NETEVENTS

EUROPEAN MEDIA SPOTLIGHT

"INNOVATORS IN CLOUD, IOT, AI & SECURITY"

FINAL

The Mind of the Hacker - Insights from GCHQ, MI6 and Israeli Intelligence

Introduction:

Manek Dubash, NetEvents

Panellists:

Brian Lord, OBE	Former GCHQ Deputy Director for Intelligence and Cyber Operations; Managing Director of PGI Cyber
Guy Franco	Ex-Israeli military intelligence; CTO & CO-Founder, Javelin Networks
Arthur Snell	Former head of the Prevent programme at the Foreign Office
Alan Zeichick	Tech Analyst, Camden Associates

Manek Dubash

Good morning. Good morning, NetEvents. I can't hear you. Good morning. For those I've not met before, my name's Manek Dubash, I'm your MC for today. Delighted to see so many friendly old faces, if you don't mind me saying so and to see some friendly new faces, that's good too. We have a fascinating day ahead of us, talking mainly about cyber security, intelligence, cyber-attacks and terrorism, amongst other things.

I think it might be appropriate just at this moment, before I get into the detail of what we're going to do, what we're going to talk about, just to give us maybe five or 10 seconds of thoughts about the seven people who were killed in the London Bridge attack a few days ago and the 22 who were killed in Manchester, just shortly before that.

So that kind of sets the scene really to the backdrop, if you like, without sort of - to what we're going to be talking about today. We're going to have a presentation on the mind of the hacker from Brian Lord, who is former GCHQ deputy director for intelligence and cyber operations. This is a first for us, this is going to be a fascinating talk. Brian said he can talk and talk and talk, but I think we're going to have to cut him short at some point. He'll then be joined on stage by Arthur Snell from MI6 and by Guy Franco, ex-Israeli military intelligence. So you have a lot of brainpower there hopefully and some questions and answers after that.

We'll be talking about tracking and attacking the hackers, we'll be talking about combating the current threat landscape. We're going to hear a guest speaker presentation, another keynote from Galeal Zino, founder of NetFoundry. We'll be talking about leveraging the efficiencies of the data centre, led by Clive Longbottom. We're going to be talking about SD-WAN today and tomorrow, the security issues of passing that data across the public internet. Tools and techniques for protecting the endpoint and a whole host of other things - and my agenda's fallen apart.

The way it'll work is we'll be talking this morning here in this room and then we'll have some lunch and then this afternoon there'll be some meetings, between the press and analysts and the vendors and some of the vendors - and again this is another first here at NetEvents - will be talking to some of their potential channel partners, led by Keith Humphreys at euroLAN Research.

I'm not sure there's much else I need to say up here, apart from to say welcome, delighted you could come here today at this city not reeling, but standing firm. Okay and without further ado, I'd like to introduce Brian Lord from GCHQ - ex-GCHQ, I should say - to come and give us his wisdom on the mind of the hacker, ladies and gentlemen.

Brian Lord

Thanks very much indeed. My name's Brian Lord, I'm currently managing director of PGI Cyber. Before that, I was deputy director for intelligence and cyber operations at GCHQ. Those of you who've heard me speak before, I have three particular bugbears about why the problem of countering cyber is as slow as it is. First of all, let's try not to use the word cyber, because it's an awful word, it doesn't mean anything. It means things relating to computers, which is just about everything that we use today. But it is a word that is used, it's a word that is adopted generally when government organisations or CSOs or CIOs need some more money, they create the word cyber and try and get more money to do what they want to do.

I have three big bugbears about why we are where we are. First of all, from the time that I was in government, government has always had an inability to be able to talk to industry about what the nature of the threat is. Governments by their very nature are securocrat and that's not a criticism; it's a fact. They care about security, they care about the security of the nation and therefore, they will portray security risks very highly and with increasing levels of passion. Industry have a very different view on threat and tolerance of risk. Their tolerance of risk is far higher and therefore, governments and

industry struggle to talk to each other effectively, to be able to genuinely explain what the nature of this cyber risk is.

Secondly, the IT security industry, information security industry, are all extremely good at saying they have the solution. Everybody has a shiny box which always is the cyber silver bullet to all cyber problems. There is no one solution to this problem and there never will be one single solution to this problem. I think it is always worth the IT security industry remembering that there are still a lot of elements of industry, particularly industry who remember 1999, when they were told that aeroplanes would fall out of the sky, satellites would spin off into space, screens would go blank and the world would end as we know it. That didn't happen. So as a consequence, the perception of advice, information from the IT security industry is jaundiced by history. Selling by fear never works.

The third element is media. The media love reporting this stuff. Everything is a cyber-attack, everything from let's say website defacement, which I call vandalism, all the way through to an attack on the critical national infrastructure, which I call an act of war and everything that sits in between is always reported as a cyber-attack. Cyber, bit of a scary word, attack, very scary word, put them all together, it sells copy. It doesn't help, it doesn't help the public understand what the problem is, it doesn't help industry understand what the problem is. No other nefarious activity has such a wide spectrum covered by two single words.

