NetEvents

EMEA Press Spotlight

DRAFT

Analyst Round Table IV: Best Practices for Delivering Security Value to the Enterprise Customer

Led by: Manek Dubash

Editorial Director, NetEvents

Panellists:

Roz Parkinson	Research Manager - EMEA Enterprise Networks, IDC
Scott Raynovich	Principal Analyst, Futuriom
Rik Turner	Principal Analyst, Infrastructure Solutions, Ovum

Manek Dubash

We're going to be talking about how we deliver security to the enterprise, how the enterprise can basically maintain its posture. I'd like to start first of all, we had a brief discussion over breakfast this morning, what do we mean by best practices and can we apply that in a generic way? Given as the previous session has noted that businesses are all very different, all segments are different, it varies by vertical, by individual company. So can we actually talk about best practices, best security practices in a generic way at all? Thoughts, Roz?

Roz Parkinson

So interestingly, when we were talking about this at breakfast, I think it was Rik who brought up the example of a healthcare provider or a hospital. If they are using connected devices in that environment, they will have different limitations on when they can apply their security patches, et cetera and do that kind of maintenance. If you compare that to financial services, or you compare it to retail, or just an ordinary enterprise, you can already see that there are going to be differences in the type of data that they have, where they are storing it, the latency that's required, what are they going to be using it for. So I think it's very difficult to have generic best practices and that it would actually be more useable for enterprises if we focused on best practice for industry or for vertical, would be my view on that. I'll pass it on to you now, so you can disagree or agree.

Scott Raynovich

Great, I'll talk about best practices in a few seconds, but first I have something very important to say. So I was catching up on my news just before this panel and I read that a study from Cornell University indicates that we consistently underestimate how much people like us. It kind of made my day, I thought maybe it would brighten up the room. Greg probably has something negative to say about that.

[Aside discussion]

Scott Raynovich

So best practices, it's kind of a wooden term, isn't it? It's something that we're supposed to talk about as analysts, but the way I look at it is management. Are you managing your business? Are you managing your security? The thing that I find hilarious is that consistently when you read about these big security breaches and these disasters, these billion dollar disasters, what you consistently find is that somebody was completely out to lunch. It's not about the technology; it's about the daily management of the business and paying attention to details.

You might have all the security technology in the world, but if nobody's paying any attention to it or looking at it, it doesn't matter. Such as the Equifax breach, where apparently the CEO didn't even talk to the one security officer in one of the largest handlers of people's personal data in the world. When I read about it, it sounded like there were two guys in there, eating sandwiches and watching the NBA or something, they weren't even doing anything. So I think that's the biggest challenge for me in the security industry. It's not at the IT security level; it's at the board and executive level of making these managers aware of their responsibilities with people's data and applications and actually then having that be a very high priority as a manager.

Rik Turner

We do get asked by enterprise customers, we get enquiries from time to time, fairly often, can we point them in the direction of any best practices for firewall management, identity management, any of these areas within security. So people are interested. I would go as far as to say a lot of companies that I come across with [unclear] they're just as interested in any set of best practices as - they're just as much interested in being benchmarked against their peers in the same vertical. I think the best practices are a kind of an ideal set of procedures and ways of doing things which you can at least set up for your security team to aim at always, as Roz said earlier, with the proviso that your particular vertical maybe requires some changes and tweaks to best practices.

Best practice would seem to suggest generically in security that one should always patch key vulnerabilities as soon as the vulnerability is published and the patch is made available. But in the case that we were talking about which was mentioned earlier, clearly it's not good enough in the case of say the National Health Service in Britain to say well, we couldn't do any blood transfusions unfortunately for the last three days because our systems were down. So clearly there are mitigating factors in different sectors which mean that patching maybe has to take a back seat for a while, until they can find a good period where there aren't so many people going to be affected or whatever.

So there are some vertical tweaks, I suppose you could call them, that need to be made to best practices and I find with [unclear] I mentioned earlier, that a lot of them actually in order to go the board and be shown to be delivering value or whatever, they have to translate it into some kind of benchmark against their peers in their particular sector, say in the financial sector. It's almost a case that the board needs to be shown well we've scored three points better on security than the other six banks on the high street or something, because being able to say we adhere to all best practice is not really very good or very comprehensible for people on the board who are not technical. So I think that there's that element as well to security, of being able to translate it into something that board members can actually consume and understand the quality of what you've done for all this money that they've thrown at you.

Manek Dubash

Which begs the question of why is it they're just not interested in something that's as fundamental to their business as all the other stuff they're interested in?

