(no title)

65 MIN · YOUTUBE · HTTPS://WWW.YOUTUBE.COM/WATCH?V=G50FHC-PZK8
https://www.youtube.com/watch?v=g50FHC-PzK8

SUMMARY

The speaker shares their extensive career journey in technology and cybersecurity, detailing experiences from the U.S. Department of Justice to major tech companies like eBay, Facebook, and Uber. They discuss the challenges of building trust between government and tech firms, the importance of transparency during security incidents, and the evolving landscape of cybersecurity, especially in light of recent legal troubles and their subsequent efforts to rebuild their reputation.

- *The speaker began their tech career in the 1990s, advocating for internet access within the U.S. Department of Justice.*
- *They transitioned to eBay and later Facebook, focusing on legal and security aspects, and eventually became Uber's first head of security.*
- *A significant incident at Uber led to their legal troubles, culminating in a trial where they were charged with obstruction of justice.*
- *The importance of transparency in handling security incidents was emphasized, showcasing how Cloudflare managed crises effectively.*
- *The speaker highlights the shift in cybersecurity focus from data protection to operational resilience, especially with the rise of ransomware.*
- *They advocate for building strong relationships between security teams and other executives to foster trust and effective communication.*
- *The speaker is involved in nonprofit work supporting children affected by the war in Ukraine, reflecting their commitment to community service.*
- *They stress the need for resilience in leadership roles, particularly in the tech and cybersecurity sectors, as challenges are inevitable.*

I I have two kind of themes that I want to touch on that I hope at the end of this uh session um kind of get a little bit in your brain. Uh I have been working in technology since the 1990s uh when I got out of school. I um moved uh here to Northern California in 1995. And when I got to San Francisco in 1995, I was working for the US Department of Justice. And it was funny, Mike said had asked me, "How do how did you get like into doing technology uh for the for the government and it was because I asked the Department of Justice if they would give me a direct internet connection to my desk in 1995 and they said absolutely not. we can't let our network touch the internet. So I just kept asking and eventually they let me have a separate computer to use on the internet. And then I was the only person in the office who had a computer that was connected to the internet and I became the gatekeeper to everything.

Um but let me tell you a little bit uh about let's see how do we here's my background. So, I spent my first eight years with the Department of Justice and then I uh in 2002 I went to eBay. Back then, eBay was kind of like the

hottest company in Silicon Valley and it was a really fun place to work for a few years. Right after I got there, we acquired uh PayPal and so I spent a bunch of time uh for eBay and PayPal um building out kind of both the legal side and the um safety and security side of those companies. And then in 2008, I went to Facebook uh when it was smaller than MySpace. Uh it was here in downtown Palo Alto. We were scattered in a bunch of little uh uh I don't know, I was like in an old law firm office where I was working with a with a group of other people and uh we it took us years to get to having a campus. Um, and so I was at Facebook until we became basically the company you know now after we'd integrated Instagram, WhatsApp, Oculus and all that. And then I went to Uber and became their first head of security. So at Facebook I I inherited three engineers and built it up to a large group. Then I went to Uber, inherited three engineers and built it up to hundreds. And then in 2018 I went to Cloudflare, inherited three engineers and built it up again.

So today that's a lot of what I do. I work with startups that need to scale security and technology really fast. So I have my own company and uh we work with three or four startups at a time helping them scale. I also advise uh cyber security companies startups and uh some nonsecurity companies on on security best practices. Um I I'm a venture partner at Costaoa Ventures and I am the CEO of a nonprofit helping kids in Ukraine. So that's kind of my background in a nutshell, but I'm going to take you through uh in particular something uh that I had to go through when I was at Uber. If you look at my roles and my career, there's one theme which is uh I've been at the intersection of where government and technology tech companies meet.

And uh I've spent a lot of time like when I when I was that federal prosecutor here in Northern California, I would go around all the tech companies and I would say tell me about your cyber crime. I want to prosecute it. And they would all say, "We don't have any." There was no incentive. If you're a company and you're having bad things happen to you, why would you tell anybody about it? Is it good for your brand? Is it good for your business? Not at all. So the companies would always say to me, "Oh yeah, we have this." And so they would tell me about all these other issues they had. I ended up like prosecuting the was actually a a guy from Stan who'd gone to Stanford. He was a joint uh he had a law degree and MBA joint degree from Stanford and he ran all of business development for Cisco and he felt that the CEO of Cisco didn't appreciate him enough apparently. So he stole 40 mill as they acquired companies he created his own uh subsidiary called Cisco Systems Inc. Bahamas and he um uh when when they would divide up the stock portfolio, he would put about half of it in actual Cisco and half for himself. And then eventually we figured it out and and so I prosecuted him and I was like that's not exactly cyber crime.