So what we are looking at now, what we are looking at now, is an environment where nobody really understands what they have to protect themselves from, nobody really understands why they are at threat or from whom. So as a consequence, we end up with decision-making stasis, decision-making stasis at industry level, where organisations don't know what to buy, CEOs, CFOs don't know what to believe and so as a consequence, nobody invests in anything.

I'm only going to concentrate on three things. The online hostile capability is incredibly wide, I don't have time to talk about them now; I'm going to talk about the three major threats, or certainly the three threats that have the biggest impact. First of all, crime. Let's not forget in all this world about state attack and state rigging of elections and state attacks on critical national infrastructure, between 80 and 85 per cent of all hostile activity online is carried out by criminals, pure criminals, that's all.

Now let's just take a look at the spectrum now of criminal activity. Criminals are operating in an online sense of being able to walk into the equivalent of a town centre, where everybody's doors are open, windows are open, tills are open, safes are open, cars are left there with the doors open and the keys in and no one is watching. That is the environment, that's the criminal environment that exists at the moment. So anybody with a basic set of skills can carry out a criminal act.

So what is it criminals are after? Primarily we now have to recognise that all our industry, all our industry is dependent upon IT, all our industry is dependent on the internet and connectivity. Every single - I look in front of me, everybody operating online, everybody operating on laptops, can any of you understand or can all of you put yourself in a position where the ability to have IT was taken away from you. As an

individual and as a company, that ability to have data now suddenly has a commoditised value to a criminal. This is, for example, where ransomware, or the concept of ransomware, or anything to do with ransom online comes from. Organisations that are solely dependent on processing data will, to a greater or lesser extent, pay to have that access restored if it were taken away from them.

Now criminals know this, criminals know this and they have taken it and they have adopted that and they've rolled it out against small individuals, or individuals and small businesses. Why? Because it's easier to do it like that, but are now continuing to work out how can we do that, how can we take that capability, how can we roll that out against larger corporate organisations.

Let's not just consider ransomware as a specific issue and let's take the concept of ransom, which is increasingly growing. The ability for criminals to steal data, copy data from corporate organisations and then simply demand money to have it put back, to have it returned, to make sure it is not publicised, to make sure it isn't made public. How much money would organisations pay for that? This is the modern online version of kidnap and ransom. It is happening, it is happening more and more and the more dependence we have, the more dependence we have on processing data, the more attractive it is to a criminal mind.

The other element which has a commoditised value is personal data itself, personnel data itself. People's personally identified information now has a commoditised value on the dark net. If I steal a whole load of people's personal information which organisations hold, I can sell it, it has a value. I can go online and sell that information and people will buy it. So unless organisations - and so if I want to go and steal a lot of people's identifiable information, I am going to go after the organisations who store an awful lot of it. That is simply a criminal fact of life. It's a commoditised data so, therefore, I will go after it to take it to sell it.

Now this is why, for example, the GDPR - the latest piece of regulation to come out of the EU, which regardless or not of Brexit, will apply in the UK - imposes massive fines on organisations for losing personally identifiable information. Four per cent of total global revenue is the maximum fine, that can be fined for losing people's personal data. This is primarily because we as organisations have adopted the use of technology, but have not invested in the security to follow it up. Now in no other crime - and I think it's probably worth bearing in mind this is where it's slightly different - in no other crime is the victim also looked through the same prism as the offender.

If you are a large organisation and somebody hacks into your system and steals your data, at one level you're the victim, but at the same level you are also viewed as the offender because you have not taken enough effort to look after the data for which you are responsible. This is an area we have not yet normalised. However, what I would probably say to the vast majority of crime, I'd say about 85 per cent of all online activity is criminal. About 70 to 80 per cent of that is basic opportunist criminals. These are low level people, these are low level people with basic skills, using publicly available tools, just exploiting a very, very rich marketplace at the moment.

All we need is a responsible IT security market to sell basic tools, advise on basic control measures and basic education and in effect, the vast majority of that problem will go away and it will leave. What it will leave then is the serious and organised crime capability. Now the serious and organised crime groups are not new to law enforcement, there have been serious and organised crime groups around forever. But what we have to be able to do is strip away, take away the peripheral opportunist crime and leave the fundamental problem, which is serious and organised crime groups.

Now serious and organised crime groups primarily are not interested in one-off, single opportunistic crimes. They are now looking at getting to the heart of the banking systems, getting to the heart of the payment systems. The general view from most serious and organised crime groups at the moment is any operation, any single operation needs to be able to yield £1 billion for it to be worthwhile doing. That is where the serious and organised crime groups are operating now. Large scale, wide, global attacks on banking payment systems and large scale data theft and processing. That's the area of crime.

The other area we then look at is state. Now a lot is said about state capability, now all states, every single state is looking at cyber and saying at one level how do I weaponize this. That is not new, that is not particularly unusual, every single time a new type of ability or capability is being developed, countries have looked to weaponize it. They do it with air power, they've done it with sea power, they've done it with any kind of power. The environment of online activity is not new.

