NETEVENTS GLOBAL IT SUMMIT

SAN JOSE, USA

OCTOBER 3 & 4, 2019

FINAL

Conference Debate Session I—The Cybersecurity Threat Landscape

Introduced & Chaired by Vikram Phatak, Founder, NSS Labs

Panellists:

Michael Levin	CEO & Founder, Center for Information Security Awareness
Paul Kraus	VP of Engineering for Cybersecurity, NETSCOUT Systems
Ted Ross	CEO & Co-Founder, SpyCloud
Thomas Edwards	Special Agent in Charge at U.S. Secret Service San Francisco Field Office; Department of Homeland Security

I thought I'd have a bit of fun to start with, which is when you think about where we are right now with cyber security, it very much feels like we are creating a lot of problems for ourselves, and very much in the way Wily Coyote turns up on the wrong side of his traps trying to catch the Roadrunner.

That's - where are we at, sort of from a threat perspective in defending ourselves? Well, right now cybersecurity industry is Wily Coyote, and you can quote me on that. So, what's going on? There are two ways of looking at this. This is data from the World Economic Forum on the amount of losses, which you probably have seen before. Last year was a half a trillion, 500 billion, and they're saying it's going to get to three trillion by 2020, which to me seems big. But they're sticking by it.

These are big numbers on cybersecurity spending, but there's two ways of looking at it. One is, compare how much you're spending versus how much you're losing. The ratio seems like we're spending a whole lot of money. If on the other hand, you think of it from an R&D perspective, they take, say, 10 per cent of your revenue and you're going to plough that back into R&D. The bad guys are able to fund their research at a rate about five times of what the good guys are, which does not bode well for the future.

From a where are we at current status, we have a massive skill shortage, which I'm sure you guys have been writing about and read about. The - as Ravi was mentioning, we have a lot of labour-intensive solutions that require experts. When you think about that in the context of the skill shortage, and keep in mind that of the folks that know cybersecurity, the number of folks that really know it well is only a small fraction of the folks that have [unclear] into the field.

Then you keep on opening up new attack vectors, whether it's IT, we're starting to go heavily into dev ops, which sounds great at first, dev sec ops, et cetera, but then you think about people that are somewhere in the world that are doing coding by what Google tells them to do with a search, and they're grabbing an open source repository that may or may not have been backdoored by the North Koreans, Chinese, Russians, Iranians - pick your adversary. We're literally embedding the next attack vector in the code that we're developing today.

So, last but not least, the self-awareness of what's going on, situational awareness of what's our current posture - if you ask most CSOs where do you stand, they probably can't tell you. They may give you some hand-waving and some numbers, but the fact is that they're - they get surprised on the downside by breaches all the time.

So, top targets - by the way, I'll move through this part very, very quickly, so that we can get to the panel, but afterwards, if you want some of this presentation, please feel free to ask, we can get it to you. Then you can see the who, what, where, why and how. It's - basically it's about money, as well as coming down to, yes, there's national interests involved in some things like elections, but by and large, you're talking about money.

Now, we haven't mentioned, so we're booby trapping the future, we have the cloud, which is great, but we've got this dev ops moving very quickly, embedding flaws into the system very quickly. We have IoT, which - there's a lot of devices out there that are hard-coded, and when the next version of some vulnerability comes out, like Heartbleed, that kind of a thing, for SSL, there's going to be a lot of obsolete devices.

By the way, it would be interesting to hear what you guys have to say on this, particularly you, Tom, I think, which is the supply chain - I've been told that you can still buy devices at Best Buy for routers and switches that were built a couple of years ago, and they still have the Heartbleed code in them, and there's no way to upgrade them. So, people are still buying things, because vendors are not going to throw away equipment just because it's got a vulnerability. At least, not today.