Uh but you know it was interesting. Uh, and then I had to build trust with the companies and then they would actually start telling us about the real issues when they understood they could trust us to actually just go prosecute and not do big negative PR against the companies. Then I switched over and was on the company side. And at eBay, our number one problem was trust. Like if you remember, maybe you don't remember before PayPal, but the business model of eBay when I joined was identify an item, win the auction, put money in an envelope, mail it to the seller, and hope they send you the goods. That was literally the eBay business model. When I joined the company, a small percentage of transactions were going through this little startup called PayPal. and we had our own competitor to PayPal and then eventually you know digital payments caught up and now um we are able to use credit cards and things like that and have asurances on our transactions. But I went to 46 of the 50 states for eBay to talk to regulators and trying to get them to work with us and uh to enable

this platform. I trained law enforcement in like a dozen different countries on how they could uh prosecute somebody for doing bad things on eBay. So, we were like trying to pull law enforcement and government to pay attention to what happened on the internet in the early days. By the time I got to Facebook, it was it was still the same thing. Uh but there was a little bit more tension.

There was a whole uh situation with that guy Eric uh Snowden and you know, he left the NSA and he revealed all these documents that made it look like uh Silicon Valley was sharing everyone's data behind the scenes with the NSA. Um, that wasn't the actual full story. I ended up in the middle of all that basically as the face of of Facebook interacting with the NSA because I had managed our relationship with them all along. And so that was the backdrop when I got to Uber in uh 2015.

And Uber was kind of like um the beginning of that mobile explosion. If we think about like the transition and how technology has become such a bigger part of our lives in the last 20 years, it was really like phase one was like regular internet. Uh oh, we can do e-commerce. Wow, this is amazing. And then part two was that mobile explosion. Uber couldn't exist until there was an iPhone. And uh it's like led to this next generation of explosion of technology companies really taking over the world. And when this happens, when technology becomes the most important thing, all of a sudden the government folks really start to care about technology. And that's what's happened in the last decade. We've seen a lot more initiative going back to around the time of the uh first Obama administration, 2008 to 2012, they really started trying to figure out how do we get closer to Silicon Valley. U President Obama came and visited us at at Facebook. uh so did George W. Bush and Al Gore. Uh and so like you started seeing uh a lot more of that interaction.

So I was at Uber, everything seemed to be going okay and then one day I got this text or email. It was from Eric Newcomer who's a reporter at Bloomberg and he messaged me because he wanted to know about me getting fired from Uber. I had no idea what he was talking about. I was on vacation with my family up by Lake Tahoe. It was Thanksgiving week. I'd taken the week off. Um, after uh getting that, this was the headline I saw. He wrote, published an hour later.

I paid hackers to delete stolen data on 57 million people according to the news. And it just blew up across the planet. My phone started going crazy with people texting me, trying to call me. And right in the middle of that, my phone stopped working because my phone had been issued by Uber and my team had put software on that. And then my team used that software to break my phone and my computer because the company had decided to fire me.

So I was all of a sudden like the most famous person in cyber security for the wrong reason uh about a decade ago and um that hurt a lot. Uh I w I um I'm still involved in litigation related to that. But I um I went into hibernation for about 2 months, grew a beard, didn't want to show my face, and then in early 2018, I decided I got to get off my butt and get back going in life. And so I went out and tried to apply for some jobs. And that was when I got um hired.

Well, the funny thing was after after going through this, the first three companies to contact me about working

for them and running security, Huawei, Wei Work, and Bite Dance. I am dead serious. They would love to have me despite all this. Uh instead I chose to go uh work at a small startup called Cloudflare. Uh and Matthew Prince uh I think maybe speaks to this class.

Um Matthew did his due diligence. He talked to Travis who had been my CEO at and manager at Uber and a lot of other people and decided he would take a chance on me. So I went to So I went and worked at um Cloudflare starting in uh spring of 2018 and then 2018 was the midterm elections and 2016 was when President Trump was elected for the first time and then there was the midterm elections. Cloudflare got so much negative heat because I got doxed and this uh organization uh these group of organizations I'd never heard of went after me. Please don't go to that URL because you'll see the entire doxing of me because Google refused to take it down uh even though I submitted a takedown request. But uh I guess if you go there, you'll see uh I have six brothers and sisters. You can see all of their addresses. You can see my family's information. Uh there's a whole timeline. There's all kinds of information about my mom who worked for the CIA like the and and lots of other stuff that I didn't even know about myself. Um, and so like just me because of what I'd gone through before, I ended up inflicting this on Cloudflare.