What I will say is this. Being able to develop coherent, coordinated attacks against critical national infrastructure in a way which delivers a very specific sustainable effect is extremely difficult to do. It's extremely expensive to do and it involves a huge amount of effort and we need to put that into perspective. There are a few examples of very, very focused activities which have taken several years to develop in order to deliver an effect. But the general view at the moment that states have the ability to act randomly, take down critical national infrastructure in a meaningful way, is not the position.

States are developing that capability, they are developing that capability slowly and they will get there. But if one looks at the example of the Russian attack on the Ukraine, the empower system in 2015, yes, they delivered an effect, they delivered an effect only for a matter of hours. That was an element of power projection rather than a deliberate effort. That is because the capability being able to sustain that, the ability to sustain that capability is still not here. The same attack, TeleBots attack against the Ukrainian banks, same kind of thing.

If one looks at the TV5Monde issue, when TV5Monde in effect took their own systems offline as a result of a cyber-attack, that was simply a state determining exactly how capable they were on taking a TV system down using the Charlie Hebdo attack as a flag of convenience. Once again, the ability was not sustainable for any length or period of time. We've seen the German steel manufacturing plant go up in flames. That was a result of an R&D operation, a research and development operation which went wrong. All this means that the state capability is growing and it's developing, but it is not of the dramatic world that we see now. It will happen and states are making it happen, they

are development their capability, but let's just keep that in perspective as we look at other areas where states are investing their capability.

The second is the ability to influence the internal affairs of other nations. This is not new. So the absolutely outcry we heard from the United States about the Russians interfering in the US presidential election and the Russians potentially interfering in our election and the French elections, states interfering in the internal affairs of other states is not new. The use of cyber, the use of online capability, the use of false news, the use of disinformation is a tool as old as the hills. We just have to be able to recognise that, we have to be able to make sure that the public understands how to identify it and we have to make sure we understand how to report it. We will not stop it from happening, we will not stop it from happening because it is state activity and believe me, the Russians are not the only nation in the world to try and manipulate the internal affairs of other countries. All states do it, they always have done it and they always will do it.

But the area in where state activity is growing and growing significantly and growing in some areas greater than others is the area of economic espionage and economic secrets stealing, industrial secrets stealing. Historically, state capability only ever focused on the top level priority, which was generally areas of defence, foreign policy, intelligence agencies and security. So they deployed their intelligence gathering capabilities at the highest pinnacle of the requirements that they set. The ability to be able to exploit data, the ability to be able to hack into computers, the ability to be able to extract information in large scales, the ability to be able to take information, store it, index it, search it without ever having to read it all in its totality has changed the dimension of state espionage. Therefore, states themselves will now and are focusing their intelligence gathering efforts because they can and they have the resources and capability to do so around economic targets.

So industrial targets are far more than they ever have been subject to state attack. Large contractual deals, large merger and acquisitions data, large commercial data, product IP, geological data for extractives, all of this is now randomly, regularly taken from corporate systems and taken and stored to use for national economic effect. The UK does not do this. I'm not saying this for effect; the UK does not do this, it does not have the remit to do this. My view will be increasingly the UK industry is not on a level playing field internationally, it's not even on a level playing field with some of the countries it calls its allies in this space. There is a gradual change around the general acceptance of this activity and that is an area that we probably need to track quite carefully.

So the areas of state capability, still in the foothills of capability on mass industrial disruption and weaponization will continue to interfere and influence the internal affairs of other countries through disinformation and the ability to be able to do state espionage, commercial espionage, at scale.

The final area I want to talk about is terrorism, which is particularly relevant. One of the areas I get asked about most of all is what is the impact of online capability in support of terrorism. The first thing I will probably say is that terrorist organisations, going back to the state capability to take down critical national infrastructure, to be able

to attack critical systems, that is not at the moment either within the capability or even the mindset of terrorist organisations.

Terrorist organisations still focus their online activity in two particular areas. First of all, they will use it as a criminal element to be able to gather money and obtain money for their cause. Secondly, which is the biggest area and the biggest area of concern, they use it to fund their propaganda effort. They use it to fund their online social media, their online radicalisation capability and this is the area of biggest concern around. So when we talk about cyber terrorism, we should not get distracted by thoughts of terrorist organisations trying to make trains come off the tracks, aeroplanes fall out of the sky. That is not within their capability or mindset at the moment.

What they are looking at is how they use our use of social media in a way to be able to radicalise and turn people and organisations to support their cause. The biggest challenge I always have from the media questions that I get is what role should the social media organisations play in this. I have one very firm view around this, which is national governments struggle with the concept of the positioning of social media organisations at the moment, which generally is not of the most cooperative sense.

