NETEVENTS

EUROPEAN MEDIA SPOTLIGHT

"INNOVATORS IN CLOUD, IOT, AI & SECURITY"

DRAFT

Combating the Current Threat Landscape - Ransomware, Ransomworms, Credential Theft and Advanced Spearphishing

Chair:

Duncan Brown, Associate Vice President, European Security Practice, IDC

Panellists:

Laurance Dine	Managing Principal for the Verizon Investigative Response Team
Greg Fitzgerald	Greg Fitzgerald, Chief Operating Officer & Chief Marketing Officer, Javelin Networks
Carl Gottlieb	Carl Gottlieb, Consulting Director, Cognition Secure
Eduard Meelhuysen	Jason Steer, Solutions Architect, EMEA, Menlo Security
Jason Steer	Eduard Meelhuysen, VP Sales EMEA, Bitglass

Manek Dubash

Thanks, Mike, and thanks again to a great panel. We're hoping, one day, that they'll develop time compression, so that we can actually let these panels run for longer, because there's a lot of issues in there.

Okay, so maybe one of our biggest problems, as intimated on this panel and on the previous one, I guess, is the perhaps over-obsessive nature of security, which is to do with not sharing anything. Too many secrets. Is that the answer through our next panel? Combating the current threat landscape. If the panel would like to come down as well, please, that would be great. Thank you. And we'll crack on.

Duncan Brown

My name is Duncan Brown from IDC, I run the security team for Europe and joining me on the panel hopefully there's a list - maybe not. So Laurance do you want to go first, everybody remembers Laurance, remind us who you are. Laurance Dine from the Verizon Investigative Response Team in EMEA. Greg Fitzgerald, Chief Operating Officer at Javelin Networks, Carl Gottlieb from Cognition Consulting in the UK, Eduard Meelhuysen, VP EMEA for BitGlass EMEA.

Thanks chaps. So I just wanted to frame the discussion, the debate that we're going to have for the next 30 minutes. It struck me that when we were putting this panel session together maybe six or eight weeks ago, we would have to spend quite a lot of time in explaining what ransomware is but WannaCry has done that job for us. It turns out that now everybody knows what ransomware is, so job done. So I guess we can take it easy on the panel Jason, do you just quickly want to introduce yourself. I saw you sneak in there? Yes, sorry, I sneaked in the back. Yes, I'm Jason Steer, for Menlo Security in Europe. Thanks Jason.

So awareness of ransomware isn't the problem apart from Greg, you were telling me you had never seen this slide before, so there just for your benefit that's what it looks like, that's WannaCry. The thing about WannaCry for me - I guess there were two things, one was that we think there's a cyber skills shortage globally. It turns out there isn't because the world seems to be an expert in ransomware and particularly WannaCry and they all came out of the woodwork one weekend about three weekends ago.

So crisis over, there was a huge amount of information - I'm being ironic by the way, just for clarity, thanks. But there was a huge amount of debate and discussion about the blame and fault and I wanted to pose that to the panel in just a moment. There was a lot of finger pointing going on and so the apportionment of blame was interesting to see. The other thing that struck me - the biggest surprise about the WannaCry attack for me was that it was a surprise to many people, that most of us in the industry were acutely aware of the threat and the impact that that had.

But I think what we got wrong was the risk assessment. There was clearly a failure in the risk assessment in terms of organisations misunderstanding the likelihood of these attacks and clearly then the impact and we talked in the earlier session about incidence response, the lack of incidence response that organisations appeared to have. So one of the benefits, I suppose you would say, of the job that I have is that I do a lot of transatlantic flights and when you do a lot of transatlantic flights you tend to watch some pretty interesting movies, movies that you wouldn't normally watch.

I watched a movie, it was called Equity and it's actually quite an interesting thing about a cyber security company going public, so it's kind of in our domain anyway. But there's a lovely quote half way through and it says, the trouble with privacy, not security, is that half the world is paranoid and half the world's password is password. Most of the people in this room probably fall into the first category. We're all aware of - maybe not paranoid but at least aware of the stuff that is going on and is possible out there.

But we have to remind ourselves sometimes that there is another half of the world who really doesn't know or care or is completely unaware of the challenges that are facing them. We got an exposure to that with the WannaCry attack, that there were so many people out there for which it was a surprise and they fall into the latter category because they're not typically aware. So what if I start with the panel session, who wants to go first. I'm going to pick on Carl because we had a talk about this.

Carl Gottlieb

Oh, you'll regret this.