Rik Turner

They may be interested in it, but quite frankly they've probably got 50 other things to do as well and they just don't have the time, the bandwidth as they say, to be able to really devote to it at a certain point. They may be older school folks who predate technology in a lot of cases as well.

Roz Parkinson

I think sometimes the interest in benchmarks, particularly for security, is about demonstrating plausible deniability. So you can say yes, we did industry standard, we know that what we were doing should be acceptable if there is a breach and if they do get court cases, if they get sued afterwards because of that. I think what's interesting, going back to Rik's first slide that he showed yesterday, where the security conversation has moved from trying to protect data so much, to what do you do when you have that inevitable breach. Well, I would imagine that there's quite a lot of interest in benchmarking, or in how do you detect and respond as quickly as possible and how do you manage that PR nightmare.

Manek Dubash

Exactly as the breaches will happen. So this is down to - it's a people problem. Security is always a people problem, we know this. Incidentally, do hold your hand up if you want to ask a question, because this is interactive, we hope. So is more training the answer? I think you had some thoughts on that.

Roz Parkinson

Okay, well, at breakfast I was talking about how at every organisation I've worked at, I've had to do some kind of security training and it's basically a tick list exercise. You get sent a link, you have to flick through the slides, say yes, I agree to it. Basically it's about the company being able to say yes, we've done basic training. So Roz knows that she shouldn't click on links that look obviously dodgy, or open attachments which look at bit weird.

Scott Raynovich

Don't respond to the Nigerian prince.

Roz Parkinson

Yes, exactly, even if he offers me millions and millions of pounds, I just have to say no and ignore that email. It's pretty basic stuff, but it's about again the organisation being able to say yes, everybody's done that training.

Manek Dubash

Question there.

Oliver Schonschek, Insider Research

Oliver Schonschek from Insider Research, concerning best practices benchmarking. Sometimes I feel it even risky that benchmarks maybe say all the basics in security are well done by the companies and if you look at the techs, a lot of the techs could be no problem at all if there was basic protection. Even the basic training, sometimes the employees have the basic training and all know about it, but we all know about the psychology problems of course and the security professionals themselves. They not only have basic training, but high level training and sometimes they think well, what about it, I know the risk and I take it. Then they are breaching themselves.

Rik Turner

Yes, it's inevitable that you have to have things like - I suppose the easiest one is the example that Roz was just giving of phishing training. It's quite clear that you have to have phishing training, all companies need to do it. It's as necessary as having insurance or health and safety training. You have to get somebody on every floor of the building to have health and safety training and whatever, in case somebody has a heart attack or a massive asthma attack or something, that you need somebody there that knows what to do. In the same way, it's good common sense to have good practice, to have phishing training, given the sheer prevalence of phishing as the attack vector at the moment.

But clearly you are working against good old human curiosity and if the people who are sending them happen to know that you're really into speedboats or something and the link really does look like hey, take a look at this really great speedboat that I've just come across, there's probably a 50/50 chance that - maybe they'll reduce the 50/50 chance down to 70/30 or something, but there will still be definitely a chance that someone's going to click on something dodgy at some point during the course of their working day. So yes, it's only as good as it is and as good as it can be. I think the training is required, yes, definitely, but we're working in a world of fallible human nature, so it is what it is.

Manek Dubash

Question here. There's a microphone, there should be one on every table. Can you pass the microphone along? Thanks.

Guy Hervier, Informatique News

I'm here from InformatiqueNews, France. I have a simple remark about what you said, Scott. I think - don't you think, no matter what you do, there always will be somebody like two guys eating sandwiches, watching the NBA and the only solution to solve that problem would launch - to have everything automated. But even with that, you will have somebody to launch the automation. What's the solution to that? It looks like there is no solution to that problem. You can have best environment and a lot of training and people doing their jobs and everything, but there are real - you mentioned Equifax and when you think what happened, it's just two people didn't do what they were supposed to do, so what can you do?

Scott Raynovich

Yes, it's a good question. I don't know, it seems like sometimes our industry or the cybersecurity industry is very immature, I don't know. Going back to Equifax, the details when I read them, they didn't really even have a security department, it was just like the IT guy. I'm scared to say the answer might have to be some sort of regulation, though I don't necessarily philosophically agree with what's a regulation. Like the new EU regulations have made my life probably worse and made my IT attention span worse. But maybe, I don't know, shareholders should speak up. I don't know what the answer is, I really don't. All I know is that the industry is failing.

