NETEVENTS

GLOBAL THREAT LANDSCAPE: HOW CYBERTERRORISM DEFINES INFORMATION SECURITY

FINAL

Global Threat Landscape: How Cyberterrorism Defines Information Security

Chair:

Joel Stradling, Research Director, GlobalData

Panellists:

Roark Pollock	Chief Marketing Officer, Ziften Technologies
Ray Ottey	Fellow Cybersecurity Practitioner, Verizon
Andrzej Kawalec	European Director of Strategy and Technology, Optiv
Joe Baguley	Vice President and Chief Technology Officer for EMEA, VMware

Joel Stradling

Okay, thank you, welcome to this conference debate, the Global Threat Landscape: How Cyberterrorism Defines Information Security. I've already introduced myself, because I was just on up there with Joe. What I'd like to do first of all is for the panel to introduce themselves, perhaps moving - starting with you perhaps sir, and then we'll move to the right, yeah, to the left then.

Roark Pollock

So, my name's Roark Pollock, I run marketing for a company called Ziften Technologies, we're headquartered out of the US in Austin, Texas.

Ray Ottey

Good morning everyone, Ray Ottey, I run the security practice for Verizon, I'm that Telco, across UK, Ireland and Nordics, thank you.

Andrzej Kawalec

Hi, Andrzej Kawalec, I'm CTO and Head of Strategy for Optiv.

Joe Baguley

I'm Joe.

Joel Stradling

Thank you, so just to set the scene, I have a couple of slides here to share. We'll start off by defining by what terrorism is.

What we're seeing is that terrorist groups today, they have far broader agendas than before, beyond just physically harming civilians, which is the traditional mode of attack, hurting non-combatants. The objectives, their objectives of those groups have evolved to cyberwarfare levels, with the objectives of causing disruption politically and economically. I understand in the US there was an activity to call in 500,000 pacemakers, so potentially, and with critical infrastructure, with autonomous cars and so on, it's quite easy to see that through that type of cyberattack, physical harm is also becoming a closer reality.

Then the bottom point here is we're seeing a new supply chain emerging. So, the bottom part there, and this concept, I also spoke about with Aaron Turner of Hotshot, who will have his opportunity to speak with us today as well. Whereby all of these groups could potentially be a part of building a sophisticated attack. It's not necessarily just this cyber terror group here, hackers and lone wolves, petty criminals, may crack into a certain organisation and sell that online. It can be picked up by criminal gangs, which will be quite happy to share that with state sponsored cyberattack organisations, and then that ends up in the hands of cyberterrorists.

So that whole supply chain is changing and there's a big black market, or dark web place out there, where bad actors can get their hands on pretty sophisticated stuff. I think there was an example I wanted to raise here, where the German police arrested, something like two or three individuals just a couple of weeks ago, for their activities on the dark web. Where they'd stolen data and shared it onwards. But their other activities were actually drug smuggling, international trafficking of drugs and so on. So, these people are not just taking part in those illegal activities, it's gone up a level to cyber criminality.

The people that are vulnerable in this, businesses and governments, are increasingly dependent on automated IT systems. The management of critical infrastructure is increasingly online, cloud based, and physical device security is not very well integrated with the IT and network, and that's an understatement. Another way of saying that would be, very poorly integrated. So, all the people that are vulnerable to

cyberterrorism attacks on the IT side, are electrical companies, supply chain and transportation, so all the lights can go off, all the hospital electricity can go off during critical operations, and disruption and ransomware is taking place pretty severely in the transportation industry. Which can all have economic and political impact on countries.

Just expanding on the healthcare, to paint the picture of how serious this is, the healthcare industry itself is not just limited to protecting patient data, and related to the previous slide about physical devices not having security very well, built into them. Medical device security, compromises not just the data privacy side, but also patient safety and the whole operations of hospitals. It has been seen, that the breaching of internet of things, medical devices, is a pretty simple thing for hackers to do today.

So, these are the dangers, the ambitions and attention on national infrastructure attacks is increasing, that's a fact. The sophisticated tools are widely available on the black market, and that these are being shared. Actually, that example of the German police shutdown, is just being shared here at the bottom of the slide here. That's actually all I wanted to speak about now. The intention here was to have a good old robust debate about this, and so at this point, I'm going to just throw it over to the panel there.