Now we're adding 5G, which now connects these things together in a way they've never been connected before, smart cities and so on. So, what's going to happen when all of a sudden, attacks jump from the virtual into the physical world, and things start going boom? The due care that we have for cybersecurity is - if you caught 99 per cent, that's not even remotely adequate, compared to what we would expect from our airplanes, as we mentioned earlier. From a boiler in our basement. It's a completely different due care expectation. What does that do to the insurance industry, and so on.

Last but not least, before I get to these couple of last data points. How many of you have heard of the Dunning-Kruger Effect? Okay, I strongly advise you to look it up,

you can do a search on it later on. But what it basically means is that folks who are incompetent are so incompetent that they don't know that they're incompetent. They don't have the tools to judge their own capabilities. So, the data here, basically, the bottom 25th percentile, the actual performance is terrible, but they thought they did really well.

So, you have a problem where there are people who don't know what they're doing are overestimating their capability. Conversely, people who are highly competent, people on this panel, things that are easy for them, they assume are easy for others. This happens in Silicon Valley all the time, with all the security products. Software products in general, right? So, we overestimate the ability of others, and underestimate our own ability, if you're on the higher end of the scale.

So, you have dumb people who think they're smart, and smart people who think other people - the dumb people are as smart as they are. It creates a very bad situation. That's largely what we're dealing with.

So, some test results - short version is that just about everyone had evasions, and I will - again, this will be available. The evasion is how you basically - you make a minor change to an attack, and you can bypass the security product, that's an evasion. Basically, you put the hood on, and suddenly the camera doesn't see that you're the bad guy. Putting on a mask, and they can't tell who you are, that kind of thing.

This is a money slide, here. Just about everybody had pretty major problems. All the red is bypassing things. I actually had to do a briefing with some folks in DC about this, so that they could tell the vendors to go fix their stuff. If you see some voodoo dolls of me, that's probably why. If you have questions about this afterwards, I'm happy to talk about it.

Lastly, we did some testing on anti-tampering, which is interesting - how many of you guys have got AV products? Well, 11 of the 21 that we tested, the bad guys could reach it and turn off the AV, so that they could then get into your system. So, with all the protection they (enterprises) have, the bad guys can just reach in and remotely turn it off. Almost everybody was responsible and stopped it, but not everybody. Some folks are still out there who do not address the problem.

All right, so summary. We're falling behind, and the bad guys have got the upper hand. We keep on making things worse. The tools that we rely upon are incredibly complex and are not getting any easier. Hopefully, with some of the AI stuff it will be, but as you heard, that's not a guarantee. Bottom line here is, from my perspective, I'm really excited about this panel, because it started with situational awareness, with where do you stand? If we can just get back to some basics, people could start making informed decisions.

So, with that being said, hopefully these gentlemen here can introduce themselves. Is that going to be the next slide here? Yes, here we go. We'll start with Paul.

Paul Kraus, NetScout Systems

Hi, my name is Paul Kraus, I'm Vice President of Engineering for Cybersecurity at NetScout Systems.

Ted Ross, SpyCloud

I'm Ted Ross, CEO and co-founder of SpyCloud, if you never heard of SpyCloud before, we have a team of researchers that interact with criminals, and we social engineer data from them as they steal it, so that we can turn that around to our customers, so they can prevent account takeovers. Before SpyCloud, I was CEO of a company called Exodus Intelligence, where we built, we found zero-day exploits, sold them to mostly government agencies. Before that, HP, and started the intel team at HP a couple of years ago.

Tom Edwards, US Secret Service; Department of Homeland Security

Good morning. My name is Tom Edwards, I'm with the US Secret Service. The Secret Service is part of the Department of Homeland Security. I'm in charge of the San Francisco field office. For those that don't know about the Secret Service, the Secret Service has a dual mission. Not only do we protect our president and vice president, family and foreign heads of state, most people don't know that we also investigate cyber-enabled financial crime. We started investigating financial crime in 1865 with counterfeit currency, and we have evolved with the criminals all the way till today, where they're doing complex cybercrime towards our financial institutions.

