very difficult for those controls to be effective.

Vikram Phatak

That really leads to the next question which is how this technology is going to impact security for better and worse, and that was a really good segue Brian, so thank you.

Unidentified Participant

Vik I would say that, building on what Brian offered, because of virtualization, really standing back and looking at what are the bad guys after. Building a fortress around your network no longer works, everybody knows that, members of the panel here are introducing products to try and defend against it. The bad guys are inside, they already have access to your network, in fact you may have hired them. So now what do you do?

Our view is that you protect what matters, you find a way to lock down the data, you find a way to reduce the attack surface, so even if they're inside you can block them. And, quite frankly, with cloud virtualization your data might be somewhere else, so even you're confident that you're running your datacentre and you can trust your people, what if you data is in someone else's cloud? How do you know whether the systems administrator who is managing that server is someone you can trust? These are the some of the challenges and by focusing on the stuff that they're after or the stuff that they want to change, the data, that's a way to defend against some of these new threats.

Unidentified Participant

It comes down to having the visibility of where your data lives, where you IP is and where your people are and whether or not their activities fit with the actions that are

happening. When we start talking about sharing this information across industries and detecting the malfeasance and the attackers and their advanced methods, closing the time gap, today we're, I think the Data Breach Report from Verizon put us at, 100-plus days to close the gap from detection. I think fundamentally as this information sharing and analytics come to play we can close that gap down, we can close it to weeks, we can close it to days, for some organisation we may even be able to close it down to hours or minutes. That's when you really start understanding where your data is going, who is after it and how to bring the controls in.

While we have two conflicting priorities with the openness and consumerisation of IT and the ability to access date from anywhere, we have the virtualisation of networks and SDN and the ability to create business process controls that are above physical infrastructure. The information we achieve in consumer IT devices contrasted with our ability to change the way the network looks and change the way our services look in real-time, I think should allow us to bring them back together in some amount of time and bring those controls in without having a traditional border.

Unidentified Participant

So Vik, I just wanted to add to the point made earlier about the challenges in security. Since my focus is datacentre one of the things we're seeing is that with the level of granularity and fluidity afforded by some of the cloud computing structures, software defined networks and other technologies that are allowing flexibility and agility in the datacentre, the consequences of that are going to be complications and complexities in applying security policies in the traditional manners in which we're used to. Now we've got a whole a bunch of moving targets, some of the notions of how we'd apply security or segregate security no longer apply, so I think that over the next three to five years those will have to dramatically change in order to accommodate those newer environments.

Manish Gupta

Yes I would say that, look I think the fundamentally the biggest challenge that we have is that the CIOs and CISOs are almost at loggerheads. Because CIOs are incented to embrace the latest technology, we were talking about Wi-Fi, higher speeds, software defined networking, faster datacentres etc. and the CISO has the challenge of protecting all of these new-fangled ideas. CISOs are still struggling with technologies that have been deployed over the last 10 years, they still have to, unfortunately part of this challenge with security everything that I've deployed over the last 10 years I can't take the risk of throwing any of that out. So I think fundamentally what we have to be able to do in the security industry to help our customers, is to be able to make managing security easier and that has to start from not having to need 10 or 20 different products but a fewer set of products that provide far more actionable information.

Unidentified Participant

And increased visibility, absolutely.

Unidentified Participant

I think, I agree with what Manish has been saying, I think manageability is a key thing, but one of the interesting things that I see and I've been in the security industry a very long time, is the way that we have actually, in a sense you can look at it as if we have created a smarter attacker. That's actually, I think, a good thing because what has happened is, as we've innovated, as we've secured things, as we've been able to create more visibility into our security we have also forced attackers into further smaller and smaller corners, enabling them to come up with new types of attacks.

But what we've actually got a challenge with now is there's just so much data, there's so much information and there's so much noise and as we see more and more noise the challenge is trying to pick out the difference and the change in the noise that shows that you've got an attacker. I think this is one of the big challenges that we're going to have, when it comes to data, it comes to data management, how do you create layers of defence that actually allow you to identify within all the noise, the activities of an attacker, or the activities of someone who is doing something that you don't want them to do with your data. There are different ways of doing that and I don't think all of that is technological either I think some of that is educational because, as we have developed more and more technologies that enable us to catch infiltrations, the attackers have simply gone after the simplest part of the network which is residing in half an inch of [skull] behind it.