If there's something that I said in the last couple of slides, that you would like to actually raise a comment or you object or you really have something strong you'd like to say. Then this is a good chance to do that. Do you agree or disagree, or otherwise I'll just get right in there with my own questions to the panel. They were really talkative at breakfast.

Ray Ottey

I'll kick off, I guess trying to frame it really, I guess from our perspective, we kind of see this as two areas. There's cyberwarfare right, and that's really an evolution of what's happened in terms of the normal evolution of war, and it's just another tool and another weapon, and it's only getting worse in that regard. But then there's the impact on business and critical infrastructure, as a by-product of cyberterrorism. Really cyberterrorism is just really a different motive, it's a subset of the wider threat, but it's just coming with a different motive. There's no different toolset, and it's not in some cases different people either. So, it can be the same person during the day being a hacker, or having a normal day job, and by evening a gun to hire. So, I think it's just framing that distinction between those two areas, I think is key to sort of kick us off.

Joe Baguley

I think the IoT that you touched on is very important, I think IoT is a really good name for it, because the biggest problem with IoT is IT meeting OT, and what you're looking at here is literally that. Is that IT-OT boundary, where Stuxnet, that was really hard from them to try and essentially socially engineer software on to those systems. They won't have to do that in 10 years' time, because there'll be ways to somehow get around that. Because we'll connect all that stuff up. What I'm seeing is just fundamental failings in basic principles of security when we get to IT and OT.

You know people deploying, oh let's put security cameras on everything, there's these cheap USB ones I found, it's like yeah, cheap USB ones, of which there is no patching model and no way to update them. It's just people missing basic fundamental steps in deploying IoT systems, that will set us up for massive failure in the future. I'll finish, my favourite is Hargreaves Lansdown in the UK, my friend's the CEO, were attacked by a cyber botnet of kettles last year, of internet connected kettles. Took down Hargreaves Lansdown trading platform for quite a while, which is you know, no one thought about patching and securing internet connected kettles.

Andrzej Kawalec

Yeah sure, [unclear] we shouldn't have said, could you put the kettle on and make a cup of tea, and the whole organisation goes down. But I think you're right, cyberterrorism is an emerging threat, it's just one of many emerging threats. IoT is going to completely explode it, and it forces us to think about devices again. Which is something I think we've forgot doing for a while, we stopped thinking about devices [and end points]. But we need to start doing that again.

But there's also a really interesting thing happening, and if you think about that that cyberterrorism domain in a sort of geopolitical sense. It's not just the fact that to perform and create a physical safety implication on a network, you used to have to have quite specific deep domain capability. You don't anymore. You mentioned that at the front, that integrated industrial cybercriminal global network, allows you to do anything, whether it's malware as a service, ransomware as a service, being attacked by swarms of kettles or toasters.

Your ability to orchestrate that has become, I think quite different, and I think the conversation shouldn't be about a step change in or a strategic shift in terrorism. Moving from using IT as an enabling function for funding, we all know that crime and cybercrime and drug cartels fuel terrorism, and that's a funding model. Use it for recruitment and propaganda, to actually being quite disruptive. I think we've seen that very, very recently in New Zealand, the use of information warfare and propaganda, to completely change the impact of an isolated terrorist incident.

All the way through to quite destructive attacks, and we don't think we've seen any of those yet. But arguably it's going to happen, and the ability to walk through the capabilities needed, to recruit to spread information, propaganda, to fund different business models, to sidestep having to have deep domain specific capabilities. Because you can just buy that, or collaborate, and you can do it in an anonymous way. You think about the, as Homeland I think identifies 61 terrorist groups, international terrorist groups. The Home Office in the UK identify I think 71, there's 13 in Northern Ireland, nobody quite knows whether that's international or not.

But I you think about those groups, and slowly and surely, their physical, geographic territories are being shrunk, and its forcing them to move horizontally into a digital twin, or an online virtual world, where they can continue their operations. Ideally, at a better scope and a greater impact. We haven't seen that tipping point. Where we've seen that tipping point is cybercrime, or actually just crime as I think we ought to call it.

Cybercrime as an industry has overtaken the global illegal drugs trade. National crime agency in the UK, moved drugs off their top three focus areas, and put online fraud and cybercrime on. These things are fundamental strategic shifts in how crime and terrorism are being operated. I think if we don't recognise that, that's the emerging threat, not cyberterrorism. I think there's a lot in there to be unpacked, but I think it's actually about digital world influencing cyberterrorism, rather than cyberterrorism influencing digital world.