If you look at all the statistics, the security threats get worse every year and there are more breaches and there's more economic damage. The CEOs certainly don't have an answer. One of the things we touched on yesterday, I think a big problem is some of these tools have to be consolidated. If you go to your average cybersecurity department or [CSO], I talked to a guy who said he's consistently evaluating a dozen or so tools and he already uses a dozen or so tools. So a lot of his time is consumed evaluating the new tools and there has to be more, I think, consolidation in the industry so that there's more of a dashboard approach.

We're talking about - Rik was talking about [unclear] yesterday, they're rolling out more functionality and their competitors are rolling out more functionality, but I think it would be better if the industry maybe consolidated a little faster and you had six tools with 24 functions, instead of 12 tools with four functions, kind of thing. Because the automation will be the answer, but there's new automation being added to process alerts and consolidated alerts that tell you which ones to pay attention to first and things like this. This will improve the process, but there's still just too many things to manage for the finite amount of humans, as you pointed out, that are the choking point in the process.

The other one was Target, the big Target breach, where FireEye allegedly flagged the breach and it was - I can't remember the exact time, something like 72 hours before that even got up to the CEO level that there had been this point of sale breach. It was three days before - even though the technology had flagged that it had happened, it was the human choke point that stopped something from happening. So I don't exactly know what the answer is, other than I just feel like these people are being irresponsible.

Roz Parkinson

So Scott, can I ask you a question actually, on what you've just said, because it just made me think about managed security services. So not my area that I know much about, but what we're saying is we need more automation. There's fatigue in terms of how much attention the humans who are responsible are able to pay it and how they're able to respond. So what do you think about enterprises saying okay, somebody else manage my security? Because I think that a lot of people would feel - well, I imagine quite a few people would feel uncomfortable about giving that away, but I'm just curious about what you might be seeing.

Scott Raynovich

It probably makes sense if you're working at Equifax and you don't know what you're doing, that maybe you should probably have a professional organisation come in and do an assessment, an evaluation. That's probably another thing that's not happening enough. I actually know a big security consultant where I live who's an outsourced contractor for the Federal Government. He has all sorts of stories, when he goes into some of these organisations they just have no clue. He worked for the Department of Defense and fought hackers for 10 years and he says he goes into some of these organisations and it's like a sieve, there are so many holes that it's unbelievable.

So absolutely some of these companies should be hiring professional security assessment companies to come in and figure it out. With that, it all comes back to the money question which we were also talking about, how much money should they spend on security, what percentage of your IT budget should be in security and how do you spend that wisely.

Roz Parkinson

Yes and I think it's that money question which brings us back to the it's about limiting our liability, because that's a way of trying to, I guess, prevent you from having those legal costs.

Manek Dubash

Doesn't it say that there's actually not enough penalty from a financial perspective in not putting enough money into security? In other words, should there be - what kind of mechanism could we find for making that happen?

Rik Turner

Certainly in a previous role I wrote about financial services technology. It was quite clear in watching the regulator in the UK - it used to be called the FSA, now it's the FCA, but anyway, the Financial Conduct Authority. It was quite obvious in watching them and they're considered to be something of a bellwether in Europe in terms of financial regulators, so other regulators around Europe tend to watch what the UK one was doing and follow suit. But certainly with them it was quite clear that they would introduce something like anti-money laundering regulation and say okay, all banks are required to do this.

After they passed the regulation, they'd wait roughly 12 to 18 months until they picked on one particular bank that had failed, found one that failed, fined it quite a significant amount, not enough to threaten its future and viability, but they would impose a significant fine and would also put out very high profile press releases and brief the *Financial Times* and make sure that it got into all the right newspapers. Then what you would find is that all of the other people in the same vertical, all the other banks, in other words, basically would run round like headless chickens until they found the right anti-money laundering technology to deploy so that they wouldn't be the next one to be fined.

Manek Dubash

I would have hoped that the financial industry, being one of the most heavily regulated industries, would actually be one of the least…

Rik Turner

No, trust me.

Manek Dubash

But then there's all the others. There's a question over there. Sorry, there's a microphone. Can you pass the mike along?

Unidentified Male

I think this is pushing towards the point where, as you say, I don't think we should have regulations which say we need to do XYZ, because that is inflexible and I agree, philosophically it's not where I would go. But as a cost of operating for businesses, every year they do financial audits. Do you think every company should have to do a security audit, where we can use as much automation as possible to judge where those holes in the sieve are in order to give them advice and potentially fine in order to do it? If we were to implement that, going to some of the discussions we've had over the last few days, do you treat different industries differently? For example, a critical infrastructure business, where if their site explodes because it's got a virus or affects the whole electricity grid of the country, should they be treated differently to a Target, who are a customer facing business where it doesn't kill people?