I think there are two things around this. If one looks at Facebook, for example, Facebook provides a social media platform for getting on towards a quarter of the population of the globe in terms of users. No organisation can operate, can provide that level of public service - because that's what it is, a public service - and still abrogate its responsibility to work collaboratively with governments in order to provide them the data that they have. It is not a sustainable position for social media organisations to not do anything about online radicalisation, nor is it sustainable for them to continue to withhold any degree of cooperation with law enforcement.

It is not sustainable in any society whatsoever and I sense there is going to be a change there, but the change primarily has to be a balanced one, because security organisations, intelligence agencies, law enforcement agencies, are used to getting what they want. They're used to producing a warrant, they're used to producing a piece of information and getting the information they want. That's not going to happen either. In reality, a level of cooperation between state and industry, state and social media platforms, is going to come between two horses, but it has to happen. It has to happen because it isn’t a sustainable position anymore, where we have incidences like Westminster, we have incidences like London Bridge, where online radicalisation, images and encouragement online cannot be hosted anymore and I think we will see a change in that.

Secondly, if I was being defensive, or if I was being supportive of the social media organisations, is they are still very young, they are still very young organisations. They may be global, they may be huge, I do not yet think they understand what (1) their responsibilities are in a world of social media, but (2) I don't think they genuinely understand the influence they can and can't have. So our approach to social media, our ability to social media and as an industry, how do we help social media overcome this problem, is the biggest challenge.

So what we now need, which I think is to be the focus of the rest of the day, is how do we help law enforcement, how do we help the agencies develop the tools to be able to

take the vast quantity of data, the huge quantity of data that is available. How do we help them profile it, how do we help them identify trends, how do we help them identify the tools, the techniques, the capabilities which threaten our country and our industry, whether through crime, whether it's through counter-state activity, or whether it's through terrorism. There are a lot of tools, there are a lot of capabilities that industry have that can support our law enforcement in that way.

How do we help social media, how do we provide the tools that allow the social media companies to maintain their support to their consumers of privacy, whilst still accepting their social responsibility towards providing the state with what they have. There are tools, there are security mechanisms, there are devices that exist and prevail in the world at this time. How do we continue to help educate our public, the whole public on what cyber security means, what false news looks like, what disinformation looks like and how do they put the most basic measures and steps in place to be able to counter what is basic opportunism, low level crime.

Because once all those low level opportunist crimes go away, the threat becomes normal and it then becomes the normal threat between law enforcement and serious and organisation crime, law enforcement and terrorism and state on state activity. There is nothing complicated about this stuff, there is nothing difficult about this stuff, but what this actually means is we need to be able to work far more coherently between media, industry and government, closer than we ever have before, against any other type of threat, because the solution to the threat lies in industry, not in government.

I'll pause there and bring up the other panel members.

Manek Dubash, NetEvents

Brian, thank you very much. Now I'd like to invite Guy Franco and Arthur Snell to come up and join Brian and of course, our interlocutor, Alan Zeichick, who's going to give them a hard time.

Alan Zeichick

Good morning, I'm Alan Zeichick, with Camden Associates and my specialty is cyber security. I'll try not to use the word cyber too much out of respect for Brian's sensitivities there. Let me start by asking our panel, it sounds like we have something that's been going back, I guess, to the days of the Greeks and Romans, that we have states and law enforcement agencies on one side and I'll call them bad actors on the other, whether they're state actors or criminals or whatever. As we talked about over breakfast before the panel, this is something that's been going on for thousands - I'm sure the Babylonians had their problems with their equivalent of cybercrime and people forging cuneiform messages to get treasury transfers.

So in this kind of arms race, where would you say - it's a two part question. The first part is where would you say the bad actors have the advantage in their use of technology? So the fact that we don't know who they are, so they could be doing coded tweets at each other and we don't understand it. Or the fact that they can use end-to-end

encryption or - to start with, where do the criminal, terrorist state, where do the bad guys have the technology advantage today?

Guy Franco

Sure, so I'll divide it into a few areas where I see that attackers have most of the advantage already, defenders. First of all, we need to understand that the attackers, what they usually do, the misuse of trust. Basically whenever there is IT infrastructure, I can always abuse this IT infrastructure, whether it's the server that actually manages all the assets, like the active directory, or whether it's the mail server that's actually responsible for all the correspondence between the persons in the company, the exchange server. So misusing the trust is something attackers always do and that's the first problem of the defender. If the attacker looks like a user, how can you differentiate between what the user is doing and what the attacker is doing, because at the end of the day it's all about stealing identity of regular user accounts and then…

Alan Zeichick

So they have a badge?

Guy Franco

They have a badge. So what do we do about that? So that's the first problem here and this is a huge gap that's really hard to close. When we're talking about bad actors, whether it's nation state or the others, they're always in these same methodologies. Now for the unknown or the exploitation of zero days and stuff like that, it's usually more down to the state sponsored campaigns because it requires a lot of information, a lot of money. Usually when we're talking about a state sponsored campaign, they are using it only for the initial intrusion. Afterwards they are still using the same trust and they misuse the trust after they gain a foothold in the company that is being managed centrally. So using the IT infrastructure to your advantage, as an attacker it's probably one of the only ways that I won't get detected anywhere.