If there's one thing, I think maybe we sort of leave with, is if there's anything it's going to do, it's going to ask us to focus and think about the safety component of cybersecurity, rather than the confidentiality, the integrity, the financial impact. It's the human implication of safety, the implication of hacking into an autonomous car via the DAB radio to turn the brakes off. Who thought that was going to be a thing, but it is. Sorry.

Roark Pollock

I think that's right, the fundamentals of security haven't changed, whether you're talking about cybercrime or cyberterrorism. What changes is from a [CSO] perspective, is when you conduct a risk assessment, you're looking at a different view of your infrastructure. Instead of thinking about somebody that's trying to - that is economically motivated and trying to steal something, you're thinking about data protection. With cyberterrorism, you're thinking about how is somebody coming in and trying to cause disruption to your business, or your infrastructure, if you're an industrial network.

Now we're talking about very different types of networks with industrial control systems. So now you're trying to protect a network that's very different than your information technology infrastructure, which is frankly what? 20 years behind the curve, from a security standpoint, if not more, from traditional IT. We've integrated those into our traditional IT networks, so now as you think about your risk assessment, those networks become a big part of what you're trying to protect now, as opposed to just trying to protect the underlying data that somebody may be trying to steal.

Joe Baguley

Well I think we've evolved an IT industry that's in to managing things. If you think about it, it's all they do, right? So, let's go back, what do we manage? We manage data centres. Now people are using personal computers, okay well let's manage the personal computers. Oh, now they've taken the personal computers and they've disconnected them and made them into laptops, let's manage the laptops. Oh, now they're using phones, let's manage the phones, let's manage all the things. It's like it's not about managing the things, it's about managing the applications and the data.

Roark Pollock

Joe as you mentioned earlier, you were talking about a VMware perspective, everything was about the application, but as you start talking about these industrial control systems, and now you've gone all the way back to the beginning again, of what we're trying to do is secure and manage these assets and these end points, that are sensors and other things, in these industrial control systems.

Joe Baguley

I was with someone yesterday, that was asking if I could help them virtualise power PC, because they didn't want to change their system, so I was like oh god, but that's what we deal with on a daily basis.

Andrzej Kawalec

Joe, it's what you were saying, it's absolute blinkered fixation on the infrastructure, the things, being able to manage the things and the devices and the different components and an outside in view. Which is, it's all about the threat, I'm fixated on being attacked and the threat, I'm fixated on a new piece of regulation, I'm fixated on a new piece of technology. Turn the whole thing on its head, you talk about data and applications.

I mean I add one, user and data, when those two things come together, value is created, and it's always done in an application. So, when those three things work, think about the user, think about the data and the application, when those three things work, that's right. That's how you create value, that's not all of the underlying pieces, all the external threat.

Joe Baguley

Well it's that end user computing piece I talked about earlier, the secret to success for us in that was five years ago, where we said it's not about MDM, it's not about Mobile Device Management, it's not about all these bits that the industry is talking about. We sat down and went actually, this is about enabling users to have access to applications and data securely, anywhere, full stop. We focused on that maniacally for five years, was how - until now and we're still going, is how do we give people access to data and applications securely. Because that's what they want. The device actually is irrelevant, the infrastructure to the user is irrelevant. It's incredibly relevant to a lot of people, but it's not to the user.

Roark Pollock

One of the things you said Andrzej, was you talked about the user, as we talked about users, we're normally talking about somebody using this or your laptop, right? That IT user. But now as we talk about industrial terrorism, I mean we're bringing a whole new user group in to play, because now you're talking about a user is the person in some industrial facility, that manages the safety and reliability of those devices in that industrial facility, that's not used to talking about cybersecurity.

So now you're layering another aspect of their job and trying to train them and bring them up to speed, from an IT perspective. Because most security is still falling in to the CSO. It's not the responsibility of these industrial organisations that are managing safety and reliability.

Andrzej Kawalec

I think that's really important, so we work with a lot of organisations, both private and public, that run critical infrastructure. The teams that are out there that have been

operating this stuff for decades, have been the guy that was in that facility that understood how something worked 20 years ago, and has evolved into the network manager or the operator in that environment. The corporate or the global IT function, is trying to today, wrap their arms around and put some controls in place, in this OT environment.

