Dave Allen: Hello. Hello. I'm Dave Allen, Vice President and General Manager of Oracle's Internet Intelligence Program. I'm pleased to introduce our next panel, Cyber Security, A New Frontier. As enterprises and the public sector struggle with new challenges, I'm excited to hear the views and insights from this group.

Kicking it over to Garrett Graff, Director of the Aspen Institute's Cyber Security and Technology Panel. Garrett.

Garrett Graff: Good morning. Thanks so much for joining us today. I'm excited about a great lineup. We have sort of representatives of all parts of the cyber ecosystem here today. Amy Hess, the Executive Assistant Director of the FBI's Cyber Division, along with a couple of other words in there. But the relevant thing to us today is cyber. Jeff Greene from Symantec, and Kelly Bissell from Accenture. So, we've had sort of a representative from the government, a representative from the security industry, and a representative who works with the private sector on securing companies and helping companies navigate this new territory.

I thought I would start off this morning by asking you each to help do a little bit of level setting about what the threat landscape is today. And I wanted to actually first turn to Jeff, because Symantec, just even in the last couple of days, has put out some really interesting and uniquely scary new research about an emerging threat that you guys are seeing, that sort of gives us a sense of I think how challenging this problem is going to be going forward.

Jeff Greene: So, Deepfake?

Garrett Graff: Yes, yes.

Jeff Greene: So, it's always fun to be the scary guy on the panel. So what's Garrett's mentioning is a few days ago, our CTO did a presentation talking about a particular attack, theft we saw recently where a finance executive of a company got a voicemail that said, "Hey, this is fill-in-the-blanks CEO. It's urgent, we need you to send a wire transfer end of quarter. We've got to get this done, business critical."

So, the executive thought, all right, my boss is telling me to do something. I'm going to do it. The problem is it was a completely fake audio. And unfortunately, one thing Garrett said about the new landscape, this is the old landscape in a new iteration. It is using psychology, melding it with technology, and getting people to do things that they're not going to do if they stop to think about it.

But this idea that someone is going to spoof the voice of your CEO, or your boss, or the president, or whoever is pretty frightening, and unfortunately, it's not that complicated. If you google, "Make deepfake audio, make deepfake video," you'll find tools online that will help you do that. So that is real, it's emerging. It's a variation of an old scam. Another iteration is business email compromise. But it's just one more thing that people need to start thinking about.

And you'll see this, this particular one was a financial theft, but you can imagine the impact it could have in a political atmosphere. The video doesn't even have to be that good to dominate the news cycle for a couple days and create distraction, perhaps in the late stages of a campaign. So, it's always a game of trying to stay one step ahead of the attackers or the bad guys, but this is a new one that kind of makes ...

We haven't been told. We've been told, "Look at your emails suspiciously. Don't click on that link." We haven't told, "Be suspicious about the voicemail you receive." And we're moving into that world.

Garrett Graff: And I think one of the common threads we're going to see in a lot of this conversation this morning is the continued human frailty that is the weak point in many of these threats.

Jeff Greene: If you want to dig deep on this, Hugh Thompson, our CTO, did an hour long presentation at RSA Singapore. I lost track of the day, like three, four days ago. And he has on a technologist, basically a professional scammer, and police, Singapore police, to talk about how this happens and what you can do, and it's a really interesting presentation, so you can get all pieces of it if you want to dig down.

Garrett Graff: Kelly, I want to turn to you next, because one of the things that you do that's of tremendous value to us trying to understand this annual study of the cost of cyber crime, that sort of looks like how cyber crime is impacting business on a day to day basis, and where that threat is going. And I wonder if you could talk a little bit about what you found in this year's study and what it says about the landscape that we're facing today.

Kelly Bissell: Yeah. We've been really tracking the cost of cyber crime for many years now, along with the Ponemon Institute, and they're pretty good at tracking this. And each year, we're seeing slight iteration change, if you will, in what's going on. And so, here are a couple of takeaways.

One, the internal threat, internal people doing bad things, is on the rise. The cost of cyber crime has risen from last year by about 30%. So, if you look at all the cost of a breach, we see the big ones in the newspaper, but everyday, most companies have little incidents almost everyday. So, on averages, last year, I think the cost was about $13 million. Now it's around $19 million. So it's ticking up.

What I'm worried about is which companies are failing, if you will, in that cost function, which companies are getting breached more often, and why. It's the companies who have not deployed these tools. I don't mean just the technology function, but the tools and processes across the enterprise. So many companies will deploy a tool in a pilot environment, if you will, and then stop. And then a new shiny tool pops up, and they try to get that installed too.

Really, what we find is, the ones who actually pick something like Symantec or some other vendors, and deploy it across the enterprise at scale, they get breached less than half of everyone else. So I think we've got to really make sure companies around the world, and governments, frankly, for that matter, are more mature in how they deploy these tools across the enterprise.

Garrett Graff: Amy, I was going to ask you this same type of question of, give us a sense of, you're relatively new to your role overseeing the FBI cyber branch. And as you have been stepping into this, sort of, what do you make of the threat landscape? What are you seeing that's particularly troubling, and where do you see this threat going over the next six months to a year?

Amy Hess: Sure. I think that whether we're talking about influence operations, whether they're intended to change the way you think, or giving someone access to something they shouldn't have, for whatever reason, or whether it's an insider threat, or whether it's an intrusion activity, I think that all those things clearly are on the table. And when we look across the threat landscape, particularly we're focused on both nation state actors, particular with of course the big four, with China, and Russia, and Iran, and North Korea.