Rik Turner

Clearly there are greater risks and that needs to be factored in. Yes, you're right. I think that we will, as more business becomes eBusiness or eCommerce, then clearly we need to get more and more basic health checks on perhaps an annual basis of how well companies are doing in terms of cybersecurity. It probably will move in the direction of regulation.

The other thing I would mention is also that given that the experience of things like what Scott was mentioning about the Target breach of 2013, I think it was, where in fact the company that was first breached was their HVAC provider or services provider for heating and air conditioning, there is now a growing sector of technology called vendor risk management, which operates in various ways but basically says okay, you're a major enterprise, we can run an audit and see if you're secure, but let's also see if all of the 50 or 100 companies that you work with - what their security posture looks like and whether or not they come up to muster. If not, will you still be prepared to do business with them and so forth. Carry on, Greg.

Greg Ferro

If you look at a standard physical office today, let's say we've got an office block, a 20-storey office block, how many companies do a physical audit every year, or every six months? How many companies waste money checking the door locks every day, to make sure that they're actually in good health and that the keys are working? Do they check that the - right? So now you're saying to people I start applying controls to your security infrastructure or cybersecurity, that you don't even do to your physical infrastructure.

Manek Dubash

That's not true though because…

Greg Ferro

That is absolutely true.

Manek Dubash

…in the UK you have to go round every year and check the electricity point to make sure that…

Greg Ferro

You are saying to people waste money hand over fist to do things in cybersecurity that you don't do in the real world.

Manek Dubash

But we do do it in the real world. You have to do electricity checks on your points to make sure that people…

Greg Ferro

Nobody does.

Roz Parkinson

Actually in the UK you won't have your - your insurance will not cover you if you do not do those checks, so therefore people do those checks.

Unidentified Male

But those checks are paper tigers. Somebody walking around with a clipboard saying do you have a backup? Yes, right?

Greg Ferro

Have you checked the locks lately? I waltzed through the door this morning and it worked fine. They didn't hire a professional to come in and check the locks and validate the…

Roz Parkinson

It might be different where…

Unidentified Male

Just to give you a quick statistic on that, I did a test of 10 webshops doing level 3 credit card clearing. So they need to evaluate five questions in five days. Of those 10 shops, eight lied on their checklist.

Roz Parkinson

Could you demonstrate that they lied?

Unidentified Male

Yes, because I checked the register [unclear].

Roz Parkinson

Okay and then if there was a problem, would they be liable because they had…

Unidentified Male

They would be liable but they just don't care. We create paper tigers, security professionals with clipboards saying yes, yes, yes, that don't have any feeling with reality.

Manek Dubash

So moving on to the solutions, what Philip was saying…

Rik Turner

[Unclear].

Manek Dubash

Sorry, there's more.

Unidentified Male

Actually back on that, because insurance was mentioned and actually nowadays you can take out insurance against the consequences of security breach, et cetera. So as you said, if you don't do the physical check, actually your insurance will not be paid out. Clearly to what extent might be the insurance companies that say okay, we provide you with coverage regarding security, but then in that case, yes, we'll have to do the check and indeed you'll have to be at least at a certain level.

Unidentified Male

[Unclear] insurance, because that's another - cyber risk insurance. One of the big three [unclear] insurance companies asked three questions at the intake of their insurance and one of the questions was do you have a firewall? So insurance has the same disease…

Roz Parkinson

So obviously I think there's a bit of a lack of maturity there, isn't there? Maybe this comes back to what we were talking about, about there not being a big enough penalty in order to therefore motivate better behaviour.

Manek Dubash

Which to me begs the question if you're going to say regulation is not the answer, which some people argue then…

Roz Parkinson

But what on earth is?

Manek Dubash

…then the shareholders are supposed to be the ultimate, but they're not very good at that stuff either.

Roz Parkinson

No.

Manek Dubash

So is SD-WAN the answer then?

Roz Parkinson

I think it's very, very difficult and I think that we can argue all the minutiae and the different points. I think that what SD-WAN and also more automation and more visibility on the network do is they do make it easier to detect some of those threats, therefore, in theory, to respond to them more quickly. But I think that this issue that's been brought up a few times about what are the penalties, what's actually motivating people to act and how much of your budget should you be spending on security, these are the levers that are actually going to make the difference.

Manek Dubash

Yes, so it needs internal policing or external policing somewhere along the line.

Roz Parkinson

It needs to matter and if there's the perception that it doesn't, or the few people that are supposed to be responsible for it aren't taking it seriously enough, then we're always going to have problems.