At the same time, there's this innovation going on in the IoT space, there's this evolution of SCADA industrial control systems. Where technologies going into these plants, these factories, these water processing plants, the power distribution. Technologies going in there that is open, there's no security standard in there, and how on earth these people can run and manage and secure these systems. For me this is the next big danger, in relation to cyberterrorism, because it's going to be the soft underbelly, where they'll be able to have a material impact to a country, to us as citizens. That's…

Ray Ottey

Different environments.

Andrzej Kawalec

…you know, in the next five to 10 years, we will see those types of attacks.

Ray Ottey

Those users in that environment, that OT world that you were talking about, their security was all physical. They didn't think about the security of the system they operate. So that MRI scanning machine, or that nuclear control system, whatever it was, the security around that was all entirely physical, it was air gaps, it was can't get into it, can't touch it, security badges, et cetera et cetera. Yet you're right, the IT guys coming to them now, who's like some promoted [CSO] or whatever, he's their network manager, is now coming to try and manage the security of those.

I see these lovely scenarios, where it's like what, so you want to try and connect your IT systems up, to my control system. Can I just remind you, you're the guys that gave me that XP laptop that was riddled with viruses and never really worked, and you're now telling me you want to try and connect to my OT system? Get stuffed usually is the answer there, and that's where we're seeing the friction.

Joe Baguley

Yeah, and almost everybody's answer today seems to be network segmentation, it's like…

Ray Ottey

Yeah, yeah, that's the answer to everything.

Joe Baguley

I mean it's so 101, right? It doesn't talk to the asset, it doesn't talk to the…

Ray Ottey

Doesn't talk to the app.

Joe Baguley

Doesn't talk to the data, it's just basically blind segmentation, it's basically a traffic light.

Roark Pollock

I think if there's one positive note on this conversation, it's the thinking that it's taken us 20 odd plus years to get to where we are, from a mature security perspective today. If you think about how do I start to apply security in these OT environments, okay at least we have mature frameworks we can start to apply to those industrial control system networks. Whether it's that NIST framework, or any of the other frameworks that are out there, and start to actually implement, in a hopefully a much quicker fashion than it's taken from a networking and an endpoint perspective, to apply security over the last 20 years. We're not developing the frameworks, all we've got to do is implement them and new network infrastructures, and train the people and bring them up to speed quickly.

Andrzej Kawalec

I think there's a really interesting point there, and I suspect it's both worse and better. We spent 20 years developing a really complex industry which had all the logos, that Joe you put on the slide. We've spent 20 years developing not one but hundreds of different global standards. We've spent 20 years not having any global corporation around cybercrime. We spent a long time learning how to put firewalls on different bits of our networks, but not really affect a huge amount of security rate. I think we talk about users and different types of users. Users equals identity in lots of, you know how we think about things.

When we start to throw all of these newly enabled connected devices, we create a whole new class of identities, at a scale we've not really come to grips with before. So, I think all of the last 20 years have forced us to a place, where we're not able to cope with an explosion of IT, OT, identity explosion in new device classes, or the physical environment. Which is going to force us to approach it differently. It's going to force us to think about application centric, data centric, user identity centric security.

It's going to force us to take an inside out approach, rather than a let's think and fixate on threats, let's think about what we do. If it is the golf course analogy, known good, then it's actually about who you allow to play on your golf course, and being a member of the club. Or this is a golf course that any member of the public can come and play, and you pay and it's not quite as well looked after. I think there is a fundamental change that has to happen, and I suspect we'll get there.

Ray Ottey

Completely agree, and I think what will trigger that change, and I think that change is already happening and we're doing some stuff that absolutely changes the way that you

approach this. Violently agree with the detection piece, rather than prevention. We talk all the time to clients. I've sat in front of CSO of a bank quite recently, put a similar slide up, and he said yeah, I think I've got most of those, literally most of those. Obviously, many I haven't got. I mean it's madness, it's absolute madness. But I think what will trigger the thinking, outside of that, particularly outside of that sort of corporate world.

The attack you mentioned Joel in New York, the healthcare attack, that was the first cyberattack where a death can be attributed to a cyberattack, because the infrastructure that was taken down. I think that speaks to a trigger, and when an attack has multiple fatalities against it, which I think is inevitable. I think then the wider world listens. I think actually we've got to change this.