But we're also looking at the criminal enterprise, this really evolution of the criminal ecosystem, where you have the criminal actors out there who just, for profit, have created their own, if you will, culture, where one set produces malware, and another set will buy the malware and provide the delivery system, and another set provides the infrastructure, and another set will pull the information and then try to sell it on the dark net.

I think that all those things concern us. Particularly concerning, I'd say though, from our perspective, is what causes us to stay awake at night, and those types of things are the attacks against critical infrastructure.

Garrett Graff: We're celebrating this year the 10th anniversary of the Aspen Security Forum, and since this is a panel on cyber crime and cyber security, I'm obligated to mention the term Cyber 9/11 and Cyber Pearl Harbor, which is something people who have sat through panels like this at forums like this over many, many years have heard, sort of this fear of this looming thing that was to come of a Cyber 9/11 or a Cyber Pearl Harbor.

But what really strikes me is that what we have seen over the last two years is things that 10 years ago to people on this stage would have seemed like a Cyber 9/11, a Cyber Pearl Harbor, are now sort of run of the mill events that we actually pay very little attention to as they come and go.

Over the last year, we've seen two major American cities, Baltimore and Atlanta, effectively crippled for days, weeks, months at a time by ransomware attacks. We have seen incidents like WannaCry and NotPetya hit a US company like FedEx, a $400 million damage, Merck, circa $300 million damages, sort of

numbers, that to people on this stage 10 years ago would have been the worst case scenario they could imagine, really seem like things that we no longer worry that much about.

And I thought I would sort of ask each of you to sort of speak about how you see the scale of these attacks hitting us, and what has changed that we are not that concerned, it seems, as a country, about these attacks that were the thing that we used to fear. Kelly.

Kelly Bissell: Actually, I'm really concerned about it. I think we haven't really created a mechanism by which, how do we defend against these things? So if we're talking about ransomware attacks, you mentioned Merck, it transversed across their global network in I think less than two minutes. There's no way a human can find some malware, and make a decision, and do something about it to reduce the risk.

So we have to have these automated, really advanced technology solutions, I don't really want to say AI, but it could be, to really look at these things, detect it, and then create a good safety net, a plan to make sure that we protect the companies. So, I think the companies around the world that we serve, they are concerned about it. They just don't necessarily know always what to do about it.

And then, we have a governance structure, because we have IT, if you will, and they have OT, the operational technology group, and the plants, and so forth. They don't necessarily talk inside the company. So what we find is, everybody's concerned about it, but we're trying to figure out how do we solve this problem from a governance standpoint and a technology standpoint.

Garrett Graff: Jeff, how do we make this threat more real? How much of this is sort of a language problem that we're talking about this?

Jeff Greene: You talked about what would, 10 years ago, raise alarm. I think about what would raise alarm two or three years ago. When you talked about Atlanta, Baltimore, and it couched as a ransomware attack, and it was a ransomware attack, but the piece of it I think we need to be focusing on, it was a destructive attack. There's almost a normalization of destructive malware.

Big cyber crimes in the past were thefts of volume of data, stolen IP, privacy violations. What we are seeing now is the widespread and common usage by common criminals of destructive malware. They go in your computer, they wipe it, it's destroyed. You can never use it again. And the new variants we've seen, Shamoon was a big one in 2012 in Saudi Arabia. Back then, the way it worked was if you had good forensics, you could pull a lot of the data of it. Now, before they break the computer, they delete the data. So, your recover is further complicated.

And when I was on the hill working on these issues 10 years ago, we didn't even conceptualize destructive attacks in this way. We were thinking using computers to make physical objects move and do bad things, stocks and things like that. We need to re-conceptualize what destructive means and think about the flat out destruction of hardware as a new form of attack.

And just as I said, the common usage of it, we've seen in the past couple of years and we put out a report recently, the increase in attacks on enterprises by ransomware, by this destructive malware. It used to be individuals would get compromised, bad link, bad email, whatever. You have to pay the ransom or you'll lose your pictures. Now it is a significantly more sophisticated staged attack, the lateral movement that Kelly was talking about, waiting for the right moment when you have enough computers compromised, to take down a city or a company.

And the way they're doing it, again, is destruction, and if you don't pay up, you're looking at destroyed devices. And for me, in the language piece of it, we use the word ransomware and lots of people do, but I think we need to make sure people understand that means breaking things, and the implication of breaking those things.

Garrett Graff: Amy, sort of the same type of question on this theme for you, how is the FBI dealing with what has seemed like a order of magnitude growth in ransomware attacks over the last two or three years?

Amy Hess: Yeah, clearly, the speed, the scale, the agility of attacks just has really proliferated. And what that means for us is what we're seeing, much as he said, was really how criminals or individuals are taking advantage of that. And what I mean by that is that a lot of companies, a lot of big corporations have built some really good security programs. They recognize that and to some extent, then maybe that becomes like a game to see if they can do it.

But really, where the money is is the companies who don't have those things in place, right? And so, that's your target, that's your target set, to go after the, whether it's the local government, or whether it's a smaller company or business that you think really, that's where I can maximize my potential to be able to get what I want, by deploying the ransomware, and they will have no defense to this. And so, the likelihood of them paying is exponentially increased.

Kelly Bissell: Yeah, could I add one thing? I think it's something that we're finding that is really important. It used to be that it was for a particular purpose, like I wanted to see if I could get in, or some financial gain. Now, I think it's much greater. So, there was a chemical company in the mid west that was shut down, then shortly after that, it went to bankruptcy.