And um, the thing I'll say about Cloudflare is that is a company that really cares about transparency. Um when I joined the company uh I had my first security incident and um I had been through a lot of other security incidents where we don't get to control the communication about the security incident on the security team. It's a cross functional thing. You're supposed to work with you know the communications team and the legal team. Legal says what can go out.

Communication team polishes it up. The CEO has to sign off. That's the way communications work in companies, right? So, at Cloudflare, I had my first security incident. I call Matthew, our CEO. It's a Friday night because security incidents only happen on Fridays. Um, so that your team has to work all weekend. Um, it's it's it's it's a science. It's been proven. Uh, and so on that Friday night, I call Matthew and I say, "We have a security incident." And he said, "Who's writing the blog post?"

And I always remember that. And I'm like, "What do you mean who's writing the blog post?" We we're bleeding here. I need to make sure we stop bleeding and make sure that our customers are safe. And he's like, "Who's writing the blog post?" I was like, "I'll figure that out later." And so I hang up. Five minutes later, who pops onto the Zoom but our CTO. I'm like, "John, why are you on this?" He's like, "I'm writing the blog post." like our CEO had made our CTO just join my incident response kind of working room just to write down and document everything so we could be transparent. A year later, we had our first big real outage as a company. I was over in London and it was our local team in London uh uh pushed a uh a rule to our W that basically took down half the internet. And fortunately, most of the United States was asleep because of of the timing of it. But John and I had to we called every large customer that we had. We put out a detailed uh blog report. We had literally disrupted the entire internet. And a day later, if you went online and you looked at how Cloudflare was being discussed, they were praising us for transparency.

Instead of break getting like slammed for breaking the internet, we were getting praised for being transparent

and I think there's this constant tension between transparency and not around technology what the good and bad of it and I think we need to bias more and more the way Cloudflare has towards this transparency. So after that what h uh it's tw now 2020 and uh the FBI issues this press statement saying that they have arrested me.

My eldest daughter uh was moving into her dorm at UT Austin at the time and she calls me because a friend of hers had heard on NPR that I had been arrested. And so she is freaking out and she calls me. I'm sitting at my desk here in Palo Alto. I live by Midtown in Palo Alto. I was sitting at my desk on a Zoom for Cloudflare. I hadn't been arrested. Um, so we have to add one thing to this.

Um, so uh for I hadn't been arrested, but what I had been uh was charged with a crime. So I've never been arrested, but I did get charged. I got charged with obstruction of justice and mis prison of a felony. Without going into all the details, what it basically means was I was being personally held responsible for the company's failure to be transparent with the government in 2017 or 16 when that security incident happened. Um, so I want to take you through the security incident a little bit.

I'm going to skip the legal stuff. I went to trial against the government in September of 2022. One of my daughters drew this picture because you're not allowed to take cameras in federal courts. Uh so this was during the trial. This was uh uh the person on the stand there was a lawyer from Uber. Coincidentally, when my daughter drew this picture, this is the chief privacy, the head of privacy and regulatory for legal. and she testified, "It's my team's job to tell the government about security incidents and and my team owns responsibility and my team was the one that uh and I personally knew about that security incident and yes, we did not tell uh the government agency that was investigating us about the security incident." So, she said all that, but I was the one who was the defendant sitting in the courtroom wearing a mask because it was COVID times. The jury never actually saw my face through the whole trial. they only saw a guy in a suit with a mask on. Um, so what what was the case actually about?

Uh, I really believe in this concept of responsible disclosure and trying to get the hacker community to work well with corporations. So when I in 2007 when I was at PayPal, we published a responsible disclosure policy. It was the first time a company published one. If you do security research, you know what this these policies are. or if you don't, you've probably never heard of them. But what we did, what we said in 2007 at PayPal was, "If you find a vulnerability, please tell us about it.

We promise we won't sue you. We promise we won't tell law enforcement about you. We want to have an open dialogue." So, we did that in 2007 at PayPal and other companies started to follow suit. I uh went to Facebook in 2008 and we published a responsible disclosure policy there. right after I got there because it was something that I cared about. Then a couple of years later, there was this movement in the hacker community that was like, "Wait, that was nice that you said you won't prosecute us, but why don't you actually pay us money cuz you're you're finding vulnerabil we're finding vulnerabilities. We're making you safer." And I remember the first time I got that email from a hacker and it said, "Pay us money and we'll tell you about the vulnerability in your systems." And if you own the system and you own security for that system and you get that message, you get kind of mad.