Joe Baguley

I think we're missing, so come back to the prevention piece. One of the things I've been talking about a lot, and we've been working with governments on, UK government, European government et cetera, is these sort of five principles of cyber hygiene. When we get into this world of IoT, we get into this world of IT-OT, we get in to this world of building environments that ultimately will be [unclear]. We're introducing some techniques to people, that to some people in the security industry are blindingly obvious, but to them aren't.

They're things like least privilege, micro segmentation, yeah, you know, encryption. Encryption 10 years ago, 15 years ago was a horrible thing, because it was hard. Now it's really easy and it's not a burden on processors, so let's just do it everywhere. Multifactor authentication. Tesla owners right now are crying out for multifactor authentication on their cars, because even Tesla aren't applying it now, and patching. Like I talked about, people are deploying stuff and not thinking about the ongoing lifecycle management of that box.

Roark Pollock

It's difficult to patch systems that may be 25, 30 years old, and dangerous sometimes.

Audience Q&A

Joel Stradling

We have a question from the floor. Sorry to interrupt, we'd just like to have a question from the floor.

Joe Baguley

We have a question, alright.

Davey Winder

Right, so it's Davey Winder, I'm freelance for Forbes, Sunday Times, SC Magazine et cetera. You're doing a great job of debating general information, security best practice. But the question is how cyberterrorism defines information security, and so far, I've not really heard anything that defines cyberterrorism. So, what are you guys talking about when you think in terms of cyberterrorism? Are you thinking state on state acts? Are you thinking state on business acts? Are you thinking hacktivist on state, hacktivist on business? Criminal acts against the state? How do you define cyberterrorism?

Joe Baguley

I think that was what Ray was talking about earlier, I think what we're looking at here is I don't think, from our perspective cyberterrorism isn't from the type of attack and what's going to be attacking a system, any different to any other type. Whether it's a state act or whatever it's whatever. It might be more persisted, it might be more at scale, but it's not necessarily different, in terms of the defence stance we have to take. So, it's almost back to my point, if we start focusing on different threats, rather than building well hardened systems, it's that whole different way around it. So, I think that's kind of what you were saying at the beginning really?

Ray Ottey

Yeah, it's a subset of the wider threat. If you look at [unclear], and it's a really interesting news case right, and widely known. 200,000 systems infiltrated, 150 countries, hundreds of millions of pounds of ransomware. Attributed to North Korea, you know publicly we can talk about that. No one knows the motive. Was it a by-product of another attack? Were those systems in the NHS and Nissan and Deutsche, were they infected because they just, they were in the wrong place at the wrong time with the wrong level of action? Bad action cadence was you know, the result of that. What was behind that?

The attack itself was a piece of zero-day, very sophisticated malware that's subsequently morphed into something else. So, a Taiwanese semiconductor was also impacted later on. But was that cyberterrorism? Or was it just something that went wrong? Nobody actually knows, that's the answer there. I think for me, it's those two categories. It's cyberwarfare, or it's cyberterrorism, and the only different in that cyberterrorism piece, is the motive. They're using the same tools, this could be the same people as doing other things. So, you know.

Roark Pollock

I'll make it a little more complicated. I mean we've got cybercrime which we traditionally focus on, and we're talking about cyberterrorism, which you could add to that cyberespionage, cyberwar, just all out cyberwar. I think Joe's right on, from a cybersecurity perspective, as cyber professionals, it doesn't necessarily change the things we need to be doing and the things we need to be focused on. As far as protecting our infrastructure and the prevention side of things primarily.

I think what it changes is, as we look at our infrastructure and focus on risk, and a risk assessment, and think about the different objectives of those different groups. I mean if it's cyberterrorism, you're trying to disrupt the infrastructure, or disrupt the underlying business. If it's cybercrime, they're trying to steal something of value. If it's cyber hacktivism, perhaps they're trying to steal something that they can then disclose, to creating an embarrassing environment for some political point they're trying to make. It really just changes the risk assessment that we need to conduct, as to what we're trying to protect.

Joe Baguley

To your point I think there's an angle we haven't discussed yet here, which we need to talk about as an industry. Which is the inherent potential, I don't know, how do you call it? The hardware itself might be flawed, if you get my drift? Whether it's Spectre, whether it's the supplier who's building it has built some sidecars in, and you have to ask yourself, how long did certain state nations know about these flaws?