I wonder, what was the purpose? Was it to shut the company down? Was it by accident? Or was it to allow another competing company to take advantage of

the marketplace?So, I think we've got to be really thoughtful about what is the purpose of this ransomware.

Jeff Greene: Or to short the stock of the company you took down.

Kelly Bissell: Exactly, that's right.

Jeff Greene: And there are endless iterations in the minds of the criminals.

Kelly Bissell: But even the ransomware itself, it used to be complex. Now, it's really easy to use by almost anyone, right? So that's what we're really worried about these days.

Garrett Graff: Yeah, and I think both of you sort of touched on something that we think a lot about when we're talking about this in our cyber program, which is, for all of the investment in cyber security by companies over this last decade, the rise of the CISO, the rise of chief security officers. When you look out across the landscape of American business, and even really, American government, the number of private companies and governments that have a sophisticated enough security system to protect against a nation state, or even sort of a relatively sophisticated transnational organized crime group is relatively small.

If you look at the Fortune 500, you're probably closer to 50 of those companies actually have a sophisticated enough security system to withstand a real attack. And I'm curious, how do we, when you're looking at the mid west chemical companies, when you're looking at under-funded city or county governments, I mean, I think it was two Florida counties who've been hit by ransomware attacks, with six figure payments, just in the last couple of weeks as well, how do we sort of get cyber security to trickle down from not just your Fortune 50 companies, but to your Russell 2000s, to your city governments, your county governments, your state governments, even, to a certain extent?

Kelly Bissell: I think this is an important thing. I actually think that most of the 50 actually can't do it alone. The ones who do it well are actually in an ecosystem of other players, and it's government, it's vendors, it's third parties that help them create an incredible security program. Those are the successful ones.

As you move down the stack of the size of company, and even going to state governments, it's really, really difficult. Because the state government, they can't afford to hire really good cyber security experts. So they're going to have to really depend on third parties to help them solve this problem as a team, if you will. That's what we have to do. Because it's a numbers game. We've got 100 people or even 500 people in security in a big Fortune 50 company, but the attackers, there thousands and thousands of them.

Garrett Graff: Amy, sort of the same question, how do we get cyber security to trickle down?

Amy Hess: Well, I think that, and let me just use a, flip to the example previously with the company that declared bankruptcy. We had a great example back in January with a company, a small business out of Portland, Oregon, a company of about 600 employees that was struck by ransomware and a botnet, and they immediately contacted us.

And we were able to, now, granted, all the moons aligned, but we were able to engineer a decryption key, and we were able to get them back on their feet and running within three days. And as a result, actually our Portland office ended up receiving thank you notes from the company, because otherwise, those folks would've been laid off. It would've crippled their operations.

And it goes to the point, though, of a, for us, anyway, it's a matter of how quickly we can find out about it, so we can A, do something about it, and B, figure out who did it, how they did it, and hopefully keep them from doing it again. And so, for us, it's the speed of notification when it comes to the victims.

Garrett Graff: Agreed.

Jeff Greene: So, Amy talked before about the criminals will seek out the least sophisticated victims. But I would flip it to say it's almost a trickle up. I mean, this is the part of the panel that I'm sure was said almost precisely in 2009, if there was a cyber panel, which is, they would have been saying this forever. But it starts with the basic hygiene.

You look at Baltimore, and I don't want to blame the victim, but you have to assume any systems are going to get compromised. What happened in Baltimore is they had a vulnerability that allowed a malware, the ransomware to spread almost completely and very quickly, and there had been a patch out for it about a year ago. It was the same as WannaCry.

So, you have to look at doing the basic things. If Baltimore had been able, and I don't want to fault them, because it's not as simple as pushing a button and sending a patch out, but if they had patched against their vulnerability, they would not have been hit as hard. It would be a great day if we were in a world where it took a sophisticated criminal gang or a nation state to take down a city or a company, but we're not there yet, because we're still not doing the basic things, because I think there is still a sense of it will happen to the other, and cyber security is still too often considered as the extra.

When I worked at a bicycle shop after college, we would lock the door every night because we didn't want them to steal our bikes. No one had to incent us or tell us to do that, but it still feels like to too many organizations, cyber is something they'll do if they get to it, not as a baseline of doing business today, and that's a mindset that I think we really need to change.

Garrett Graff: Adding sort of another layer to this conversation here, about sort of looking at where the threats are coming at, one of the divides between the private sector and government often ends up being the attribution question, which is, for Kelly, for the companies you're working with, they don't particularly care why they got attacked or who attacked them. They want to get their operations back up running, they want to get their data back, they want to get the work going again.

For Jeff's world, sort of understanding who the threat actors are. For Amy's world, combating and actually trying to take these operators down. Attribution matters a great deal. And I wonder if each of you could talk a little bit about how, from your seat, you think about attribution, and sort of how you're seeing the US government in particular, in sort of Amy's world, the US government make quicker and more regular attributions of large scale cyber attacks.

Amy Hess: So, basically, attribution to us is everything, right? So, for the FBI, what we're trying to do is, right, this is the Federal Bureau of Investigation, we're trying to investigate it to figure out who did it, who's behind it, and how to hold them accountable for it, or at least how to better inform our partners, whether those are other government agencies, so that they can take action, whether those are offensive actions or whether those defensive actions or collection opportunities.

And our private sector partners, so that they understand who did it, who's behind it, the techniques, the tactics, the procedures, the TTPs that are involved, and how they went about doing it, and then can better defend themselves. We work very closely in trying to push out that type of information with DHS, and try to identify, once we see an attack, here's the techniques that they use.