Scott Raynovich

[Unclear] this is pretty intense. I was wondering, can I share another one of my facts? This might have applicability to things we've been discussing. So Google recently had to change its smart reply feature because the AI engine kept suggesting that the response should be I love you. That's a true fact. Anyway, sorry.

Roz Parkinson

The response to what? To any question?

Scott Raynovich

Yes, to an email. It has a smart reply feature that you can enable. It would automatically suggest a reply and the reply that it was most commonly suggesting was I love you.

Manek Dubash

Doesn't that just show how much as humans we need some love though?

[Laughter]

Manek Dubash

Actually there is a point that Scott made that I would like to pick up on. Well of course, all you need is love. Sorry, there is a question, sorry.

Unidentified Male

Well there was a press statement of Europol some days ago that there could be the problem that the high penalties from GDPR will help cyber criminals to get ransom because it's cheaper to pay than to get the penalty. What would you say - what is your feeling about that? We just said that maybe financial pressure would help to…

Scott Raynovich

All security decisions are economic, right? As one person put it to me, they could spend 100 per cent of their budget on security, but there's still a two per cent chance they'll have a breach and they'll be bankrupt. So what's the right amount? Is it five per cent, is it six per cent? It's an economic decision, it's impossible to become 100 per cent safe, so it's just all about cost. I think the point was brought up yesterday, I think Greg said that people just don't care. It might be a valid point, as I tweeted the stock price of Equifax, it's back to where it was before the breach.

In other words, it plummeted whatever it was, 20 per cent, the day after this was revealed and then through the press accounts we learn that they were completely incompetent and nobody cared and the CEO wasn't paying any attention and he got fired, blah, blah, blah. Here we are, whatever it is, is it a year or six months later, the stock price is back close to an all-time high. This is again one of the companies that holds the most personal data in the world. So it's interesting, economically that had very little impact on them, so they're not incentivised to spend money on it, right?

Greg Ferro

Just to get a sense of perspective here, if the CEO goes out and does something in his personal life which is not right, he gets fired and the company goes on. If something happens in the - there are plenty of companies out there doing illegal practices, like British Airways, for example, was paying Saudi princesses, they were bribing people to get deals, arms deals in various countries. Those companies still exist today, make profits, listed on the stock exchange. There's no difference between a cybersecurity risk and any other business risk and we need to stop inflating or conflating this as if cybersecurity is different to anything else.

It is just an average mediocre business function that needs to be cost minimised to the absolute lowest level, and you wear the risk, just like you do that one of your employees is going to drive a car through the front building or get involved in some comprising situation, or whatever. Cybersecurity is not magic, it is just another business function.

Scott Raynovich

That is right and I do not know, back to the regulatory thing I am not a big fan of GDPR as a small business person. It is just added a bunch of headaches to me and I do not know that it is - to me it is just created more cookie spam, right, you have got to click on the stupid cookie button. Oh, there is cookies, okay, click, is that any worse than ad spam I do not know. I do not know that regulation will fix the problem.

Greg Ferro

I mean GDPR is like [unclear].

Unidentified Male

I would just like to pick up on something you mentioned earlier Scott about endpoint security and the number of solutions. I mean we have been talking for - certainly as long as I've been involved in the industry, 30 years or so, about the degree to which the security industry needs to consolidate. Somehow, compared to all the other bits of the security industry there still seem to be millions of players out there. It hasn't consolidated, why is that, and why is that such a headache for [unclear]?

Scott Raynovich

Oh, there is this thing called venture capital. To a certain extent it has been - well I am a financial maven so I think there is a pretty nice healthy bubble going on in the US. I do not know what everybody thinks of other parts of the world, obviously Europe has not recovered as robustly as the United States but we are powered by this great thing called the Federal Reserve that gives everybody free money whenever things get bad.

So that has certainly - and it is documented that that is incentivised private equity and venture capital, and it is created a lot of companies which on one hand is very good because I believe that venture capital helps accelerate innovation and pushes markets forward. But on the bad side, like you pointed out, there is too many companies and there is going to have to be a cycle that cleanses us of the excess and eventually consolidates the winners and the best technology.

But then there will be another cycle but right now there are - I was involved in a research project a few years ago where I had a boss - I was a VP of research at another company and I had a boss that said, we need to assess all the security start-ups in the world. We started making a spreadsheet and he thought this project would be like a month long and four months later it is like, oh, let us check the spreadsheet. Do you know how many companies were on the spreadsheet - over 400, and these are just venture backed or bootstrapped.