Unidentified Participant

Well that's interesting, and I think the panel would agree, that with state sponsored attacks they are well funded, they will out-fund any enterprise, maybe some of the governments around the world can compete dollar for dollar for talent and resource. So then what do you do? The idea of knowing what you don't know and big data and analytics and learning and sharing information is critical. Doing that more quickly, which I know some on the panel focus on, and then once you know that lock down the data and have a policy in place that's efficient, that's easy, transparent and doesn't require you to change your infrastructure.

Vikram Phatak

So Brian?

Brian Smith

Yes, so I agree with many of the things being said here but I have a little different view of it. I think for the last 20 years or so we've taken the approach as an industry of trying to armour the sheep and I think we need to start kind of hunting the wolves. We have tried to make the devices more secure by putting antivirus on them, by putting controls in the network that prevent breaches, and the fact is is the bad guys just figure out ways around those. To put the exclamation point on that, if you look at the Verizon Breach Report, the number, how people find out about intrusions, only 5% of them are detected from security devices. So of the $68billion that the industry spends on IT security they detect 1 in 20 of the intrusions that come out from those

devices. That is just a really, that says that that approach is not going to work. I think Jason and Alan are exactly right, is that what we need to start doing is looking for the anomalies data and the pieces that go to show that an attack is in progress and do that quickly enough that we can prevent the damage, so we can get out in front of this. If you see a sequence of events, if you see a gun being stolen followed by a robbery at a house you can predict the murder of the girlfriend in advance or the probability of that murder and get out in front of it and prevent that damage from happening. That's the type of predictive analytics we've got to get to. It's very, very challenging and in part it's challenging because of the lack of expertise in this environment. There are very, very few good IT security experts and that's one of the greatest challenges facing our industry.

Unidentified Participant

So that data point, 1 in 20, 5%, kind of supports that you don't have to run faster than the bear, you just have to run faster than you. Fundamentally it's an economics game, they want to make money and it's easier and cheaper for them to make money by hitting broad targets and having their goals and we're not making it difficult enough on them. As we close that detection gap, as we close the window of opportunity for them and make them change their business process then it becomes less profitable for the attacker and it becomes more profitable for you through less loss. The balance, of course, is going to be in a collective approach to solving that problem so that everybody is playing together in the field, not everybody trying to defend. If you try and employ small little regiments around the country and have them defend against a nation you're never going to get success right? You have to create an army of people to do this and that's the information sharing and analytics we need to bring to the table and have everybody participate in, in order to really put a dent in the economic process.

Unidentified Participant

I think that's true but I think we talk about it because we're in it and we see it and we know what should be done because we're already aware. The biggest problem that I see every single day is, most people just don't know anything about it so there people who are running five year old systems, unpatched, no antivirus, no firewall, nothing, forget all your, even your basic security controls just aren't there. Until people realise that that's really a fundamental part of the problem because that creates an opportunity for a stepping stone for an attack into your organisation, because every single one of those employees in your organisation is also a home user, it also someone walking around in the street and going into a doctors surgery and going to the car garage and giving their kids whatever on a USB stick so it goes into the schools, which comes into your university network, which goes into your enterprise research network and so on and so on. All of those things have to be taken care of, so there's a fundamental education problem right at the base before we start even talking about technology.

Vikram Phatak

And so what technology should we be investing in? You guys starting talking about it a little bit, but strategically, I know we've talked about this next budget cycle, but looking out if I'm a big enterprise and I want to see certain technologies because I'm saying five years from now if I'm going to have some of this stuff solved, where am I making my initial investment? Even though it's not perfect right now, what types of things should be doing?