But also, for us, the quicker we can do the victim notification, whether we find out about it first, or whether the company finds out about it and contacts us, the quicker we can get to who did it, then obviously then the quicker that we can take them off the playing field, or at least make them change those TTPs so that that particular attack venue is gone.

Garrett Graff: Jeff.

Jeff Greene: In any attack, there's the who and there's the how. For us, the how is really the big question. First, can we prevent it in the future or can we stop it from other customers if it's spreading, and second, can we mitigate. And so, to the extent we look at the who, a lot of times it is to connect a particular attack to previous groups or types of attacks we've seen, because that helps us get to the how faster. If we see a connection, that may speed up our research to figure out what they're going to do, what their TTPs are going to be, how they're spreading. That will effectively allow us to stop the how quicker.

So, our work on attribution is a little differently focused. It's focused on getting us to a protection faster. Sometimes it overlaps with the government interest, but more often, it's us bucketing attacks and different types that allow us to protect customers and to mitigate an attack quicker.

Kelly Bissell: This is why this ecosystem is really important, because it's almost like a patient. Patient's on the table. It's sort of our mission to keep him alive, get him off the surgery table, if you will, make sure they're back going, they're operating, if you will, and then make sure we get that information over to law enforcement, so they can actually determine root cause and some other things, intentions, which are really important, like what are they after and why, and even the vendor, so that we can create a network effect. That way, we can identify that threat and protect all the other people or patients around the world from being safe.

So, this is where this ecosystem is really important, to make sure that we work in a fluid manner. We have work to do.

Jeff Greene: But it's better than 10 years ago, the relationship-

Kelly Bissell: It is better, yeah.

Jeff Greene: Between companies, with the government and the private sector. Through DHS, there's been significant improvement in the 10 years I've been focusing on this.

Garrett Graff: Where do each of you continue to see the policy pain points in cyber security? Sort of, what is the US government not thinking about at a policy level, or not addressing at a policy level in the way that it should? I won't ask Amy first. I'll give her a moment to come up with a diplomatic answer to that.

Amy Hess: Let me think about that.

Kelly Bissell: Maybe I'll start, if it's okay. You know what? One, I'm no policy person. But here's my observation, that we have, in the United States, we have multiple jurisdictions creating their own policy. That confuses our companies. Especially if you're a multinational company, you operate outside of the United States in multiple countries, because you have to comply with not only each state and the federal government, but also all the other governments in which you operate. It's a complex thing, and it really adds an enormous burden on their companies. That's one thing.

The second thing is, the policies, in my view, many times are behind where technology is advancing. What we got to do is get government and regulators thinking about the future, not about the past, and that's where we've got to get them, so that we can not constrain the company, but enable the growth, so we can thrive.

Jeff Greene: I think the government has, for the most part, played too passive a role in driving security, whether it's in critical infrastructure, retail, whatever. I'm not advocating for a broad regulation, but the government has a lot of levers of power to push security, and the voluntary efforts in this framework, the new privacy framework are important and they've done a lot of good. But no matter how loud you yell, if someone's not listening, they're not going to hear, and there is a responsibility, particularly in the critical infrastructure sector, if you're a provider, to provide the security, and if you're in the government, to ensure that there is some baseline of security.

So I think the government, and there have been efforts at this, I was part of one when I was on the hill, and it failed, and there have been others that have failed. But I think the government needs to not be, the US government, terrified of the idea of whether it is regulation at one end, tax incentives on the other end, but use the levers of power to drive security, whether it is patching and updating or whether it's deploying software.

And that's one area where Europe is very far ahead of us, and that will impact the companies that do business globally. If we do business in Europe, our security in the US is going to have to be the same. But we can look to Europe for the good and the bad of what they've done. But we need to stop sitting back and thinking that it's going to happen voluntarily, because if it hasn't happened yet, it's not going to.

Garrett Graff: Amy?

Amy Hess: From my perspective, I would say that for one thing, the roles and responsibilities need to be clarified, whether that's in the government, or with relationship with the private sector, or what industry is doing, what academia is doing, and what should they be doing. So, for one, basically on that point, is just to be able to clarify what are the base level responsibilities and obligations among society, among the folks in this world.

The second piece, though, is what should we be comfortable with? So, when, for example, a nation state takes action against us, what is the threshold? What is that line in the sand where we say, "Okay, that's off base. You can't do that. And we will take offensive action when that occurs." What is that thing?

And moreover, are we thinking through the secondary, the tertiary implications of the actions we may take? So, when we talk about private sector, for example, having the ability to take offensive operations, that's kind of a scary proposition, because there are a lot of machinations to thinking through, what are the consequences? What's going to be the collateral damage if we start taking offensive operations unilaterally without some governance structure, without some, really, some policy in place to say what we can and can't do, or should not do.

Garrett Graff: Amy, you mentioned roles and responsibilities, and when you sort of think about the trickle down or trickle up effect of some of these cyber incidents and cyber breaches, Third Way has done some great work over this last year about the cyber enforcement gap. Effectively, I think the number is about 98% of cyber crime goes un-prosecuted.

And that really, you need to end up above a certain threshold for the FBI to be able to dedicate the resources to it, and that there's not this sort of local and state efforts to combat cyber crime. You know, if you walk into your local police precinct and say, "My purse has been stolen. My car has been stolen." Like, your local police department understands how to deal with that. And if you walked in and say, "My business has been hit by a ransomware attack," or, "We got hit by a deepfake audio attack and lost next week's payroll." The number of local and state law enforcement agencies in the country that could deal with that, you could probably count on one hand.