Arthur Snell

Thanks, good morning, everyone. I'm the one person on this panel who's not a technologist, so I was going to take this question from a different angle, which is actually in terms of the impact of communications and the impact of events and the way people act. So I think in terms of we're looking at what are the advantages that the bad guys, to use a straightforward term, what are the advantages that they have, of course, the big advantage they have is that classic thing that terrorists say, that we only have to be lucky once, you have to be lucky every time. Of course, we saw that again tragically in London over the weekend. If we think about what happened during the London Bridge attacks, the media message at the moment, understandably, is about the horror, about the tragedy, about lives lost, people who were enjoying themselves suddenly pitched into this ghastly situation.

But there's another report you can write, which is in a completely uncontrolled environment, in Central London, on the busiest night of the week, within eight minutes

three attackers were shot dead by armed police, in a country where armed police are not routinely armed. Now that's an amazing story and the other thing that's amazing about that is that I genuinely believe that 10 years ago, had the same attack happened, this might have gone on for half an hour before police were able to intervene.

And I'm a former government servant; I'm not taking any position on the public debate about whether the Police have adequate funding, whether or not it's going to become an election debate, as you're all aware this week in Britain.

So coming back to the bad guys the terrorists, the criminals or even governments who are trying to undermine other nation states, the advantage that they have is the ability to make people worry, and the ability to cause people to expend extraordinary costs on things that they may not necessarily need. As Brian said in his earlier presentation, criminality has always existed.

Now, of course, if you give criminals an environment where the doors are unlocked, the key is in the ignition, they will take advantage. But equally, if we stop doing things, because we feel that it is unsafe to do so. Or it is somehow necessary for governments to limit the ability of people for example to communicate privately, then of course we start limiting the ability of the economy to grow just for example so I think that's one way to look at this.

Brian Lord

And I think the other point I would make is that criminals, terrorists other states they are operating in what is a completely unregulated uncontrolled environment in a way in which security organisations are not used to operating. They operate across geographies and therefore they exploit the fact there are no actual international, meaningful international cooperation protocols in how to counter this type of issue. In order to counter it, it requires a lot of international law enforcement collaboration, which just does not exist at the moment.

So the environment for them to operate they have the advantage, they operate across borders. They can carry out activity in one country without leaving another country. And that just creates a set of problems, not insurmountable problems, but a set of problems where thy have the advantage at the moment over intelligence agencies and law enforcement.

And to pick up Arthur's point I think when we say if we put it into a real world context had London Bridge happened four or five years ago it would have taken an hour, two hours for the Police now it takes eight minutes. That is what's going to happen in countering the cyber threat, is the ability to able to counter these types of activities will get quicker, will get faster. But the problem is that at the moment the security apparatus are lagging behind the technology and the tools and the environment, which is creating a very enabling environment for the criminal and other hostile communities.

Alan Zeichick

Okay, with that said though let me flip my question over. Let's talk about we'll call them the good guys. Now without getting into politics and everyone's view of whether what the State is right or wrong, so you have the attackers, we are calling them the hackers here you have the good guys, who I'm going to divide into two groups. One are the State good guys who have apparatus's like they have warrants, they have human spies, they have super computers, they have what not. And then you have the non-State good guys, businesses, banks, hospitals, consumers. Where, if anywhere, do the defenders have an advantage in the cyber war?

Guy Franco

Yes, so I'll answer it. I think the defenders can get the advantage where they are doing all the preventive stuff they are still doing, using all the methodologies they are still using whether it is endpoint security or firewalls. But going also after proactive measurements, meaning trying to find and hunt down attackers that are already there and you just need to look for the signs. When you look for the signs, you will probably find them. And working with basically proactive measurements will help you to securing your environment much better.

The problem there is that currently the IT and the security market doesn’t have the right amount of people and the right amount of education to do this kind of stuff. And I think we all should look at it as currently the future, because preventative is good until some point. Afterwards you'll have to do the work yourself to find them. And usually I find it much, much more precise and much more beneficial when you take proactive actions.

Arthur Snell

I wanted to pick up on this point about an advantage the good guys have, which is to reinforce that point. If you look at this issue of consent in the public, coming back to the issue of conventional crime or terrorism, one of the things that all governments depend on very heavily is, of course ordinary people doing the right thing. Whether it's if you see an unattended bag, you notify the authorities. If someone drops their wallet in the street, the fact is most people will race after you and give it back to you. But if someone leaves their Wi-Fi network unsecured most people would just log on and use it. So that's the kind of difference.

And I think that people, and it comes back to the point that Guy made about education, people need to be better educated. People have a good understanding in a simple way and some people obviously in a more sophisticated way about physical security, about how they can be safe generally. But I think a lot of people, I'm sure people in this room are not in that category, but a lot of people have zero understanding of online safety. And not just, as it affects them personally but of course, how they can inadvertently undermine other people's safety. So I think that thing of education, the most powerful force in any country's security is the population not actually the uniform security.