I didn't want to mention that, but I'm talking about, if you go back to Spectre for example and those associated processor issues that we had at that time. How long had certain nation states known that those vulnerabilities were there, and kept it to themselves, before the wider world found out? You know, it's those kind of things were actually more worrying. So, we're talking more now with people about how you mitigate against that, in and of itself, so that if there is, when that did happen for us, it wasn't a big impact for VMware.

But you know, how do you protect against the fact that that might be there too? That's very real from a cyberterrorism, cyber state on state act thing, is a real concern. It's down to that silicon level. So, we're looking again at how do you build a layer on top of that, that almost abstracts you from that threat?

Roark Pollock

There's a saying that I love, and it's kind of a scary thought, but it's this notion of absence of evidence of some intrusion, is not evidence of absence. What that means is, just because you don't see any evidence of an intrusion in your environment, doesn't mean that there isn't one. It doesn't mean somebody doesn't have access, that they haven't taken any act upon. They may have access and they're just sitting there waiting for the right opportunity. I mean this notion of you always have to be hunting, as opposed to always, I mean we have to do the right things from a prevention standpoint. But you always have to be hunting and looking to see what's happening.

Joe Baguley

I think theft is the wrong word, we keep using cyber theft. When someone steals something from me, I don't have it anymore. When someone steals my data, I still have my data, I might not even know that they've stolen it, maybe there's some other word we need to use.

.

Andrzej Kawalec

In this conversation, it's symptomatic, and the question and our conversation symptomatic of the situation we find ourselves in. What is cyberterrorism? Cyberterrorism is terrorist organisations, when are affiliated or not, to a nation state, performing acts of terror for a political or ideological gain. In the same way that crime, we understand the definition of crime. When it's cybercrime, we seem to think they're different. When it's warfare, when it's espionage, when it's just general IT change.

The symptoms of this conversation exhibits, is it all goes into the same pot, and it's blended through an IT stack, so that we don't quite understand the motivation or the attack or the vector or the vulnerability, or the system or the component. I think that's where we get confused and that's why we struggle. To think we clearly understand a terrorist group needs funding, they're going to use the internet to drive funding. They're going to use the internet to drive propaganda. They may use it for disruptive or destructive purposes. That's super clear.

But when they use an existing vulnerability and a certain vendors hardware, hijacked through a different service, and to an industrial ecosystem with other cybercriminal gangs, share a piece of malware to perform a goal. Then it becomes really blurred, and I think that's what we struggle with. Then I think it's that blurring of all those motivations, means the focus on the threat, or the continuous hunting and analysis of those threats needs to be done. You need to go back to, what can I control best, and how do I start to create that good playing field.

Joe Baguley

Everyone loves a clearly defined [bad guy].

Joel Stradling

We have five more minutes left, so if there's any more questions, but please go ahead?

Sibahle Malinga

Thank you so much for an insightful discussion. My name is Sibahle - I'm from ITweb South Africa. I'd like to find out what are the two main challenges that both organisations and governments are grappling with, when it comes to rapid detection of these advanced persistent threats? Because surely these cybercriminals are doing something well? Because by the time most governments realise, they would have already damaged these systems. So, what are the main challenges in detecting these advance threats, before they actually do harm? Thank you.

Roark Pollock

I think there's a couple of things we can talk about. I mean we've talked about a few of them, and if we're talking about cyberterrorism and industrial control systems, and those types of networks. I think the biggest thing is, is we're talking about a whole new

network that we're trying to protect, that hasn't been dealt with before. It was always protected by an air gap, and it wasn't connected.

Joe was right when he said security was physical security, of who had access to these environments and who had the contact and get into these networks. Now for monetary reasons, to make things easy, we're connecting them to our IT networks, and so now all of a sudden, I want to be able to remotely monitor those networks, or make changes to those networks remotely. Some of them may be dark environments, where there's nobody physically has access to it, like an offshore facility.

So now all of a sudden, we're connecting them to our IT infrastructure, which makes them accessible to anyone, if you can get access to that environment. So now we're dealing with an all new environment, all new types of devices, people that manage those devices. I think that is our biggest challenge, as we start thinking about these operational technologies.

Joe Baguley

I'd go back to the point that I made in my presentation, the challenges they focus on threats, it's always what's the next threat, let's predict where the next threat is coming from, how are we going to deal with the next threat? What they're not looking at, is how do we harden and protect more effectively, more fundamentally against those threats, as we do what we do next. It's this kind of focus on where's the next threat going to come from? Which hole do we need to patch next? Oh, are they going to attack us in this way, let's look at how that would work. As opposed to have we actually started from the base up and looked at how this thing is built and secured.