Duncan Brown

This blame thing, so there was a - I found it very amusing that Microsoft was pointing fingers at the NSA for allowing the leaked tools going on which I thought again was brave of Microsoft to draw attention to themselves. We saw politicians pointing fingers at each other, we saw politicians pointing fingers at the NHS in the UK for example. What's your perspective Carl on whose fault was it?

Carl Gottlieb

So the first thing is there'll always be crime, there'll always be victims of crime, so let's take the NSA out of this straight away. So the two areas of blame I would straight away are (1) vendors. I think the security industry has got a massive area of blame they need to accept.

Duncan Brown

But given that the rest of your panellists are vendors just…

[Over speaking]

Carl Gottlieb

They I'm sure will agree this that we have an issue whereas vendors we build security products in a lab, we test they work, and we roll them out. Then we don't ever acknowledge how they will perform in the real world. So let's take an example, every NHS PC out there that got infected had anti-virus software on it. So that's not Microsoft's fault, it's not the NSA's fault. So the fault was that they weren't being updated. They had Microsoft Windows on there that wasn't being updated. The reason was because there were organisational, there were IT issues preventing them from being updated.

Now as vendors we know this goes on, we know people can't update their software for good reasons, yet we skirt around the issue. We need to be building products that actually survive the real world environment. It's like building a life vest for when a plane crashes that's going to be too big for people. We need to test it for the actual failure scenario and that's where we failed with WannaCry. The other big area is that IT failed as well. IT departments, and I include [Info Sec] departments as well, failed in that and we continue to do so in the area that we are not relating IT and IT risk assessments into business risk assessments.

So we might say - and this would have gone on in every single NHS Trust, they would have said we want to update Windows from Windows 7 to Windows 8.1 for instance or patch it, and they would have said, why? The response would have been well because bad things might happen, rather than relating this into a business risk perspective or even business opportunity perspective. If we take something like GDPR, we have the opportunity within the Europe to take advantage of this. We can say privacy is now a way we can gain competitive advantage. If we focus on getting business critical risk assessments back into IT to bridge that gap, we can avoid instances like BA and WannaCry.

Duncan Brown

Jason, you were nodding. I don't know whether you're in agreement or…

Jason Steer

I'm in agreement in one key point which is that in terms of IT vendors and security vendors in particular trying to solve this problem. This is a problem that can't be solved in the ways that we've been doing for the last 30 years. I think if we're reliant on employees to differentiate between good and bad by - do I click on this link, do I click on the email, or should I go to this web page and look at that flash video or not? Who is to blame is everyone who built these solutions because relying on employees is always going to fail.

If we look ransomware, which is the headline of the threat landscape we're talking about, email and web are the two primary mechanisms delivering ransomware every day into every business. If I look at my web browser, every web browser you're using, you're using a web browser architecture that's 23 years old. There's not another protocol in your organisation where you take unsigned, unauthenticated active code and execute it on your PC without any controls. But we do it on every website and every time we go to a web page.

We think that's acceptable and we wonder why the web browser isn't a problem. That's why we have to really re-think how employees use the internet and access the internet because the controls and technologies we're using are not effective still today. If we're focusing on detection, if I look at spearphishing there is nothing to detect. It's social engineering of your employees and again your employees are going to make bad choices. Even when we go round to customers and we do those surveys, you do the education and awareness, compelling well-written emails will convince emailers to make bad mistakes because they're human at the end of the day.

There is no malware, there is nothing to detect other than there's a change in that user's login. Things go wrong every day but as Carl was saying, we expect it to work and we expect it to be successful. My God, what utopian world do we live in and it's not that nice, as we've already heard.

Duncan Brown

So, it strikes me that what we need to try and do is to shift behaviour, certainly of the half that are not paranoid or at least aware. Greg, how do you shift behaviour for people to be more aware of the vulnerabilities of the risk and for them to do the right thing or at least not do the wrong thing?

Greg Fitzgerald

Well psychology and science tells us that people are motivated by only two things, sex and pain. In my opinion, pain has not been felt here because I mean security is a risk. If you look at what…

Duncan Brown

This debate is going in a different way that I envisaged but let's try and steer it back on course, all right.

Greg Fitzgerald

Yes, the pain of crime like ransomware is interesting, from us in the industry it's a given, it's going to happen. I don't think the people have felt the pain. I think it's interesting, in America for the first time on Good Morning America, they talked about the consumer feeling this pain, which I thought was interesting. Because now if I care as a consumer then I'll actually care more about my business if that makes sense. My business has an ability to absorb that pain and insurance for my 23 years of being in the business has been - excuse me cyber security has only been an insurance risk.