Brian Lord

So I think where do organisations have the advantage. I think picking up on Guy's point proactivity is key. And proactivity isn't there at the moment. If one looks at the National Health Service, the issue with the National Health Service in the UK two weeks ago that, regardless of the nature of ransomware and so on the impact of that could have so easily been avoided, it could have been so easily been avoided by basic proactive measures. This was not -- these are not high-tech proactive measures. These are just basic maintenance patching, what I would call hygiene measures that had they been in place, yes, there might have been one or two pockets of ransomware that had an effect but they would have been dealt with.

So the fact is businesses and government organisations if they do the most basic things correctly will raise their health, their hygiene above the threshold of most, most, opportunist criminals. And so in the short-term that gives them a degree of protection, because there is still a wealth of other targets for criminals to go after. Thereafter, as Guy says, they then start investing in the kind of proactive intelligence investigative tools that can identify where they are being looked at, where they are being attacked.

Where they, however, still are not utilising what is available to them is the area of sharing of that information and intelligence. And the reason being the reason for that is there is still a level of reluctance to admit when an organisation has been breached for two reasons. One they worry about competitors taking advantage of it and they worry about regulatory fines, so as a consequence they tend to not…

But the worst element is going back to Arthur's example of people just going well I'll hack in somebody's Wi-Fi. It is still not considered to be a criminal act in the same way as any other criminal act. So actually, the vast majority of these don't even get reported to the Police. And if it is not reported to the Police how can we get a sense of what the nature is, how can the Police really do an effective job. So we are still in the infancy of being mature as a society about…

Look, if you get hacked, if you get breached, you get hacked, you get breached it's a fact of life. It really is a fact of life. It's nothing to be ashamed of. It's nothing to be embarrassed about if you put the most basic measures in place. And that's I think a lot of space where both businesses need to do and governments need to be able to encourage the information sharing and visibility over breaches rather that at the moment there's still a lot of opprobrium being levied on organisations because they've been breached. And that we are losing an advantage there, a significant advantage there.

Guy Franco

Just to emphasis what Brian just said, I think there is a lot of difference on when do you find the attack. If you find the attack on day one or day 10, you are probably in good shape, because the damage that's already done is probably very low, they haven't had a lot of time to make their recognisance, the right recognisance in the network. They didn't have a lot of time to investigate where are the important assets.

But if it's -- usually now we see the statistics now stays on 160 days until they find the attack. And usually it's from a third party, meaning they themselves didn't find the

attack someone told them got breached. Now at this point it's already game over because they already got what they want. And the crucial about finding the attack when it happens or close to when it happens is the most important thing here. We can talk about preventative, it's always good to talk about preventative but proactive will get you from finding the attack on day one or on day 200.

Brian Lord

And there is an issue here about language, because hackers are no different to any other criminal or nefarious activity they do recognisance, they want to succeed. They do recognisance, they look at your network, they find the vulnerabilities, they move about your network. And as Guy says by making sure, you have the tools there to detect that recognisance you can counter the threat before it becomes a breach. And there is a difference, so you breached as an organisation when people start looking at you. You then get breached when they want to carry out the additional attack. And we sometimes cloud that in our analysis. There are different stages to that.

And the same applies to state attack on critical national infrastructure. What we see at the moment when our governments get, quite rightly, horrified because state A is all over our electricity system, state B is all over our TV system, this is just recognisance. This is just state recognisance in the same way as state's always do recognisance against everything else. It's no different to having a satellite four miles above your manufacturing plant. It's just this is what states do. And so being able to detect them in that phase and making it difficult for them to operate generally means they'll go elsewhere.

So I think we need to start looking at it in those kind of staged approaches. Whereas at the moment everybody just sort of lumps in oh cyber threat, cyber risk oh it's all too big what do we do about it, and I think, instead of breaking it down into logical approaches.

Guy Franco

It's all about ROI. If, like Brian said, like 85% of the cybercrime today belongs to criminals and they want to gain financial gain from it. If the ROI of that will be high enough, meaning they will need to invest a lot money to succeed in their attack they will most probably fall back and try to find another target.

Alan Zeichick

The issue that's been going on for 30, 40 years now is that the designers of the internet were very idealistic, very happy people and they created something open. And security was bolted on later, and as we, all know if you don't design something to be secure from the beginning, it's not secure. That's what drives, for example, a lot of the problems with email, email was designed not as a secure protocol, centres are not authenticated and so on so that's how phishing works or can work.

And we are seeing this everywhere, with the Cloud, with Internet of Things, with wearable's and health systems. First inventors, start up's make great products, people love them and then we discover that they weren’t secure by design and they become

exploited again by criminals, by states or whatever. Remember Dick Cheney, Former Vice President of the United States when he had a pace maker installed insisted they turn off the remote management capabilities of that because he was worried that a bad act could stop his heart. And who is to say that wasn't correct in that paranoia.