Unidentified Participant

I'll jump right in there. We approach the problem set from a number of ways but one is focusing on technologies that allow you to interdict at various points of the attack chain and give you visibility into what's happening and allow you to bring some control. Fundamentally the business wants to answer, are the attackers here, what did they get, when did they get it, where did it go and what's my exposure? If the technologies you're investing in can't help you answer those questions or don't help you product a funnel to be able to answer those questions you need to rethink the investment. A lot of organisations today sadly do not have the ability to go back and see what was compromised when, they have the ability to take a phone call but, you know, some customer's credit card information is now out there and we've correlated to you organisation and now they're not able to answer how it happened. We need to start with that fundamental premise of being able to answer those questions and get technologies that can give you the visibility into how it occurred.

Unidentified Participant

Vik I would say, technology that allows you to implement policy, policy that allow your network to change, that will allow your data to move and still give you confidence that that policy in enforced. Something that scales, that's transparent, that's easy, that's strong and that, quite frankly, doesn't impale the performance of the solution.

Vikram Phatak

Why don't I give Brian a chance, just one question, one thought here which is ecosystem. So what's coming to mind from what you guys are talking about is having a technology ecosystem that supports the business as opposed to sort of retrofitting security in after that fact. Is that sort of that we're saying Brian? I don't know if that changes what you were going to talk about there but --?

Brian Smith

Well I'd think about not just the technological aspects of it but there's really three key things I think that CIOs need to invest in from a very broad perspective. One is allowing more information sharing. It's been changing, this attitude has been changing in the industry but people tend to be very secretive about their security threats and we need to, as an industry, start sharing that knowledge more because the attackers are essentially business that develop a piece of software and then they want

to make a return on investment on that software and they'll attack one company and attack another company and attack another company and walk on down the line. So we want to collapse that economy and the way we do that is by sharing what we're seeing in one organisation so we can get out in front of it and the other organisations. So sharing of information is number one.

Number two is developing the security expertise in professionals within your organisation. Most organisations where they get into security is they have an IT infrastructure and then someone says 'Oh we should worry about security' and they appoint one of the IT guys and say 'You're now Head of Security and by-the-way you haven't lost your day job.' So we need to invest in that training and education and professionalization of that group of the industry.

Then the third part, to Alan and Jason's point, is visibility, technologies that allow you visibility into how users are actually using the network, how users are misusing the network, those sorts of things. Once you have that visibility it begets policy and it begets effective policy and effective policy management. Without that visibility, if you look at the way people break into networks that's what they're exploiting, is the fact that the policies are ineffective because the IT guys don't have either the expertise to set correct policy or the visibility to know what the policy is that --?

Vikram Phatak

So let me ask this, it's not on this subject but it's interesting question, are we giving too much power to the consumer? Are we giving too much flexibility in their devices and they're basically shooting their own feet off? Is there a model that we would like, you know, take my iPhone here right? You have your App Store, you can do everything you want to do, but it's an ecosystem and it's meant for the purpose, it's a specific purpose-built device. Is that the kind of thing we should be looking at?

Unidentified Participant

I think you have to work out how you're going to manage that. Fundamentally I think you have to understand that every network is hostile, every network, your own network included, it's a hostile environment. So what you have to care about is what's happening to you data and do you care at the point at which something happens to compromise you, is your data still protected regardless of the fact that you're compromised? So you're in a dirty, hostile environment yet you still protect what matters. I think those are the technologies that we need to be looking at and those are not necessarily single point technologies and I don't think there's a one-size-fits-all approach to any security problem, it really comes down to what you look at in your risk profile. You might be a person who accepts more risk, if you like skydiving your accepting a certain amount of risk but you're hoping that the technology has developed enough to be able to protect what's important, your limbs and your legs and the piece of meat inside your head. That's important, the rest of it just has to work. But you might be very risk averse on the other side and so you might just never want to connect that specific piece of data to the network, ever, because that's important. So you have to find a balance.

Vikram Phatak

Okay, Ian and Manish are both chomping at the bit here.

Ian Foo - Huawei

So I want to quickly just go back to the recurring theme of visibility and policy applicability, the ability to enforce policy. Stepping away from maybe focusing on point technologies or products that do that, but making a more comprehensive approach to it and including the necessary support structures in even, like the infrastructure for example. Choosing infrastructure elements that are able to provide the information needed to add to the analytics, to tie in activity on the network aside from activity at the application level. So the ability for network infrastructure, selecting network infrastructure such that interfaces are available and vendors are supporting the ability to program policy flexibly into these advanced environments.