It's how much from a cost perspective if we can shift it into that realm, what is it going to cost me versus what is it going cost the attacker? I loved Brian Lord's comment earlier this morning as well stating that, the risk factor to an attacker is going to be a business. It is a business bar none. So I think we spend as an industry $100 billion defending ourselves with all these technologies for which I'm a part of it yet none of it is working.

To me, as we had our breakfast I said, there's something wrong, it's a philosophical discussion of we have more cyber security technologies in the world today than ever in the history of the world yet we have more successful cyber-attacks ever.

Carl Gottlieb

Bingo.

Greg Fitzgerald.

There's something amiss, something is wrong, and I think to your point where we all need to sit back and think about the cost benefit of the attacker and then how do we - I hate to say it but defer that attack to something else. Let them go back into prohibition, go into sex trade, whatever it is, because that's where the motivation of consumers are. But I think pain is one of the - I guess when we talk about blame or the pain, pain hasn't really been felt even though we talk about it today, it's still not there to create that action.

I mean a report that came out here in the UK said that 54 per cent of all businesses in the UK are completely unprepared and unaware of attack. That the cost in…

[Over speaking]

Duncan Brown

…are unaware, yes.

Greg Fitzgerald

Yes, unaware to your point on the thing and that it's a $30 billion problem for the UK businesses. Honestly, that's not a lot of money. I mean when you think about all businesses in the UK and the impact, it's kind of like [ugh] I'll charge my customer a couple more dollars on the ATM charge and I'll make up for that.

Duncan Brown

Yes, so we need to feel pain, our customers to feel pain as well.

Greg Fitzgerald

That's my thought.

Duncan Brown

Eduard, any comments?

Eduard Meelhuysen

Yes, I agree with Greg here, is there's not motivation, right. So the fact that we've just shown is that the most common used password is password. So how do we educate those employees, how do we educate those customers to make sure that they understand the risks which are at hand? I think the WannaCry outbreak was fantastic, so everybody in the entire world new about this outbreak, so security came to a high level. Say okay, how do we make sure it doesn't happen again anymore and people start thinking about it?

Not so much internally in terms of what we can invest more in technology, which of course everybody should because that's we live for, but more in how do we educate those customers, how do we educate those employees to make sure that password is not a password anymore? So how do we make sure there sometimes is a new way of authentication, or new way of logging on to a new system, which is not so nice as it was in the past but at least it does its work, right.

So that's really key and I think thinking about - and as my or our expertise a little bit more is Cloud, right, Cloud based computing. How do we make sure that that's under control too? Those are facts which I say where we can have a little bit more control but we will be always behind the curve and always those hackers or phishers or builders of ransomware will be in front of us. Well that is what it is but to close that gap is to make sure that definitely education is one of the key things here.

Duncan Brown

Interesting. Laurance I wanted to come to you because one of the interesting things about the WannaCry attack was the incident response process or sometimes lack thereof that was evident over that weekend. What's your perspective on the way in which companies were prepared for that kind of attack.

Laurance Dine

Well they weren't. I mean that's the simple answer. I mean obviously your large organisations have systems in place to deal with that kind of stuff but the vast majority of people that were hit with that ransomware had no idea what they were going to do, how they were going to restore the data, what they had in place. It's all about taking away the profitability of the attackers isn't it? If you have backups that you can restore in the same amount of time that it takes to pay the ransom and get your data back you're better off going with the backups aren't you?

So that is the number one key thing to have in place, is to have your data available to restore in case of an attack, that's the simple answer. Ransomware is not new, ransomware has been around for a very, very long time. It went dormant for quite a few years but it's back and it's been back statistically for the past couple of years all the time. It's a constant thing. We've got to address that and why it's back and the reason why is because it works and people are making money off of it. If we take that away then they'll go and find something else to do.

Duncan Brown

I wanted to pinch a question from the earlier panel about GDPR because GDPR is designed if nothing else it's designed to change behaviour of companies in the way that they treat data because the consequences of getting it wrong shift the risk profile. Do you see GDPR having an impact on forcing companies to do the right thing? They're supposed to do the right thing now but there's no consequence of not, so do you see GDPR as having an impact on the market? Jason, you're nodding.