Is this ever going to change or are we doomed to always be playing catch-up. That first, we build things, we build shopping malls, we build whatever and then we go back later on and say oh we need to put guards in it. Is that going to be always the case with all these technologies, Cloud, IoT, AI that they're designed to be open and idealistic and then later on we realise that they can be exploited.

Guy Franco

I think the problem here is that security always comes with a price and the price here is operational. So it's always a balance between security and operational. The more security measurement you have the less operational the system will be. So you will always need to find a balance.

I think today when people develop new tools to the market, develop new technologies security does come to mind. Security is a big issue for every company, for every developing company out there. But they still need to make the balance between the operational and the security it can't be just security.

Brian Lord

I agree. But I think the one thing, you're right, the developers the people who introduced the internet and helped it grow we would -- the one thing I will say we would not be in the position, the positive position we are in globally if security had been introduced at the outset of that, I guarantee it.

We as a society -- we've always got to remember this about cyber security is that the benefits that technology brings us as a nation, as a globe, as a world are huge the internet has brought such massive enablers. And security, the risks that are brought from security is only a small percentage of that so let's keep that in perspective.

We wouldn't have, internet would not have been able to deliver the fantastic things it has done if security had been built in right at the outset. We just wouldn't have taken the chances we wouldn't have been innovative. So I think in some ways the fact that we had to play catch-up is a good thing, because it allowed it to flourish and then we've got that kind of positive mind-set.

But as Guy said, I think what is happening now it's all about the evolution; it's all about the normalisation. People are just starting to build in security as a thought process when they're introducing new capabilities. I'd rather have it that way round.

The one thing I've always said is when I've given advice to companies is the last thing you want in your IT department is a load of security, IT security people because they'll bugger it up from the day one, they will absolutely destroy it from day one because that's what they do. Security people are like that. If it's not secure, it's not secure.

So it's always just use the innovation and the imagination and just allow security to develop and evolve through osmosis of those people. Occasionally you need to give it a shove, occasionally you need to give a jolt, but let's do it that way round rather than getting a little bit too constrictive.

Arthur Snell

I think there's a very good analogy here with air travel in the sense that we all remember the days where even if you didn't have a ticket you could probably convince them that you had a booking and you'd wander on. And, of course, now travelling anywhere by plane is such a nightmare you feel like you have to sort of undress before you've even got anywhere near the flight, you forget your bottle of water and all the rest of it. And there is a practical implication of that, which is for very short-haul flight most people will always try to avoid flying, take the train, take the car whatever. Obviously, there are still journeys you have to do by plane so you do them.

And this comes back to Guy's point about the impact on operations. You can make flying completely secure if everyone had to turn up, strip naked, put on a jumpsuit and sit in a secured hold. But most of us would probably not to do that as a means of transport so these balances exist there. And ultimately the most secure systems, and I speak as someone who has worked inside government, are some of the worse systems, the most user-unfriendly systems, impossible to do the simplest things with. So we all live in this -- we have to make choices ultimately.

Alan Zeichick

So it's a trade-off. And speaking of trade-off's we are not going to trade-off from my questions to your questions. And here we have a roving microphone. So raise your hand to flag the microphone. And if you could say, who you are and whom you represent.

Audience Q&A

Hector Pizarro, DiarioTi

My name is Hector Pizarro from DiarioTi. I have a question regarding the security by design, which sounds like a very good idea and probably software would be a very important area to deploy it to considering that most of us use software. I think that isn't it a challenge that software companies and platform companies like Facebook, Google and other products they try to get as much data as possible from the users, whether they agree or not, whether they know it or not.

And then this creates the need in some privacy aware users to protect their data from these legitimate companies that are selling them onto other companies as well like Facebook does. So then by doing this they need to control the software and tweak some -- the configuration in the software, but then they would be exposing the software to attackers.

So do you see a challenge there that companies, software providers and platform providers, should need to behave themselves in order not to create in user that need of protecting themselves that then again would expose them to attacks?

Alan Zeichick

So are you talking about that they should be gathering less data that that makes them less of a target or that they need to have better security in their platform or both?

Hector Pizarro

Well actually, both if the idea is to embed security in the software then people would need to trust the software vendor not gathering more than necessary information from them, so not everybody will feel the same need to tweak their operative systems for instance but those who are aware of it.

Arthur Snell

I would just say, and I'm not as I said at the outset, a technologist so I'm not going to talk about software development. But I think there is a point about data where a lot of companies exist in the social media space particularly where their primary revenue source or certainly their primary expected revenue source for the future is the sale of data.

And yet the users of those systems have no conception of that. They think Facebook is there so that they can share pictures of cute kittens, and they don't realise that Facebook exists to sell data about people. And, of course, a lot of other less well-known platforms and apps are even more or even less responsible in the way that they use data. And the classic thing is what's on page 13 of the terms and conditions that no one ever reads.