Michael Levin, Centre for Information Security Awareness

Good morning. I'm Michael Levin, and I'm proud to say I'm a retired Secret Service agent. I spent 30 years in government, and my expertise was cybersecurity. I worked for Microsoft for nine years in their physical security department. I'm now the CEO at the Centre for Information Security Awareness. We help organisations induce security into their organisation to create a culture of security.

Vik Phatak, NSS Labs

Thank you. I actually want to start with Tom. From the Secret Service's perspective, what is it that you're seeing from a - what are the top things you're having to face and deal with?

Tom Edwards, US Secret Service; Department of Homeland Security

Vik, like you mentioned, profit is becoming more and more the motive for cybercrime. The cyber actors that we deal with are organised groups all over the world, and it's profit driven, as far as getting it to the networks, whether it's public sector or private sector, through ransomware, through business email compromise. They're going after the money, they're going after credit card data, they're going after personal identifiable information, and then turning that into profit. That is the main driver.

Then the next thing would be the credential theft, so they can get into cloud-based servers and steal that data so they can monetise it on the dark web or in other places. That's what we're really seeing. Credential theft, and then really the profit motive for cybercrime.

Vik Phatak, NSS Labs

When you talk about credential theft and people selling information - maybe this is a question for Ted. How does that work? What's the value? Is there something we can do to break that chain?

Ted Ross, SpyCloud

We're all about disrupting the criminal's ability to profit. It's really an unfortunate scenario. We started this company three years ago; we have over 13,000 breaches in our database right now. Almost 80 billion assets. Basically, if you have an online identity, we probably have it in our database, which means the criminals have it. They're highly organised, they take this data, they build their own databases.

Oftentimes, when people think of credential stuffing or account takeover, or somebody logging into your Gmail account, or business email compromise, they - I think they underestimate the criminal's ability to be creative. They also think about it at the end of the timeline, when the information leaks on the deep and dark web, when some companies like Akamai can detect it, and protect their customers.

But there's a year and a half to two years that goes by before it gets to that point, where fairly sophisticated criminals have access to the data, and they do really nefarious creative things. First thing they'll do, is they'll start separating the data into people that they can go after that they know are high-value targets, they put them in a special category, and they have very sophisticated techniques to go after them. They're targeted attacks. Then they leave all the rest for later, or they run automated tools against them.

One of our customers recently presented - our customer advisory board, the financial organisation that deals with a lot of crypto currencies. They actually had a really interesting statistic. Ten per cent of all the attacks that are coming into their network are targeted, and they lead to 80 per cent of their loss.

So, I'm going to talk a lot more about this tomorrow. Do an actual keynote, so maybe I should save the rest for then.

Vik Phatak, NSS Labs

That's okay.

Ted Ross, SpyCloud

I feel like I'm talking too much.

Vik Phatak, NSS Labs

Michael, you've got a company that helps people understand how to educate their employee base and so on. What role - again, I'm talking about getting back to basics. How do you - what's the impact of that? How well does it work out? Is this working? Okay, here we go. Do you want to talk about the role that education can play, in terms of combatting these kinds of attacks?

Michael Levin, Centre for Information Security Awareness

Absolutely. Well, you think of - how do we create a culture of security within an organisation. I guess my headline for you would be, we're doing a terrible job, still. We're finding that many organisations, and I talk with executives from companies all over the world, are doing one of two things. They're doing nothing, or they're just checking the box.

We know that phishing testing will help an organisation, and reduce risk, but the problem is that - and I use this analogy, if you're a car burglar, and you want to break into cars, what is the first thing that a smart car burglar should do? Check the door handle to see if it's unlocked. You don't have to break a window first. Many of our hackers are doing very good reconnaissance, and they're finding all the open windows on our networks, like admin passwords that haven't been changed on servers. We're still seeing those same problems.