So over 400 and we had filtered out a lot of garbage, you know some guy in a garage in Dubai and we didn't include that, so it was like over 400 cybersecurity start-ups. It is insane. I do not know how anybody can go into that spreadsheet and look at it and be like, oh, we need to evaluate this, we need to evaluate this, it is impossible. So it is definitely a challenge and there should be consolidations.

Rik Turner

It kind of goes back to Catherine's point earlier about - just buy it from the operator, right.

Scott Raynovich

No, that is not the answer.

Rik Turner

I think there is also - I mean, yes, there are clearly financial incentives on the part of - if it is easy, if there is lots of cheap money in the post-crash world where we kept interest rates low and we were quantitative easing, whatever it was called, to printing more money to keep inflation low and have a - whatever. Clearly there was lots of money sloshing around particularly in Silicon Valley for security start-ups in the last few years.

They have tightened a little bit now, I do not know, but some of those numbers we have been seeing suggests that that is the case. But in any case there is also a technical issue with the security space, which is not so in most other areas of technology, which is of course that security is an adversarial sport, in as much as if you are developing data storage your challenge is to be able to get more data into whatever storage devices you are coming up with, if you are putting them in the Cloud you can put even more in and so forth.

But you do not have anybody out there who is deliberately trying to limit the amount of data storage you can get or the amount of data you can get into any given storage device. You do not have any enemies as such. Clearly, the difference in security is that it is adversarial and that therefore the people who are interested in - who have a vested interest in attacking you to get whatever, your valuable data, or just to mess up your infrastructure, to muddy your reputation or whatever.

The bad guys, as they call them, do come up with new ways. As technology evolves clearly there are new ways to launch attacks, there are new vectors as the industry calls them and the existing industry mavens, the big guys, do not necessarily have the wherewithal to respond quickly. Therefore, it is inevitable that if they cannot do it all there will be start-ups. Maybe it is a bit different in say the pharmaceutical world where it is only the really big drug companies that will be developing the new ways of attacking a virus or whatever.

But clearly when you are Symantec, or McAfee, or Trend Micro, and those guys have been involved in - are busily promoting their existing very broad portfolios. They do not necessarily have the time or resources immediately to respond to a new threat vector, a new form of attack, a new way of getting into corporate infrastructures. So it is only natural that somebody else will leave, try and do it differently in their garage as Scott was saying, maybe not in Dubai but certainly in Silicon Valley.

The classic Hewlett Packard model is very much an inspiration to a lot of people and there is basically money to make it - to help. Of course there is also an incentive to a lot of them because a lot of people leave Cisco, start a company doing something clever in networking and get brought back in by Cisco in a matter of a couple of years. You can almost feel that a lot of the really big companies at the high end of the usual suspects, if you like, at the high end of the security space certainly 10 years ago up until the financial crash, there was almost a conscious effort - a conscious decision on the part of the likes of Symantec and McAfee and others to actually adopt Mao Tse-Tung's philosophy, of let a 1000 flowers grow and then at a certain point once that sector reached a degree of maturity you'd go in and lop off the heads of one or two of those flowers by acquiring them.

It does strike me that we still see that even in the post-crisis era say with the example of Cloud access security brokers, CASB, where there 25 start-ups I think two years or four years ago, and over the course of about 18 months everybody bought one amongst the top companies. So there is this kind of - the natural evolution of technology, the development of new adversarial approaches also is a spur to more start-ups. But there will always be a consolidation at a given point until the next big thing comes along and new start-ups come into existence to address that. I think that is just the nature of the beast. Of course, with capitalism it is even - US capitalism in particular, it makes it even easier for that to happen because of all the VC money sloshing around.

[Over speaking]

Manek Dubash

A question there from [unclear].

[Unidentified]

Actually a question, because you are saying this is an adversarial environment, actually there is another one. If you take for instance the military complex there as well you had a consolidation in the large Lockheed Martin, et cetera. So to what extent - and you are saying it is much more start-ups, but if we look at companies like Thales, et cetera, these are big companies and do have enterprise level and enterprise grade security practices.

So why do not you see perhaps those kind of companies who are already in an almost principally and basically adversarial environment taking up then, for instance, Thales as well taking up the interest…

[Over speaking]

Unidentified

…and doing enterprise level. So rather doing a start-up perhaps doing the Lockheed Martin or perhaps…

[Over speaking]

Rik Turner

Yes, it is an interesting point you make and indeed it is true that a lot of defence contractors in the US did at one time or another consider and indeed go and actually make efforts to develop a cybersecurity arm, Lockheed Martin is a case in point. Raytheon, General Dynamics I think was another one, about half a dozen of them. BAE in the UK, British Aerospace, the guys that basically helped fund a lot of the lifestyle of the Saudi Royal Family.