Vikram Phatak

So that's with respect to SDN and --.

Ian Foo - Huawei

Right, correct, so I think taking it one step below and making sure it's a comprehensive approach from the infrastructure up all the way through the analytics is really important.

Vikram Phatak

So we've got to (inaudible) the core protection and to your point about giving the user too much power. It's my belief that the user is your power, that we try and constrain them and impose policies and restrictions upon them that become so burdensome that they go outside of their scope in order to get their job done. An example would be an infected laptop that a sales person uses, at the end of the quarter he knows its infected, he knows its compromised, he keeps getting browser pop-ups but it's going to take him two days to get it back to IT, so he keeps doing business with this technology instead of being able to solve his problem keeping and continue moving.

Unidentified Participant

It can't get in the way of the users, it's an overwhelming force. Most, I meet with the Chief Information Security Officer a couple of weeks ago of a global payment company and he said 'Look if the business wants to run down the hallway with scissors in their hand, his job is to figure out how to help them do that and help them understand the risks and the trade-offs in doing so.'

Unidentified Participant

It's to remove all the cord from the hallway so he doesn't trip, but let him run.

Vikram Phatak

So Manish, you've been very patient.

Manish Gupta

Well I think I would largely agree that we can't put restrictions on users, that has never worked in the past and that will never work in the future. I do take a different point of view though from some of the panellist here, I don't necessarily believe that visibility is all what it is being touted to be. We read reports every day, all kinds of statistics, such as we're seeing targeted malware roughly every three minutes, what good does it do to me to have rather poor sensors deployed in my network that scream every three or five minutes 'Oh my hair is on fire.' First and foremost what we need to do is put more accurate sensors which tell me and wherever possible protect me and, yes, visibility can come later.

Brian Smith

So that holds if we assume that there is a human at the end of the loop that's directly taking that data feed into the network, which has been the model over the last several years. Provided that's true you're absolutely right, that's why intrusion detection systems are problematic, because when you deploy an intrusion detection system it immediately starts shouting all these alarms at you and so what most users do in response to that is that they turn off all those things that are shouting at them, all the signatures that are shouting at them, and they've completely lost all the signal that would give them alerting in this.

So what we need, where I think we're going to go with the big data analytic thing is we're going to see a shift where instead of that raw data feed we need telemetry feeds out in the network that gives us high quality feeds, not garbage, but that that is going into another system that is receiving all that data and piecing it together through analytics and raising meaningful actionable alerts to the end user.

Vikram Phatak

So playing devil's advocate here for a second, the stuff that's in my logs, isn't that the stuff that I was protected against? It's the stuff that is not in my logs that I should be worried about right? That's how I'm getting compromised.

Brian Smith

But every time someone gets compromised, if you go back and do an incident analysis on that, 99 times out of 100 they'll have a log management system in there and they'll find that all the evidence was there in the logs that have detected the breach in progress. There was no visibility into that and so you need tools that help you --

Vikram Phatak

So the first thing is that it's raining, you can't tell when you walk out the door it's raining right now, give yourself some sensors to tell you that it's pouring outside and we're getting wet.

Manish Gupta

Yes but it is a challenge though right which is, look, if we look historically pretty much every sensor that we've deployed to date, whether it's on the endpoint or on the network requires some sort of prior knowledge of vulnerabilities or malware. We therefore characterise it in terms of signatures, AV has been doing that for the last 20-plus years, intrusion detection, intrusion prevention tools have been doing that for the last 10-plus years. However what we're finding now is these targeted attacks are bypassing those signature centric capabilities, so first off we have at rethink our approach, we can't rely on these signature centric products. Now if we were to place sensors in the network that start feeding some intelligent information to a northbound console where I guess we could do some smart analytics, but at the end of the day those sensors are also signature based. Well guess what? There's garbage in and garbage out. So now if we take the other extreme and say 'Well now we're going to record every single bit that is on the network so that we can analyse it, the experts, to find out malicious events.' Boy, are we making this problem too complex.