So I think better public awareness about the significance of this market for data, some people are calling it the new oil, is very important. At least individuals then will make a decision. I am participating in a marketplace where I sell me, do I want to do that. That's a decision that people need to understand that they're making.

Brian Lord

That's a good point. I might take issue a little bit, if I may. Is that I have had discussions with a number of people from a number of backgrounds who recognise that their online experience of being able to do online shopping and being prompted of what to buy because of -- based on the fact that their data has been sold, they actually find that quite helpful, they genuinely do. A number of people have said actually I'm quite happy, I'm quite happy that Google has my data, that Facebook has my data because it makes my life easier. It made my online shopping experience, it means I don't have to remember my mother's birthday because Facebook tells me and it also tells me what she likes for birthday presents as well. So it fundamentally makes peoples life easier.

Now the interesting point around that is that this does demonstrate a shift of people’s attitudes. I'm quite happy for organisations like Facebook and Google to have my data and I'm relaxed about that. Interestingly, government have still yet to make that case to

persuade people that government should have access to that data for security reasons. And I find that really quite extraordinary. I have spoken to very well educated people go yes fine Google and Facebook can have my data because it makes my life better, government haven't made the case to me yet sufficiently for me to be persuaded that I want to give them that, so there is a risk there.

The point that you make about building security in, of course, they should. And this comes back down to the retrofit, not quite retrofitting of security but getting security to be an integral part of development of platforms on the internet. This comes back down to the point that I make around Facebook, Google these large organisations of course they should, all their coding should be secure, every single application they roll out should be secure because they are supposed to be a responsible organisation. And if they are not, if that is not built into their design then they are being negligent.

And the final issue, which I haven't mentioned but it, is the same point about that, is these organisations have to be able to collaborate and cooperate with governments. They cannot anymore operate in this singular view, which is hey we just provide the platform we don't really, that's just not, that is not a defensible position anymore.

Guy Franco

I really agree with Brian. I think -- I know privacy is important to everyone but there is a lot to gain from sharing your data with these companies. They can give you direct advertising that you can't get anywhere else. They know you better than your mum. It's funny to say that but that's true. They've got more information about you than any other person on earth. That's why I think it's dangerous but at the same time, it gives you a lot of benefits, because it knows you and it can direct basically advertisements just for you.

Now when these companies share data with other companies I tend to feel pretty safe because they don't share personal information. They share contextual information meaning they share what you like and what are your hobbies and stuff like that with other companies. But the other companies don't really know your name. They don't have personal information about you. So when we are talking about big companies like that I'm feeling pretty safe regarding my data.

Now generally speaking about personal information I think most companies doesn't do a really good job about it. I think it comes usually from development of start-up. Usually you need to work with very lean methods and you need to execute as fast as you can and usually security you get from down the way. And afterwards you think about it, yes I might need security here and here but it usually comes after the fact. So giving personal information I would certainly think twice when giving it to basically a service I don't really know.

Alan Zeichick

Great, and we have time for one question but it has to be a quick question and then quick answers, quick question and quick answers.

Oliver Schonschek, Insider Research

My name is Oliver Schonschek I am from Germany Insider Research. One short question, you Brian said that it's the task of the industry to make the internet more secure and not only of the government. But if you think of IT products with all the weaknesses isn't it also a question of quality that the government has to ask for certification of IT quality because the weaknesses in IT products are so huge, and they shouldn't be sold at all sometimes.

Brian Lord

That's a very good point. Government endorsement certification of certain products I think is helpful. I think when there is a -- but I think - to surround it quickly - there is a balance to be drawn between government certification as a guide for users to say our view that this product meets a certain set of standards is one thing. I would be cautious about governments being prescriptive about what can and can't be bought because that removes the element of choice. But I think, yes, some degree of government recommendation certification of certain types of products is always -- and services, not just products but and services as well is a very helpful thing.

Arthur Snell

Well we are going to make quick answers, I agree with Brian. I think great people expect quality in lots of other retail transactions they make and it's not unreasonable to expect the kind of maturity to develop in this sector, which probably as ever it's developing ahead of regulatory catch-up, but we might get there eventually.

Alan Zeichick

Let me ask you a very quick follow up though then we can all go down, which is should it be governments certifying? You take, at least in some countries, its private industries underwriters laboratories or whatever that certify it's not the governments that's certifying that something is cyber safe or whatever, should this be a private industry function or a --.

Brian Lord

I think there is a balance. Having government certification is one thing you can have academic certification, which is another. I think independent certification rather than self-certification is always a useful tool to allow purchasers to determine what is good and what is bad. But I wouldn't necessarily say it had to be government.

Guy Franco

I don't think it has to be government also.

Alan Zeichick

Well thank you. And thank you very much.

Manek Dubash

Thank you Alan. Great panel. Thank you to Arthur, Guy and to Brian. I think Guy is going to stay on the stage, because this certainly was one of the most interesting panels we've had in a long time, so thank you again all of you for your participation. I'm sure there's lots of meat there.

[end]