A lot of these guys did develop cyber arms as they call them. Some of them have spun them off again because it is a different business. I mean fundamentally the defence business you have got, I'll say one, but you have got one target customer in most countries, right, the government of those countries or whatever. It is a very different business when you are in the enterprise technology world and you have 10,000 companies with very different profiles.

Unidentified

But that is exactly the point. Once again and taking example of Thales, I talked to them recently. Clearly, they have a kind of target to go outside let us say the single customer type of markets where indeed you are talking to the governmental customers and kind of diversification, simply because they have the knowledge, they have the mind-set, they have the culture…

[Over speaking]

Rik Turner

No, I agree, you are right.

Unidentified

They would simply go and diversify.

Rik Turner

That is exactly the thinking that I think - it is exactly the thinking that spurred a lot of these companies on, not least because the likes of Lockheed Martin obviously had to develop cybersecurity for their own security. Because if you are going to attack anybody all right probably the banking sector is the largest single sector for obvious financial reasons. But there are also massive state actor attacks on the defence industry because there is a commercial advantage or there is a strategic advantage if you are China.

Unidentified

The loyal competition.

Rik Turner

Exactly.

Roz Parkinson

So just on that point about - well maybe defence contractors or people who have been - well companies that have been supplying the military moving into enterprise, so on the networking side I've come across a couple of companies. One in the US called Vergent, which does wireless communications and used to do that in the defence sector, which is now trying to diversify in IoT, and looking at things like providing the IoT connectivity in places like ports, shipping ports, somewhere where you are - it is critical information that needs to be passed in a secure manner. So there is a little bit of people looking outside and thinking about the IoT security.

Rik Turner

Oh, I agree, absolutely. I mean in fact a lot of - you will often hear people in - one of the standard things that people refer to in the security space, in the same way as most security professionals or practitioners or certainly vendors, the way they always refer to the Verizon data breach report that I think Atchison was referring to earlier, it is a standard like anything. Another one of those kinds of standard things everybody talks about is Lockheed Martin's - I was going to say - they call it the kill chain.

Yes, the kill chain, it was created by Lockheed Martin - right. So, yes, they definitely all invested in it and bought companies and developed their own business units and one thing I know it is true. I did start seeing a trend for them to sell it off because there is also - I mean it is a little bit like - you know when you find a company that - EMC is a great example. They were a company in a different sector but I mean they were very good at selling really big storage boxes to banks on Wall Street because they had maybe 30, 50 customers that they needed to go in.

It is one approach to go into large enterprise and really do a high touch model to get into them. The challenges that they faced when they tried to go more mid-market or SMB, this is before we even get to the fact that you are talking about defence vis-à-vis general enterprise security. Just going into SMB they had to start thinking about developing a channel model.

They had to start thinking about - well hang about, this guy is only ever going to buy a box this big whereas we are used to selling these massive great big boxes, and those guys do not really want the high touch model because we are not going to get any money out of it, all of these kind of things. I think that that was a kind of challenge that a lot of the defence contractors faced when they wanted to start getting heavily into enterprise security. Sorry, I didn't mean [unclear].

Unidentified

There are two elements here to begin with. EMC is interesting because actually they bought the companies, they needed it, and you could believe EMC didn't have also a security related…

Rik Turner

No, no, no, I wasn't using it terms of security. I was talking about in terms of the challenge of going from high end enterprise into SMB is akin to what happens when a defence contractor tries to get into enterprise generally, whether it be in security or any other space.

Unidentified

To be honest, is that because it was also mentioned that at a certain point you could go into a large company and say, well we also looked through your - let us say your supply chain or your contractors and clearly to an extent produce a solution. Because obviously this large company, for instance, a major retailer in Belgian [Colruyt] has plenty of - hundreds if not thousands of people or companies in the supply chain, actually might be interested in taking up the responsibility to go down the chain.

Usually then you go to medium and even very small companies to actually try to raise their posture simply because it is in their own interest, because as you mentioned it is the AVAC at the target that was actually the original culprit. So it is in the interest of a large company to go out and do indeed the SMB business, and to that extent you do not have the problem as large defence companies. Because at that point the large companies themselves will take up the responsibility and do some [unclear] about it because it is in their self-interest.

Manek Dubash

Okay, on that note given that we are straying a little bit off topic, because we are supposed to be talking about best practices and we have got about five or so minutes left, because I am aware that Roz has to disappear in about seven minutes to catch a plane incidentally. I would like to bring us back to the issue of best practices and ask each of you if you had a portmanteau of best practices to offer what would it be? I haven't prepared them for this question so they're thinking on the fly - Scott.