And I'm always struck by how little the FBI, how little the secret service, how little HSI, as sort of the three federal agencies that have cyber responsibilities, have grown to meet the cyber threat. You know, you look at the agent corp of the FBI today, and it's about 30% larger than it was on September 10th. And in those years since, you've taken on this massive counter terrorism role and this new cyber role.

And I'm curious, sort of from your desk, as you sit there everyday, and you sort of look at this tide of cyber crime, transnational organized crime groups, nation states, what do you make of how we ever are able going to be, to wrap our arms around what this threat is at the scale that it's operating?

Amy Hess: That's a great point, and something that we are clearly thinking about everyday. It consumes big chunks of my day in particular. Because we, the government, will never be able to compete with the private sector based on salary. So how are we recruiting these individuals to begin with, to come work for the government, these people with these great technical backgrounds, or technical experience, or education?

I think we need to holistically think about that, the benefits of perhaps going back and forth between the private sector and the government, and how we may be able to facilitate that type of, really, the incentives that might be offered or available to be able to do that.

The second piece, though, is, with respect to the state and locals, very much a concern as it is. A concern within each of the federal law enforcement agencies is to, how are we posturing ourselves to educate our workforce? So, when they come in, even if perhaps we don't have as many technical experts as we would like to have, we can leverage the ones we do, and perhaps identify the aptitudes of the others, who at least we can identify as, hey, they would make perhaps a

good cyber investigator, coupled with a good technical expert, so that we can address that problem.

And then to educate the broader law enforcement community. We have cyber task forces in the majority of all of our field offices, where we have state and local departments who are increasingly more interested in partnering with us and being on these task forces to understand the problem, because they are starting to see it hit home. They are starting to see it hit the pocketbooks, and the local municipalities of government that are attacked by these issues.

Garrett Graff: Kelly and Jeff, I just wanted to ask you a similar question. What do we do about, what I would loosely describe as like, the small to medium scale cyber incidents?

Kelly Bissell: You want to start or you want me to?

Jeff Greene: Go ahead.

Kelly Bissell: I actually think that we need to band together different groups. So if you look at in the US, there are 1,600 or more, maybe, credit unions. Those are small banks that you can't compare to a Citi, or a JPMC, or that sort of thing. I actually think they should band together and have one service provider help them all, and that's economies of scale, if you will.

And the same thing, you could do the same thing with retailers or other sectors around the United States. I think that's an easy thing for us to do. But they have to really be aware and be committed to be able to move down that path, with the risk tolerance. And the hard part might be universities or small-medium businesses that don't fit in a roll-up sector. And I think we do have to have an answer for SMBs.

Jeff Greene: Kelly's point is a good one, managed services for a company that can't afford a full SOC, or a CISO, or a security team. It's important, and if you can do it with another group of similar companies, you get information shared, you get economies of scale. But the other thing, and if you're playing cyber bingo, get your card out, because we have AI and ML. Haven't heard those yet.

But machine learning particularly allows you to, it's a force multiplier for a human. We use it internally to detect attacks that we wouldn't have otherwise seen, to filter out the number of alerts that goes to one of our [inaudible], one of our specialists. So, if you use the technology, you're never going to take the human out of it, but as General Thomas said, the computers are good at looking at patterns. They can pick stuff out and they can also learn when not to pick something out. So you can simplify what is ultimately going to go to that end small business, not alert them unless they really need to be alerted.

But I want to go back to what I said. None of this matters if you're not doing the basics, if you're not having the patching and updating, if you're not using two

factor authentication, if you're not using a basic security tool and turning it on, and if you're not just being aware. Because criminals in the end are going to take advantage of how we think, our psychology, as much as our technology. So that is always going to be for me the baseline. Doesn't sell as well as technology, but it is important that the human factor, the human is the weak link, but we need to make the human part of the security link.

Garrett Graff: I want to open it up to questions here in a second. So, let me ask one final question for you before we open it up for the audience. When I look back over these last 10 years of particularly nation state attacks against the United States, each of them in their own way represents an acute failure of imagination on the part of the private sector and the US government.

When you look at Iran's first attack against the United States, we were unprepared for that to be consumer-facing financial websites, and we were unprepared for it to be a casino in Bethlehem, Pennsylvania. When we look at North Korea, we were unprepared for their first attack to be against a Hollywood movie studio. When we look at China, we would spend an incredible amount of energy securing all sorts of government structures and had sort of forgotten about all of our personnel records.

And when you look at Russia, for all of the conversations that we've had about critical infrastructure for years, and for all of the hyper you hear about power grids, and water systems, and healthcare systems, and everything, we were unprepared for Russia's first attack against the United States to be our election systems, and Facebook, and Twitter.

So, my question to each of you is, what is the next failure of imagination that we should be looking for over the next couple of years, that we're not prepared for?

Jeff Greene: Want me to-

Kelly Bissell: Yeah, go with Jeff first.

Jeff Greene: Bingo again, Internet of things. And the reason I said that is IoT is great, it's going to be revolutionary. I agree with David on the 5G point. That's really where 5G is going. But the failure of imagination I think is going to be to a large degree in the people creating those devices, because when they set out to create a device that does three things, they're going to imbue it with personality, they're going to see it as something that can do what they want it to do.

The problem is it can do a lot of other things. And when you're working on that device, you need to think about it not as whatever cute name you give it that does X, Y, and Z, but as a box with sensors, and motivators, and actuators that can do anything, and think about how a bad actor is going to use it. Think about

the example of Facebook. Whoever thought it would be used for information operations? Probably someone, but it wasn't widespread.