So, the CIOs don't have visibility into some employee deploying a server out on their network, and there's no checks and balances in place for human error and laziness. So, we have improper procedures, policies, checks and balances, and then we're not training our people. The average citizen in all countries receives no cybersecurity awareness training in their lives, until they're victimised, or until they cause a problem.

So, how do we create a culture within an organisation where people are actually thinking about that every morning when they turn on their computer, and that's what we try to do.

Vik Phatak, NSS Labs

There's an active adversary, though, that's trying to use disinformation and different social engineering techniques to get people to do things. How - do you have any statistics on how effective, in practice, using - taking the training approach - how effective really is it?

Michael Levin, Centre for Information Security Awareness

Depending on the type of crime, it can be very effective. In the US, especially, we're seeing business email compromise, which is basically a scam where a business wire transfers money to a bad guy. Simple policies and procedures, like - almost like a two-factor authentication in the process, usually solves that problem.

So, education and training work very well on certain types of crimes. In many cases, it's exactly what organisations need. In conjunction with good policies, they require

employees to do certain things and be accountable for those things, is really important as well.

Vik Phatak, NSS Labs

So, accountability requires some sort of monitoring. Paul, in terms of monitoring, how should somebody go about taking - approaching this? I mean, if there's a - every network is bespoke, everything is different. Where do you start?

Paul Kraus, NetScout Systems

I think the first thing, and I think Michael hit it very early on in his discussion. It's about visibility. How do you know what to monitor, or how do you put value on the assets in your organisation, if you don't even know they're there? The first aspect is gathering up the inventory of actually what you have. Second of all, can you actually take statistics? Can you look at the changes? Can you monitor to the level that your organisation can accept the risk for that asset being compromised?

I think at the very core of it, and we touched a little bit about the hygiene. It's - understand how valuable that asset is to you. Then can you have - do you have visibility across, not only that asset itself, but across the infrastructure with which it touches. So, there's been a lot of discussion already this morning about moving to multiple clouds and AI and all those other good things.

That just - that sort of complicates the whole scenario. Moving to multiple clouds, putting dev ops, and you talk about sec ops, just in your introduction as well. Are they actually going to either of these infrastructures together, or are they not? I presented a couple of months ago, and I asked a group of security engineers, you know, when the dev ops team in your organisation moves something to the cloud, are you involved?

Out of 300 people, a half dozen of them raised their hand. Does the security team even understand what's out there? Does the IT team even understand what's out there? Let's go back to visibility, where really, I started, that's the key bit for understanding, again, your risk posture. Without that visibility, you really have no way. I think at that point, you're really just putting yourself in a hole.

Vik Phatak, NSS Labs

I'm a big believer in that. Earlier, I pointed out that the bad guys can get through the security defences, right? I mean, they can. But on the flip side, having people running around trying to trace everything, it just doesn’t scale. Okay, so we get some visibility, and [unclear] Ted.

Ted Ross, SpyCloud

Yes, it's interesting that we started this conversation talking about device security and patches and things like that, and things that you would think would be taken care of. When you install a network, you install security with it. It's part of the install. Hopefully, that's happening in most places.

When you start out, though, to actually implement a security practice, I think most people forget about the human element. The attacks - if you look at the attack surface, the weakest link is the human. I think we are all wired to start with the devices, but I think we should also be starting with human training and educating them on concepts like zero trust, and not to click on an email, not to click on an attachment, and if they do get an email from the CEO asking them to go buy a bunch of gifts at Apple, call your CEO. Just pick up the phone and call him, and see if he actually sent it. Really basic things.

I think those things are lost, and I think that's probably a bigger problem today than even forgetting to patch a vulnerability.

(Unknown)

I totally agree. Even if you look at Ravi's slide from the very beginning, 94 per cent of corporations are multi-cloud. Of those 94 per cent of organisations, are the humans trained to understand what multi-cloud actually means? That's just a staggering statistic.