Jason Steer

I certainly do. I think certainly for UK companies beyond the *Computer Misuse Act*, for example, there's something compelling finally that's pulling executives and boards to account for how do we deal and respond to this? I think as we see every day play out in the media headlines, most organisations are not thinking about this, not worrying about cyber security is something that's critical to the business. Now GDPR does make everyone in every business accountable if they have a U data. So thank goodness, finally, there is something compelling that does make people change habits.

Greg Fitzgerald

Just a quick comment on the pain. I think we've talked about the ability for pain here is significant if it's enforced. You brought up this morning Facebook got fined pretty significantly and that was before GDPR. But I'll give you an opposite example, in the United States, the Target Store attack, it cost billions of dollars, the CEOs and executives were fined. Some were thrown in jail but the company was only - just settled in court, it was only charged $19 million. That was it. To them that pain is kind of like whatever, and to my executives, hey it was under your watch - sorry.

But the company stock has rebounded and the company is doing great, the brand integrity is still there. So I guess my point is, pain is a short lived opportunity for companies to frankly invest properly because it gets hit but people's memories are very short. So unless that pain is significant I think…

Duncan Brown

Sustained.

Greg Fitzgerald

Sustained, it doesn’t make a big difference.

Carl Gottlieb

I think Greg has probably got the best point of the day so far, talking about motivation. Because we can all talk about how we can train people to do this, train people not to use password, train your parents not to - to back up their software. I think we could all personally look at our own IT security and say we should probably do better ourselves with passwords, with backups and so on. But yet we're supposed to be the experts. So if we focus on this motivation thing and what would motivate someone to do better then as Greg said, we've got the pain and we've also got the pleasure side.

We've got to focus on what caused BA to have this incident where they had a worldwide outage. This wasn't even cyber security, this was purely based on a business risk assessment of - can we reduce costs and what is the impact? Related to cyber security GDPR is this great thing of, yes, we'll have massive fines, but the fines are going to be a lot bigger from things like class action law suits and potentially PR damage. But the better side is, what is the competitive advantage people are going to get?

Now we've all talked and sold in the past about how people should buy security because security is an enabler isn't it? It's not just about reducing risk and cost and that was never the cost. We couldn't ever think of a really good business justification to buy a firewall, now we can. GDPR creates that competitive advantage and it's the real reason why people are getting behind it. The boards that get the benefits, the wake and win with GDPR, they're the ones that are going to do very well out of it.

Duncan Brown

Eduard, you mentioned Cloud earlier on and a lot of people think Cloud's data protection, opposite ends of the spectrum, do you have a view on this, is GDPR going to help or hinder Cloud?

Eduard Meelhuysen

It's going to hinder and if you don't have the proper tools in place it will massively hinder you. Because what we see currently is a lot of people want to go to Cloud for whatever reasons and whatever that means. It could be really simply deploying [unclear] or whatever it is but the fact of the matter is if you look at GDPR is, how do you take control of data moving into the Cloud because it's out of your control? So getting control back is a way of - not only control back but also making really sure where the data resides is a way of getting more to GDPR compliance.

I see now that a lot of my customers and prospects are looking at it really intensively and I'm talking about real large organisations and understanding that they want to move to Cloud because of cost efficiency. But next to that is also making sure that they are safe as well and GDPR rules are met. So I do think that GDPR is helping us to move to the next level, getting more attention from the board room and getting more attention in terms of the budgets being spent on security. Next to that is those outbreaks of WannaCry et cetera also really help.

I'm not saying that security should be the number one focus because I should not need, this is always number one. But how do we make sure that those things are combined and done in a proper way? So moving to Cloud it makes life a little more difficult in terms of CISO but there are tools out there and for one reason we sell one of those of course. But is how you do take control over that traffic and that data, specific data, and we you do not allow stuff to happen or even enforce certain passwords to be used.

Audience Q&A

Duncan Brown

Very good. I want to leave enough time for questions, so any questions from the floor? Do we have a microphone - just behind the pillar, there we are.

Unidentified Participant

So just a question for the panel, what burden do you feel that the vendors should assume regarding assisting the consumers who perhaps aren't aware? I don't know if you've ever been in a support call with your parents to try to help walk through a password change but default passwords, for example, remain default for a period of time. I'd just be curious to know your perspective on how we as an industry help those that may not be aware of the real risks.

Greg Fitzgerald

That's a good question, I'll take the first stab at it. The reality is we can only help people who are willing to take our help. We do things like this, we come in here and we do panels. I do presentations all year round globally about information that we receive through doing our investigations and making people aware. But if you have a CISO or a CIO or somebody who is in that position without that title, who thinks they have all the answers already there's not much we can do as vendors to change them.