So both on the security side and on the invention side, you need to think about how a device can be used, not how you want the device to be used.

Garrett Graff: Amy?

Amy Hess: Yeah, I would say that certainly, the Internet of things would be right up there, because this proliferation of technology, this rush to time to market then really manifests itself in the sense of, it's at the expense of security. And so, without thinking through the security implications, the front end is going to cruelly present vulnerabilities on the backend.

But what we see from the FBI's perspective, is I would say that then from the government's perspective, is we look at, again, who's doing it and why they're doing it. It really comes down to, how can they either on, let's say, on a criminal perspective, how can they separate you from your money faster than the next person? It's because they're going to try to gain your trust. It's the typical confidence game, is that how are they going to do that. They're going to make it look like it came from somebody you trust. They're going to rely on the fact that updating your system or downloading the latest patch is inconvenient.

And so, therefore, it's the human factor. It's that human link. And so, to be able to get you to click on that link, or to be able to believe the person on the phone or in the email, that's key to them, and that's where we see an education process, really, a public awareness campaign needs to happen, so that people don't just believe everything they read. Consider the source.

Kelly Bissell: Of course, no one's ever accused cyber security people of being creative. More propellor heads then anything else. But I would say that we've seen a little shift in the marketplace, where we've added professional skepticism to cyber security people. And that's where law enforcement people have come over to the private sector, and that's helpful.

But I would really couple that with the imagination of the next generation. As companies are disrupting their own sectors, so think of things like Uber, what we have to do is embed security into those disruptive ideas. I think by all accounts, the United States has great creative capability in thinking of new things to do. We just have to embed that security piece in that ideation phase of that idea, so that we don't lose track of it and have to go patch it once the you-know-what hits the fan.

Jeff Greene: There's no reward for being secure to market. It's only about being first to market, and that's ...

Kelly Bissell: But executives must change their thinking, because if they go to market fast without security, they're actually doing it, I don't want to say negligently, but they're putting their firm at risk. So I actually think they need to be holistic in their thinking.

Garrett Graff: And I guess, a little bit to what Jeff was saying earlier about the role of government stepping into this is, how does government sort of re-shift some of these incentives to encourage security as part of that process-

Kelly Bissell: Yeah, because like, minimum viable product is something that we've got to really correct, I believe, when it comes to cyber security, because we usually cut out as much as we possibly can, to get that minimum viable product out to market, even within government. So, that's just one of the things that we probably have to change the mindset of.

Garrett Graff: The other thing on the failure of imagination that I would put on the table, data manipulation attacks, that we've gotten so used to data theft as the problem, that I think particularly for society-wise, we are unprepared for the level of attack-

Kelly Bissell: We've seen it.

Garrett Graff: Where you could begin to see people wondering whether the amount that's in their bank account is correct, whether the stock that they think that they bought at a certain price was actually the thing that they bought. Or you look at medical systems and whether hospitals can actually trust that the medical record that's attached to you is the thing that's actually attached to you.

Kelly Bissell: Yeah, I think that's the hardest thing and the thing that scares us a lot, is the integrity of that data. And we have seen just a couple of examples, and that's just us, so maybe there are many more out there. But copy, and then destruction, and then that integrity of that data is really important.

Garrett Graff: All right. Start down here, the question.

Joe Nye: Joe Nye from Harvard. I'd like to press you a little bit more on the Internet of things, in particular the way we perceive the problem of the cyber issue. You described Pearl Harbor to ransomware, to destructive ransomware. But is it possible that the IoT may change public attitudes in a dramatic way that we haven't thought through, when you talk about imagination?

For example, no lives have been lost in the things that you described. One of the things about IoT, it's not just machines talking to machines, it's something which can lead to lives rather than economic expense. When the CEO's pacemaker is hacked, or when your self driving vehicle goes off the road because it's been hacked, and lives are lost, you may get a very big change in public attitudes. Bruce Schneier suggests that this may be, in a sense, the turning point, the

Sputnik moment of how we perceive the cyber threat. And I'd like to get the panel to speculate on that aspect.

Kelly Bissell: I think you're right. As a matter of fact, when NHS in the UK was shut down, they had to divert ambulances all over the place, they couldn't perform x-rays, CT scans, all that. It does impact human life. If we shut a plant down and all the electricity goes off in a city, that has cascading effects.

And this is not a fear mongering sort of thing. This is reality. And I think David Sanger's book did a really good job of sort of painting the evolution of where we're going or where the bad guys are going, and we're still in test mode. But those tests are getting stronger and more direct, and that's what, I hope the public as a whole is aware. I'm just not sure it is.

Garrett Graff: David, was that sufficient as a book plug, or do you want me to sort of ... So, The Perfect Weapon is available in paperback right now. New chapter on 5G in paperback edition, out last month.

David Sanger: You didn't hold up the cover?

Garrett Graff: Amy?

Amy Hess: So, yeah, I think your point well taken, is that what will it take for everyone to recognize this is a real, big, huge issue. And it does, lives are in the balance. And so, for us, that takes me back to the consequences. What are the consequences of these attacks? Are we providing a sufficient deterrent effect by attributing this type of activity to someone that we could potentially bring criminal charges or sanctions against? Are we, not only from a defensive perspective, are we playing enough offense? And what does that offense look like?

And again, whether it's consequences of a, we hear a lot about the name and shame type of approach when it comes to indictments, and that's a good thing, but I worry sometimes that it also implies that, well, you're never going to catch that person. Well, maybe that's okay, but from the sense that we've just limited their ability to travel, or we've influenced people behind them to look at that example and say, "That means I won't be able to travel. That means I won't be able to go study in another country." Are we deterring that type of behavior?