Vik Phatak, NSS Labs

It feels like cybersecurity has become like gym membership. People buy it, it makes them feel good, but they're not really deploying and using it properly. They're not actually going in and doing what they need to do. In that kind of environment, Tom, where would you recommend people spend their effort? You see a lot of this.

Tom Edwards, US Secret Service; Department of Homeland Security

You're right, it is like a gym membership. You think you have it, you don't use it. One of the things that we try to do at the department and at Secret Service, is build relationships with other agencies, the private sector, the public sector as well as government. We have a strong relationship with the National Crime Agency in the UK as well as Europol. We are not going to solve this problem as a government entity.

It takes a lot of players, a lot of partners, both in the public and private sector. If we're not sharing information about the latest cyber threats, and there isn't that synergy between government and industry, then we're losing the battle against cybercrime. We're learning that the hard way, with mounting losses. But our relationships are getting stronger overseas, and internally, domestically, as far as being able to push the information out to our partners.

For example, the Secret Service has electronic crime task forces around the country. We also have a task force in Rome, in the UK, and in Hong Kong. We're able to push out the latest malware or ransomware so that our private sector and public sector companies can inform their IT teams how to address those threats.

Without that information sharing between private and public, we're going to lose the battle every time.

Vik Phatak, NSS Labs

Do you see a lot of vertical - if one oil and gas company gets hit, do you see that that same tactic is being used for others?

Tom Edwards, US Secret Service; Department of Homeland Security

Yes, exactly. Mike mentioned lowest hanging fruit. They will just move from one industry to the next, finding those vulnerabilities until they patch. Then they'll move on to the next one. That's just the way they operate. They'll go from large businesses to medium businesses and then to small businesses. Obviously, the prize will always be the whales, but they'll go for your trout, they'll go for your minnows. It just depends how sophisticated that criminal organisation is. But cybersecurity is working. There are some safeguards that are being implemented that are protecting us. But it's not a panacea.

Vik Phatak, NSS Labs

I think you're a little more optimistic than I am.

Tom Edwards, US Secret Service; Department of Homeland Security

Two years ago, I was at a presentation with the FBI where they presented to a BEC audience, and they said at that time, over the last five years, there was over $12 billion in loss, just in BEC crime that they were tracking. About 65 per cent of all the cases that were sent in to the FBI were BEC-related, which - I mean, it's overwhelming, right? Only three per cent of that 12 billion was recovered. So, it just seems like this is - this problem is not going to go away any time soon.

The interesting thing I picked up from that conference was, when we all get these emails from the Nigerian prince, we roll our eyes and think, this is nothing. But we don't think that Nigeria now, as a country, has had several decades worth of training on how to social engineer us. They've gone through several generations and trained those generations on these techniques. They also are becoming a lot more capable from a cyber perspective - from a technical perspective.

So, even the Nigerian prince now is somebody who's formidable. We just don't think of it in that context here.

Michael Levin, Centre for Information Security Awareness

When you think of cybercrime, you have to be thinking hand-in-hand with social engineering. This is one of the things that we try to educate companies on, and employees on, is that it's not just the phishing email, it's the different ways that employees can be socially engineered. It could be over the phone, it could be in person, it could be through social media. There are so many ways that organisations can be affected through social engineering that you have to come up with mechanisms and reminders for the employees in the organisation on a daily basis to be on the lookout for all these different things.

The business email compromise scam, I can't begin to tell you how many financial institutions have contacted me because they're having this problem. It's so pervasive in

our society, that we really have to do a better job of coming up with simple mechanisms to solve these crimes.

(Unknown)

I think we were talking earlier about - before we got here, we had the coffee, and I mentioned that a friend of a friend ran into a problem where he was going to China and he put on Twitter, wheels up, heading to Beijing for the next few days, kind of thing. He was CEO of a company. A few days later, his CFO got an email saying - purportedly from him, saying, I've been arrested by the Chinese government, I need money. Send it here. They sent the money. It was - because there was enough detail that they'd gotten on social media to be credible.