Things like GDPR make a difference. My comment on GDPR is it's fantastic, the reality we'll see a real impact when the first person gets fined, that's when the massive impact is. There's preparedness for it right now but when somebody gets the big fine that's when everybody is going to come in.

Duncan Brown

[Unclear]

Greg Fitzgerald

In the security world I think there's very much a - do as I say not as I do. If you check the security posture of probably every cyber security company you would be woefully appalled. We do not use two factor authentication, we do not secure our environments. Our own CISOs are just as confused as everybody else, we're using the Cloud but in an unsafe way. So I think there's a couple of things. I mean there's I think some answers. (1) we need to start eating our own dog food, as your point. Like we created the products, now go and use them.

The second one is that we too should force in many cases some of the capabilities that we believe in, even though from a marketing sales perspective they can be a hindrance. Like you said, the passwords, that's a great one. There's a ton of technologies here I could tell you exactly what passwords everybody is using and force those people to change those passwords. There is some policy around every 60 day, 90 day changes, but I've got five, I can't remember them. So what do I do, I use the same one. In fact, I'm hacked because I'm a target.

Because I'm in the community just like you are. They know who we are, right. I'm socially all over the place and we were laughing in the office the other day because my phone has got this little delay in it. We're going, I'm probably hacked. I think I am. So what do I do? I change my phone. I've got to do all that other - but you know what it's a pain. You know what, I'm like let them take whatever the hell is on my phone, they can listen to my conversations, they are not that bad.

So it's like - I guess the point is I'm not following my own advice but I'm going to sure tell you what you need to be doing. So I don't know if there's an answer but I think there are some things that we could do as a practice to get a little bit better as well.

[Unidentified Speaker]

That was a really good question because this is something that really is a frustration of me as a consumer of technology in that cutting edge security vendors do not sell to SMB and consumers. Consumers and SMBs get a product that's half baked, built for somebody else but we'll repackage and repurpose it and I think for me personally is those hairdressers, those nail salons, those are companies who are hugely impacted by ransomware that literally take out their businesses. How do we help them protect themselves more because they assume that the products they buy solve the problem and this is my frustration as a vendor is, they don't.

Quite frankly, I'm writing off anyone over 60 of actually being able to be helped. Because bad habits are engendered for way too long, can't understand. If I take my parents a great example, they can't patch, they can't update, they can't follow the instructions, my 12 year old daughter absolutely no problem with and full confidence. But where do we sit in between that as an SMB consumer, it's hard to say, but can we wrap every consumer in bubble wrap, no, we can't? But we have to deliver better products that solve problems. My frustration is that we've been buying something that doesn’t fit for purpose any more.

Duncan Brown

Question right down the front, can we get a microphone to the gentleman in the front row.

[Andy Vestruntek]

Andy Vestruntek from Germany, Insider Research. One good thing about - one of the many good things actually from GDPR is the model of shared responsibility when you think of data processors. Wouldn't it be also a good idea to have shared responsibility in other fields like the whole IT security? Because we all know we are all users actually and it's very difficult as you just described here to keep secure, so to maybe make the responsibility of the security industry higher by this model of shared responsibility.

Duncan Brown

Carl do you want to have a ping at that?

Carl Gottlieb

I think you've nailed it. I think you're absolutely right. I think one of the things we forget though about vendors especially is they are sales companies, that's the business we're in. Vendors are about creating products, selling it, same as any other manufacturer, and the people that actually sell it are going to be a mixture of sales people out on the ground in every country and we sell as distributors a whole mix-mash of people. They are different to the marketing people, the PR people, the product development people, the product-marketing people.

There's always different departments and they rarely speak, apart from a few different places, and so one of the challenges is we end up in a situation, as Jason said, where we've got people out on the street saying, whatever your problem is this will solve it. You've got an engineering guy back in Seattle going, whatever you do don't ever say that in this situation because it will not work. The problem is we are focused on quarterly sales numbers and it's just a sad reality, we're just really struggling to get there but you're absolutely right.

Duncan Brown

We need to leave it there but there is coffee, so plenty of opportunity to follow up individually with members of the panel. Panel, thanks very much, thank you.

Manek Debash

Again, this could run and run and it seems to me that the problem is that security has become a cultural question that people talk about over their dinner tables. Anyway, go and get some coffee, come back in 10 minutes.

[end]