There's got to be real consequences behind this type of thing, because otherwise, we absolutely run the risk of the boiling water example of where you slowly turn up the temperature and before you know it, and it's too late, you can't do anything about it.

Garrett Graff: And I will say, the FBI has had remarkable success catching some of these Russian hackers and eastern European hackers when their girlfriends insist on taking vacations in western Europe. That is in some ways the most powerful tool that the FBI appears to have at its disposal these days.

Jeff Greene: I hope Bruce is right. I hope there's a turning point. I don't think it'll be a Sputnik moment, I think it'll be a Tylenol moment, and there were no safety caps on every bottle before then. But I am increasingly skeptical that we're going to get there, because going back to the first briefing I got on this stuff in 2007, we probably had a dozen things that I would've told you in 2007, would've fundamentally changed public perception and government policy, and I think we are immune to it.

So, I don't hope people die, but I hope there's a moment when we can shift the focus and create the incentive for security that doesn't exist today.

Garrett Graff: And I think one of the things you are seeing changed is the way that industries are beginning to try to think about this more as ecosystems, and those downstream effects of an attack like this. And I think sort of one of the moments that you did see, that actually was not a cyber moment but had some impact in the cyber realm, was the long term power outage in Puerto Rico. One of the things that was not on anyone's radar is the one factory in the United States that makes hospital saline was in Puerto Rico.

And so, when Puerto Rico lost power for four months or whatever that was, every hospital in America ran short of hospital saline. And that sort of I think really fundamentally for the healthcare sector began to have them think differently about what the downstream effects of some of these IoT or critical infrastructure sector attacks could be.

All right. I think we have 75 questions and six minutes remaining. So, let's start right here in the middle. Yeah, you, you. Close enough.

Bill Coleman: I'm Bill Coleman from the Carlyle group. Talked a lot about 5G and IoT. Now, what links the two of them is not just high performance and high throughput, but it's that 5G is TCP/IP. It's a software-defined protocol. That means you're going to have applications at the network all the way up level, and they can go all the way out to the devices. That's great, because that will really make it much easier to manage data, things like that. It also means the attack surface went up 5,000%.

Now, under the Obama administration, the Wheeler FCC came out with a set of suggestions, published the paper on what we should do. Trump administration took that down. Is there anything going on to actually help that vulnerability? Because we're going to make these devices and everything out of the internet through 5G 1,000 times more vulnerable.

Kelly Bissell: I actually don't think this is a government issue. I mean, look, we're working TCP/IP, UDP, Telnet, rlogin, all those protocols that we use today were made when? 40 years ago, with no security in mind and no really application vision for where we are today. 40 years ago.

What we have to do, the vendors, the Ciscos, the Microsofts, and now IBM, with Red Hat, and so forth, we've got to change the protocol stack that the internet rides on to be more secure at the foundational level. Then, I think we can be safe across the board. Otherwise, we're band-aiding the problem across the board.

Garrett Graff: Gus HAll right. Down here. Gus.

Speaker 9: [inaudible]

Garrett Graff: Okay.

Gus Hunt: Thanks Garrett. Gus Hunt at Central Federal Services. Throughout the conference, we've heard a lot about the importance of coalition, and coalition engagement, and solving our problems. We didn't talk about it at all here at this panel, so I'm kind of curious as to where are we in terms of engaging across the globe with our partners and our friends in the cyberspace, what's going well, and what can we do to improve it heading into the future?

Garrett Graff: Amy, I'm going to put that question to you.

Amy Hess: Yeah, sure. So, yes, when I talk about partnerships, we talk about partnerships. We're talking not just among the US government, inter-agency, and the private sector, and academia here in this country, but clearly across the globe. We have, in the FBI, we have cyber specialists, cyber agents deployed to strategic locations across the globe in our legal attache offices, where we're in about 90 different countries total.

Obviously, I'd love to have a cyber agent in every one of those, but even despite that, that doesn't stop us from constantly interacting with our foreign counterparts, particularly with respect to the Five Eyes, with respect to other countries that we are constantly engaged in exchange of ideas and thoughts, whether it's Germany, or the Dutch, or others. We are constantly looking at how they're addressing the problem and how they're collecting, and what that means for us.

So, yes, that's occurring across the board, and it's interesting to see the evolution of their policies surrounding this.

Garrett Graff: Amy, let me ask you a followup on that, which is, one of the things that has struck me over the last year, year and the half, maybe, at this point, is that the Five Eyes, which has sort of long been a very strong intelligence sharing network, but has stayed very much in the background, appears to be sort of trying to step out as an organization. And you're sort of seeing Five Eyes come out and speak about encryption, other topics like that.

Do you have a sense of sort of whether that's a conscious shift among the Five Eyes intelligence agencies, to try to become sort of the NATO of cyberspace for this next generation?

Amy Hess: Look, I think everybody recognizes, all these countries recognize that one country can't come up with some unilateral way of doing business, because everything is affected. So, we've got to be thoughtful, though, in the way we get on the same page. The problem is that clearly, there are countries who don't share our values.

We have commonalities with the Five Eyes countries in particular and with other countries, with a norms-based regime that has been established over time with the rule of law, and do not have some of the issues that are associated with certain other countries that perhaps don't have the same record of human rights protections and privacy protections that this country does or those countries do.

And so, I think what you see in sense is correct in the sense of a collected effort to say, how are we going to address this globally, because companies are global. They're doing business in those countries. And so, if we try a one size fits all type of approach, how is that going to look? And We've got to be thoughtful and think about that.