Most of that information, people are - it's out there. So, how do we - it seems like we're getting back to people and monitoring and knowing what's going on. Where would you guys start? Maybe we just - from my perspective, complexity is the big problem here, right? How do we make it simple so that it can scale? Where do we start?

Michael Levin, Centre for Information Security Awareness

Well, we have a list of things that we try to tell people to look for. One of the first things that we have to educate employees to look for is the sense of urgency. Nine times out of 10, when there's this sense of urgency, it forces people to make decisions very quickly and it often results in a fraud. So, we tell them, if you have that sense of urgency, like the executive that is emailing, there needs to be a phone call, as Ted said, where someone's calling and verifying information.

We get so quick to click on links and attachments in emails. There are many employees in organisations that get up in the morning, and that's what they do. The first thing they do is click on every email and attachment they get. So, it's how do you get them to slow down and start thinking about the risk associated, and giving them mechanisms so that they can actually make smart decisions.

Go independently to the website. Go independently and contact someone, before they open that unexpected PDF or something. It's creating that policies and procedures as well.

Tom Edwards, US Secret Service; Department of Homeland Security

To follow on Mike's point, once you create those processes and procedures, employees have to be empowered to come forward without consequence, without penalty. If I'm afraid to [tell] my boss that I clicked on a phishing email, then I'm - not only denying power to do that, and the company's in trouble, we could go bankrupt by the end of the month. So, you have to have these open lines of communication. People make mistakes all the time. It's not the end of the world. But if employees don't feel like they have an open culture at work to flag cyber threats, then you're already losing the battle, because they're going to hide them from you 100 per cent of the time.

So, open culture about cyber threats. I talk about these guys earlier. I see cyber threats as a mosquito in the room. We all see the mosquito come into the room, we notice it,

we hope it's going to go away, but it doesn't. We can swat it away at it, we can move away from it, but eventually, he's going to land on us to try to bite us. If you're not trying to get rid of that mosquito early on, it's going to bite you, and you're going to have yellow fever or some other - dengue. But you have to really empower your folks to be transparent with their cyber hygiene.

Michael Levin, Centre for Information Security Awareness

I would start with the individual, and go over that zero-trust model, and enforce some policies. You give an employee a laptop and you train them on, when they go to the office and they open up that laptop and they sign onto the network, that they don't trust that network. Even if it's the work network. They don't trust it. They launch a VPN; they don't trust anything outside of their little device. Treat everybody like they're an adversary, and usually you're going to stop 90 per cent of the threats that come your way.

I'll also share something that I heard, it was at a NATO event, and we had an admiral talk about cybersecurity, and their approach to cybersecurity. He made the point that on a battle ship, every day they run a fire drill. Because if there's a fire on a battle ship, it could kill everyone. It's really important to know how to deal with a fire on a battleship.

When it comes to cyber, those same people that are in the fire drill every single day, they would have to take a one-hour class every year, and click through some kind of painful video to be trained on cyber. Where the threat is a lot more severe than that, right? So, yes, training people, test them, I agree that there should be some way for them to come out and let the organisation know they might have done something wrong without being penalised. But there probably should be a penalty if you don't do that.

Tom Edwards, US Secret Service; Department of Homeland Security

I look at it sort of as a triangle. You have your vendors, you have your users, and your people, and then you have your hackers. Understanding, as I look at the topic, understanding the landscape. The vendors are companies like NetScout. I don't believe that the cyber landscape is doom and gloom. But I don't see everyone who comes through NSS either. I have successfully passed NSS in the past, as well.

But if you look at the vendors, whether it's a cyber vendor providing you security - these people are working hard every day to fight - as you saw in the very beginning, whether it's five to one from the investment versus the reward, or if you actually look at the numbers, it's more like one to almost 500 thousand security professional who is highly trained to an actor that is unsophisticatedly trained. Just the statistics are just ridiculously out of whack with regards to the vendors. But the vendors are trying.