Andrzej Kawalec

Yeah, I'd say the two things. I would say first understand what assets can be impacted. So, whether you're an organisation, or private organisation, or if you're running critical infrastructure for example. You really need to get to grips with what assets can be compromised, and what the impact of that compromise could be, in multiple ways. So that for me is always the first parts. Whether that's data or systems, so once you've classified that, obviously you can then put your controls in place. Those controls aren't just finding things, I completely agree with that.

But once your controls are in place, the second thing I would say is to really test the processes, and stress those systems or assets, and mirror an actual attack, and do a real sort of simulation, and we don't see enough of that. This isn't whether the system finds the thing, it's what happens when the system finds a thing. Who does what, where and when? That could be decision making by people, that can be automated systems. But that whole robust response if you like, which can be a fairly robust and wide program, including PR, if you've been here. You need to really test that process, and understand what that looks like. So, if it does happen in the future, which is kind of expected, you understand what that's going to look like and how that's going to unfold and play out.

Roark Pollock

We've circled back to the people Joe.

Andrzej Kawalec

I mean sorry, I think that bits fundamental. If you can't see what's happening, you can't detect it. So, if you don't have basic core level visibility of what is under your control, and the understanding of where your crown jewels are, to place enhanced visibility, you can't detect it. If you can't see it, you can't begin to understand what on earth's happening. So, the two things, visibility and seeing what's there, and then understanding and interpreting those actions, people need a lot of help doing that.

At the moment, as you say, 63% of CSOs in the report we did in January, said they're fundamental in a reactive state of their security programs. They're not allowed, by various rules, regulations, to step outside of their own organisation. It's like putting somebody in a boxing ring, and saying right, you're ready to go, there's your opponent. Right, just wear this blindfold, so you can't see what's going to happen. You need to listen out for the tell-tale signs of somebody trying to hit you. You can just imagine how hard that is.

Then you say okay, and you say no I'll put my hands in front of my, so no, no, we're going to tie your hands behind your back, so you're now in the boxing ring, with your blindfold on, hands behind your back. Then you say okay, but due to a certain amount of government regulations, you can't move either. Because you have to keep this data here and treat it in this way, and we've given you a whole roadmap. I think a lot of organisations find themselves in that position. They don't have visibility, they can't react, they can't move, and they're just waiting to be hit.

At that point, it's you know, how many times do you fall down before you get back up again and you lose your job as a CSO, and you change that. It becomes about visibility, understanding what's going to happen, and being able to move and change, and understand the realms of that boxing ring.

Ray Ottey

But your point of watching everything as well, I mean this is it. A lot of people don't know they're being hit, because how they're being hit, doesn't fit in to what they're looking for as attacks. A process running a bit longer every day, because it's doing something else. A machine occasionally pinging some other machine, which isn't necessarily out of the ordinary, but it might be because it's not what it normally is, you know I'm banging on about my knowing good thing. But it really is, and most organisations don't know what normal is for them.

So, what you see when they have an attack, is this mad running around of people going, oh my god, that's at seven, and people are going well that's always at seven actually, because that's normal for that system. What we're worried about, is that this counter's at 24, and that never, you know, it's that kind of thing. People don't know their systems well enough. So, you go and talk, okay what do nation states have to worry about? What's their biggest problem? Their biggest problem is they really probably don't know

what they've got and how it should be running today, so that when it's doing stuff it's not normally doing, they don't even notice that. It's getting more complex.

Roark Pollock

These companies need to create some sort of cyber range, where they can play red team, blue team, and train their people, of how to respond when something does occur. Because it's too late when it happens.

Joel Stradling

Thank you very much Andrzej, Ray, Joe and Roark, that was a fantastic debate, and thank you for listening. We'll now move on to the next session.

Let's move directly on, what a fascinating topic that is. Security has been one of NetEvents standards topics for obvious reasons over the, well since 1996, you do the maths. Which is the first NetEvents that happened, which I remember very well indeed, as a handful of people in this room will too. We'll return to that topic sometime later on tomorrow I expect. Okay, would the next panel like to come down please, come on down, with NetEvents veteran, if I may call him that, Ian Keene.

[end]