Scott Raynovich

What I think would be interesting is if - unfortunately this isn't like a venture capital conference, there is not a venture capitalist who is going to give me all this money to do this, but it would be an interesting model to have. I am interested in private, third party ratification models. An example is somebody was talking about customer service or is anybody familiar with the Temkin survey?

The Temkin survey is like a big customer service-rating agency. Basically, kind of like you have Standard & Poor's which rates securities, they rate customer service. Coincidentally what Greg was poking at is actually true. The cable companies and service providers consistently rank at the bottom of the Temkin survey. Contrarily, Amazon consistently ranks at the top. Then in the consumer industry, you also have J D Power and you see the plaque on the airline, which - that is always a little bit out of place for me - an airline is rated great.

I do not know but it is a third party agency that is charged with somehow rating. It would be interesting to see that in the cybersecurity business. If somebody could go in, you went to the Equifax website and then you could check what is there J D Power security rating. It is a D plus, well I think I am going to take my data someplace else. I do not know, maybe I am wrong, is there anything that exists like that?

Manek Dubash

There are attempts, yes, there are.

Scott Raynovich

They're not well publicised though.

Manek Dubash

It is true, there have been initiatives.

Scott Raynovich

Or you know you can go see that it is certified or whatever. I think that would be an interesting way to check. We talked about how do you keep the industry in check that would be interesting?

Roz Parkinson

Yes, I mean - so I keep on thinking about the human factor of this because that seems to be the weakest link that we have all discussed. I was having a conversation yesterday and somebody came up with the idea of common sense as a service. Yes, not my idea, but I really, really like it. Because obviously I've been a technology analyst for about five or six years now and there is always a lot of excitement about the new technology and what it is going to do, et cetera, et cetera. A lot of what actually solves the problem is using your common sense, is behaving in a kind of a sensible way.

Manek Dubash

A rational way, in the circumstances.

Roz Parkinson

I think that the issue that we have at the moment for security and I see this in networking as well, is that people are overloaded by how many alerts and how many threats there are out there and it is an overwhelming task to try and tame this. So although I am very happy with the idea of applying common sense, we need to give the people who are responsible for security the right tools to help them do that. That will come through with - and in particular on the networking side when we are seeing more software definition in the network, the ability to detect threats more quickly, et cetera. So, yes, as we see more automation we'll be able to give our people better tools.

Manek Dubash

Okay, Rik the final - we are almost out of time.

Rik Turner

Yes, but it is relevant to what we have been talking about. Common sense and service absolutely, two or three years ago we mentioned it. Anything to do - sort of any kind of best practice et cetera, et cetera, is just an artificial restriction, right. There is no logic behind it. I mean if you look at something like ITIL, if anybody is familiar with ITIL compliance rules for IT service management in the UK, all it does is enable people to say, I am ITIL compliant and that sounds like a great reason to buy a product, when actually it is completely meaningless.

In terms of actually certification, [unclear] as a product tester obviously but all we can actually do is prove that something works. We cannot actually then say it will work when a human being gets involved until we have some kind of company called, we stop people fucking up.com and then the world starts working. But it is always an artificial limitation. Beyond that how do you stop someone being stupid, right?

Manek Dubash

Yes, good question, okay, your portmanteau of best practice.

Rik Turner

Well I mean ITIL [unclear] there a bunch of frameworks that are out there for best practices that people can be referred to. They're all good, they have all got good points and bad points. I tend to be fairly cynical about them for the simple reason that humanity screws up. I mean the classic example of which was probably the agent from MI6 I think it was, that is the spy organisation in the US and the UK government who a few years ago had a few too many beers and left his laptop in the back of a taxi. Now what could you do with best practice of that? Well you cannot take your laptop out of the building anymore, or if you know you are going to a pub - it still goes around human factor.

Scott Raynovich

It should be okay if the data is encrypted though, right.

Rik Turner

Yes, right, yes.

Scott Raynovich

The US Government still cannot unlock an iPhone so…

Rik Turner

Exactly, but then by the same token here we have got quantum crypto coming around the corner, we have got quantum computing that presumably is going to break all of current day - current cyphers, so that is a whole different conversation. But yes, I mean there are frameworks that we can refer people to in terms of that best practices and that - a mixture of common sense. What is it - hope for the best and prepare for the worst?

Manek Dubash

On that note, I would like to thank the panel very much, thank you. Thanks for your erudition, your wide ranging contributions and I hope you catch your plane Roz.

Roz Parkinson

Thank you.

Manek Dubash

Okay, so that concludes the formal part of this meeting.