Unidentified Participant

So I'll jump in as a vendor that has products that play in all of these places, the point of an intrusion detection or an intrusion prevention system is to afford you operational capacity to solve the other problems, to stop the known bads so that you're not spending all of your time fixing your network with things that you just don't need to deal with. Then you need to get into the advanced analytics and detecting the things that are targeted at you, but until you've solved the fundamental operational problem of keeping your business running, keeping your users happy and keeping the nuisance off their systems, then you can't being to hope to have the resources to solve the attacker that's hiding in the noise..

Vikram Phatak

So just to paraphrase what you're saying, I'm going to use my rain example because I like it, in IPS and AV it's like an umbrella right, so it's the known way that you're going to get wet, or the known way you're going to be attacked, it buys you the time so that you can deal with the stuff that's coming at you sideways and focus there. Is that it?

Unidentified Participant

That's a way of looking at it.

Unidentified Participant

But it's the stuff that's coming sideways that’s the most malicious.

Unidentified Participant

I think back to Manish's point is, if the attacker sees your holding an umbrella they're resorting to the fire hose. It's a known quantity right?

Unidentified Participant

But their goal is to get you wet, you at least need the umbrella.

Unidentified Participant

But look, I think there are very, very many real-world parallels here and I think Jason is right, there is a huge, there's a great prophylactic value in having a lot of these technologies in case they take care of the 99% of the threat of that we know about. The problem is finding the single threat. Unfortunately the real-world parallel, we saw it yesterday in London, the real-world threat is someone driving a car into someone and then hacking them to death in the street in a terrorist attack. You find out, you go back, you peel it apart, yes we knew this guy, we knew he was there, we knew what he was doing, we knew who was involved. The problem is being able to prevent every single attack is never going to be possible, it's just not. But what you can then do is to take the knowledge that you learn from each attached and then build that in to future defences. So whether we can talk about signature or whatever, and I disagree that everything is based on signature technology, there's a tremendous amount of work been done in improving where we were 20 years ago with signature, so we can talk about heuristics, we can talk about predictive networks, we can talk about all kinds of different things that help, what we can't do is make sure every single individual attack cannot happen. What we can do is take that individual attack, apply our knowledge very, very, very quickly to everybody else on the internet who runs those products and prevent it happening to all of them.

Vikram Phatak

So we need to wrap up here but I want to try and summarise what I've heard. Which is that, one is we should through different technologies stop what we can and then the stuff that we can't that goal is to find out as quickly as possible from the point of infection to the point of the discovery. If it's years you've got a problem, if we can make it days, or weeks or hours even better, and the game is about shortening the lifespan from when a compromise occurs to detection. So that's the priorities, that's what you'd prioritise. I've got to wrap up is that --?

Brian Smith

I want to add one more thing just to clarify a point, which is that each of those detection things that we use as prevention, the signals from those actually are part of the signal. So the strategy is you increase your protection and then you use all that data as signal input to say that this attacker, this hacker out there is doing something bad. Then from that you, you're essentially setting up trip wires, barriers that they walk into. That alerts you to go and examine them more carefully and, as Andrew

points out, gradually ratchet up the number of trip wires and the better prevention. That's the circle we --

Manish Gupta

No look, I'm not saying that customers should throw out their AV and customers should throw out their intrusion detection products, that's definitely what I'm saying. What I'm saying though is that those products are not protecting us from the malware that is the most malicious, the malware that is going after your most sensitive information and over a period of time, and this always happens in the IT industry, if you're not solving the most complex problem you're not going to get as much money as you yesterday did. We've seen this over the last 10-plus years, we've increasingly seen the cost of AV going down and that's a great thing because that frees up budget for the CISO to go and spend it on technologies that are protecting him from more advanced threats and that's the trend that's going to continue.

Vikram Phatak

So the new summary is invest more in the things that work and invest less in the things that don't. Okay, I think that's it. Is there time for Q&A? No, I think we're out of time.

Well thank you everybody. A great group of panellists, hopefully this has been informative and I know we will all be around at least for a little while and if you have any questions we'd be very happy to speak with you. Thank you very much.

[End]