Garrett Graff: Right. Next question. Down here.

Bruce McEver: Bruce McEver, Berkshire Capital. It seems that there's this big elephant in the room that we seem to be walking around, and that is, why don't we have a cyber police? It seems like the FBI is trying to get at it, but there's no mandate, there's nothing else. There's no one in this room that hasn't been hacked. There's no one ... All your companies have been affected.

So I'm a little angry about this. Why don't we get on it? I mean, these are criminals. It's what happened with how the FBI was created, when a bunch of criminals shot up some bars in Chicago. You know, we're doing worse. So, why don't we get together and put together a police force and stop this stuff?

Amy Hess: So, I would say that actually, the FBI was created a little before the whole Chicago bar thing. But despite that, I get your point, and actually, when you think about this particular problem, I would say that, think back to the way criminals used to operate, is, so, let me take you back to the beginning to the automobile, which actually does coincide with the start of the FBI.

Is that before that, it was really hard to get around and to conduct perhaps a bank robbery in one particular location, and then to move to the next location. All of a sudden, the automobile made that pretty easy, a lot easier. Now, you've got cyberspace, where now you can do it at pretty much the speed of light. And

not only are you hitting one bank, you're able to hit hundreds of banks at the same time.

And so, the problem is exponential from what it has previously been, and the problem set we're trying to attack. To your point, though, is we've got to be able to leverage each other. It's not just, the federal law enforcement is going to be able to solve this problem. We've all got to be able to come up with a solution and how we hold others accountable, and what are the thresholds, are there the thresholds. If you lose a dollar, versus somebody losing a million dollars, should we treat those things differently?

And whether it's an individual or whether it's a company, should we treat those things differently? And what is our prioritization schema when it comes to that, and how are we educating state and local law enforcement to be able to address this problem? What laws are we seeing in the states and the local municipalities that will help us address this problem?

Garrett Graff: All right. Is there a woman anywhere in the audience who has a question? All right, over here.

Michelle: Hi, my name is Michelle, and I am one of the Aspen scholars. My question is just kind of along those lines. Do you think that the laws are sufficient in sort of deterring people or allowing you to hold people accountable, or does it need to change, and how do you think that needs to change?

Amy Hess: I feel like the only person speaking. And anyway, but yes, I'll let them weigh in on their perspective. But clearly, I believe that our laws have not kept up with technology. And what we see is over time, laws change because of the way society changes. And the issue that we have at hand now is that society is changing so fast, in a way that how we keep our data, how we value that privacy.

And for that, that means that we can't spend, in my opinion, we can't spend years philosophizing how something should look, whereas we had that luxury perhaps in the past, and say who all will be implicated. Those things are very important to understand from a legal perspective, because when you enact a law, clearly, you're affecting a whole variety and gamut of people, and companies, and organizations.

And so, it needs to be a thoughtful process, but I think we need to do it faster, because in one respect, and I mentioned this earlier, is that what are those thresholds we're going to put in place? What are the obligations of the companies? Not just the law enforcement perspective in reaction to what has happened, but also, what are the obligations of American industry or of state and local governments? What are their obligations?

And really, we need to be clear about that. That needs to be codified, I think, in a way that's clear, to lay out the roles and responsibilities.

Jeff Greene: I don't want Amy to feel lonely.

Amy Hess: Thank you.

Jeff Greene: But I agree, there are laws that need to be changed in a variety of ways. We need to be really careful, and one concept that's pushed out a lot is the whole idea of hack back, and that's one that we need to think really long and hard before we put forward in any way, shape, or form, because there are second, third, fourth order consequences. And how we will then incentivize criminals to create havoc through the hack back.

So, I don't know if that's where you're going. But it feels good and it sounds good to introduce a bill and tell your constituents that you're going to empower companies to protect themselves, but you're probably just putting more people at risk, so be really careful how we move forward.

Garrett Graff: All right. Last question. Right here.

Audience: Hello. I'm from [inaudible], actually. So, thank you for helping out my city. I guess I'm wondering what your view is on the future division of labor between federal law enforcement and local law enforcement, with respect to the proliferation of the Internet of things. That makes the attack surface area much, much broader, and I imagine that's something that will stay within federal purview. So, what do you think that will be?

Amy Hess: I would say that clearly, we've all got to up working. And I mentioned this earlier, as far as, what is the aptitude within the respective law enforcement entities, within state, local, and federal government, in order to be able to address this problem to begin with. But I will say too that we tend to think in terms of, even inside the FBI we do this, is that we tend to think of cyber as some kind of separate thing, when really, getting back to an original point that was made earlier, is, who's behind it? What's the motivation?

Really, you can usually trace that back to whether it's a espionage matter, whether it's a terrorism incident, or whether it's a criminal, white collar or whatever it may be, or something designed to influence us. And so, to be able to use the investigators who already know how to do those things, and pair them with technical experts, I think that's a hugely valuable piece of this.

We don't have to train a workforce from ground zero going up. We've got to be able to leverage what we already have and pair it with a technical aptitude that we need to figure out, how do we address that piece? How do we bring that in? Is that a third party? Is that being able to, once again, like I said, we're not going

to be able to compete with the private sector on salary, so how do we get those folks to come help, with respect to this pairing with the investigative side?

Garrett Graff: Kelly, Amy, Jeff, thanks so much for joining us today.

Kelly Bissell: Thank you.

Jeff Greene: Thank you.

Announcer: Thanks everyone. We'll be back in here at 11:15. There is a break. It's raining outside, so you may want to stay in here.