And I used to be a prosecutor. So I was like, I'm this I get double mad. Uh and I start thinking, how can I use the law against you, right? It's like and then and then my team's like, Joe, shut up. Like we should be paying these people and I came around to that. And so I think it was 2011 10 or 2011 at Facebook, we launched the third ever bug bounty program. Like bug bounty programs are a thing everywhere now. Google last year paid out I don't know how many millions of dollars in bug bounties and they just announced a new uh program where you can get $250,000 for a single vulnerability.

And so like the world has been evolving to this place where we recognize that our goal should be the best possible security uh and that we should cultivate these relationships. So when I got to Uber in 2015, we published the responsible disclosure policy. Uh and I should add that when I went from Facebook to Uber, about 40 of my team came with me. And so we brought not just me I I went not by myself, but over the course of a few months, a lot of my team so much so that uh the general counsel from uh Meta sent me that warning letter that you sometimes get. Um, and then, uh, we published a bug bounty program.

Uh, and, uh, we had it running in private for like a year before we launched it publicly in the spring of 2020, 2016. And in the fall of 2016, this is the email I got. I found a major vulnerability. I was able to dump database and other things. And I did what I always do when I get this email because I've gotten a lot of this email over the years. I forwarded it to the product security team that manages the bug bounty. Member of our security team emailed and said, "Hey, we've we use Hacker 1 for our bug bounty program. Uh, but we're also happy to work with you even if you do it otherwise." This is an email from Rob Fletcher who's now a startup founder somewhere. Uh but he uh he he led the interaction with this person who wanted to be anonymous and they showed us that they had actually found a vulnerability in the way our AWS was configured related to some old databases that we like my team didn't even know existed because they had been deprecated before we got there. Um we treated it like a security incident.

We documented everything. We had a centralized tracker uh and all my team's notes are still there from it. Uh because I was going to trial over this. These are all slides from the trial actually from like my lawyer's closing argument was showing like here are all the people in the company who knew. I went to the CEO. He signed off on us paying the bug bounty because we paid $100,000 to these researchers. It was all approved. Legal was three lawyers were in the loop. communicate our two lawyers, the communications team, all in the loop. Um, and we actually had written formal policies and documentation and it said legal is responsible doing the investigation, reporting it, etc.

And we ran the whole thing by legal and they said, uh, we don't think we have to disclose it. The communications team had already prepared documents for if they were going to disclose it. They put those aside. Uh, I said to my team, "The these people are still anonymous. Can we find out who they are and actually go interview them and make sure that they have deleted the data?" So, my team did an investigation. I'm not going to go through all the details here, but long story short, we were able to figure out who they were and where they were.

Um it turns out at the exact same time that we were doing this investigation, the FBI was also doing the same

investigation because uh these two guys uh 19 and 20-year-old 19-year-old down in Florida and 20-year-old up by Toronto who had met in gaming community where they had found vulnerabilities in a few companies of the same type. And so they reached out to a few companies. I think they reached out to five companies and said we found vulnerabilities. We worked with them, paid them, fixed the vulnerabilities.

Another one of the companies, which was uh LinkedIn, decided to contact the FBI. The FBI then tried to find them. We didn't know any of this was going on at the time. The FBI couldn't find them. my team was able to um and uh my my team and I still get involved in working with the government on situations like that um because we're really good at that stuff. And so uh we were able to find these guys and um I had a retired CIA uh intelligence officer who's specially trained in interrogation, a top trainer from he trains other people from the CIA on how to do interrogation. So, I sent him down to interview uh Brandon. Well, actually Matt from my team sent this email. We basically figured out who Brandon was, where he was work living uh down in um Florida.

And we sent him an email and said, "You got to be really careful in these situations. You'll be viewed as an extortionist. We don't think you're an extortionist. We think that you should be paid." And uh by the way, one of my team Oh, he didn't know we knew his name was Brandon when we sent him this email. So, this was kind of like we send you the email and we send it to his real email address instead of his proton mail. So, you imagine you're Brandon, you wake up that day and there's an email saying, "Hi, Brandon.

This is this is Matt from Uber." Uh, and one of my team members is right around the corner. Can you guys meet today? Um, that that happened. And then my team member, the trained CIA interrogator, went in and he prepared for me, I think it was like a six-page psychological profile of the guy and documented and validated uh that the data was deleted, that our customers were protected. So this is a situation where at the end of the day, legal had signed off on uh the communication side and my team had done the work where I felt comfortable, our customers were protected and we closed the chapter on the case um until 2020 when I got charged with the crime.