Then you look at the users, which we've talked about a lot. I totally agree, with regards to - it will have to start with you. It has to start with the people and how you actually invest in the people that you have around you. How do you train them? Is it 15 hours versus one hour for fire drills to cyber? It really shouldn't be that way. Unfortunately, we're seeing the budgets decline for cyber training as well, cyber spending, which doesn't really bode well.

Then I think, thirdly, you just have to understand the hacker. You have to understand their motivation. The hackers - five years ago, people thought the hackers were lazy, or they weren't very smart. You can look at the statistics, and the hackers are extremely highly educated. The other thing is, they're very, very motivated. They're cranking out malware, they're cranking out variations of malware faster than most agile development shops can.

Like I was saying, earlier at our breakfast, every 20 seconds, a variant comes out for IoT malware. We've been sitting up here now for 30 minutes, just think of the variants that are out there in play. Also, if you look at the threat reports, whether it's Verizon's or whether it's NetScout's, or any other security vendor, the time for discovery of a device on the internet has gone from 15 days to five days. I expect next year, that to be one day.

It's really interesting if you look at the adversaries. You take this thing together, you put the triangle back together. You look at the people and the users. You look at the vendors, whether it's an IoT vendor or security vendor, and you look at the hackers making up the threat landscape. It's sort of an interesting place to look. Again, as I said in my very beginning, understand what risks, and what's valuable to you, and understand what's assessable and accessible by that triangle, and you put your asset right in the middle, and I think you'll do better than what most people are thinking.

Vik Phatak, NSS Labs

Thank you. So, I think we have to wrap up here. It sounds like…we have time for one question.

Audience Q&A

Gerry Christensen, Founder & CEO, Mind Commerce

Gerry Christensen with Mind Commerce, North America, United States. My question is, based on the fact that we've been doing some work with helping companies mitigate unwanted robocalls, and also help them receive wanted business calls. So, you touched on the voice element of this in part of your discussion.

My question is, as the social engineering attacks get more sophisticated and they have a synchronised attack that involves not only email but also, perhaps a call, and to the extent that things like conversational AI become more prevalent, things like Google Duplex. How do you see us attacking - or dealing with those synchronised attacks? How do you see us mitigating those?

Vik Phatak, NSS Labs

Who wants to take that one? It's a good question.

(Unknown)

It's a great question. We've discussed the fake videos as it relates to our protective mission. Obviously, if somebody puts out a candidate video with a bunch of statements that were not made, or in a context that's completely out of place, it's a concern for us. Obviously, the artificial intelligence that's coming along, I know there's a lot of research that's been done by academia to identify and categorise these deep fakes, for example.

But at this point, with voice, as you're saying, it's an emerging trend - an emerging threat that we've yet to find a way to counter, honestly.

Ted Ross, SpyCloud

Yes, there's an app that anyone can download, I won't say the name, because it should be illegal. Hopefully it will be illegal soon, but literally you can download this app and for free, you can plug in somebody else's phone number, and then make a phone call, and the person you're calling, the caller ID that shows up on that phone is the other number.

So, if I wanted to try to scam somebody, I would put in the IRS 800 number, and I would call them, and they would think that I'm somebody working for the IRS. They usually trust the caller ID in their phone. So, again, the zero-trust message - educate the whole world, don't trust even your caller ID. That will be illegal, right?

But to add to that point, as you see, industry has also been at the forefront of the deep fake phenomenon. They also want to make sure that they mitigate it from their perspective, because it hurts their reputation; it hurts their business. I think you'll see a lot - I hope, a greater response from the Googles and the Yahoos and the internet providers to address some of that technology.

Vik Phatak, NSS Labs

Thank you. With that, I want to thank you, and I think we're out of time here. Thank you very much.

[Applause]