I didn't know until much later that apparently, you know, people were agitating behind the scenes from Uber and others to to to get the government to go dig into this. So, I go to trial. Uh, we come through the trial. My lawyers at the end of the evidence say at the end of the government's case, they said, "Joe, we don't even need to put on a defense. We totally won." I was like, "Okay, sounds good, but like, let's just call a couple witnesses to fill in these little gaps." We did. So, we barely put on a defense. And then the jury goes out and they deliberate for a few days and I'm just like, "Guys, if if it was such an easy slam dunk victory for us, what's going on?" And then this question comes out uh with regard to this uh hacking statute, does Uber have the right to extend authorization after the access?

So uh under 18 USC 1030, there's this is basically the computer hacking statute. It says like, "So if I access your computer without your permission, I violated the law." And then there's various levels of significance beyond that point. And so the legal question was when Brandon and the other guy accessed Uber's AWS, could we after the fact give them a permission or was it automatically a crime the second that they accessed our computer? And

do we have the ability to unwind it? All the advice I'd ever gotten, and we discussed this a million times before with lawyers, is it's like the they would say, "Oh, it's like the old trespass statutes. You know, if somebody steps into your front yard and you can be like, "Oh, hey, come on in."

That kind of effectively by law means it's no longer a trespass. And so that was the advice that like the bug bounty platforms and our lawyers had always told us. But then when the jury asked this question, the judge was not so sure. And the government was arguing at that time, no, we can't uh Uber couldn't give permission. So the jury basically got this instruction, Uber cannot give uh permission. So effectively, it just basically gutted our whole defense. Um, and so I could be held accountable uh for a criminal uh obstruction supporting the bad guys even if I had gotten legal approval and didn't think that we did anything wrong.

So, we lose the trial. Uh, it's now October of 2022. I went through that period in 2018 where I had to climb back on my feet. And in 2022, it was a lot harder because I had just lost a trial. So like I called all these different nonprofit cuz I I was s sitting around at home open again and I called all the different nonprofits who always wanted to work with me and they were like uh yeah, we can't be associated with you this time. And so I um I I had been helping Ukraine through my role at Cloudflare and I realized that the only people who were willing to work with me in the fall of 2022 were the Ukrainians uh because they had nothing to lose and they didn't care about my case. Uh so I joined uh a nonprofit called Ukraine Friends and uh became their CEO. Uh I started a program called Digital Wings. I realize that at every tech company, we have these piles of laptop computers that are sitting behind the help desk because, you know, we hire a bunch of people.

Half of them don't last two years, but we're not going to give those computers to the next new employee. So, the piles of computers get bigger and bigger. On my first trip to Ukraine, a friend of mine was the CISO of Robin Hood at the time. He gave me 20 of their uh uh cleaned up uh used computers, and so I brought them in my carry-on. You know when you get to the airport and they're like, "Do you have any lithium-ion batteries?" I'm like, "Yeah, I got 20.

Uh, they didn't know what to do. They just let me on the plane." Uh, and since I'd already been convicted of a crime, uh, I was like, "Anyway, um, I'm just kidding. I actually I really take seriously the shipping. Uh uh I've shipped thousands of computers to to Ukraine at this point and I've learned everything about safe shipping of lithium ion batteries and the like and it's it's really important you take those things seriously uh because there have actually been fires and things on planes. But public service announcement aside, um I got to Ukraine with a bunch of laptop computers and I realized uh what a need there was. So, my nonprofit, we get kids uh we bring computers to kids who've lost a parent in the war. My last trip to Ukraine was two weeks ago.

I was there two weeks ago for the week. Uh uh TD Bank had donated over a thousand computers and so I was there to kind of like oversee the distribution of those. Uh and uh we work directly with military units so that some of the soldiers in the unit can give the laptops to the kids of their fallen brothers. uh you know the the people who survive feel like almost a sense of responsibility for the families of of of of those who didn't survive and so we like to work with them to help them. Uh and uh you know what the people in Ukraine have been going through. It's incredible their resilience. I I come back inspired every time I go. I've been six times in the

last three years and I I wish I could go more frequently. Um, so I'm doing this work in Ukraine and I'm waiting and my sentencing keeps getting postponed. I had the most amazing thing happen.

I'm in like this funk. No one will hire me. I'm volunteering in Ukraine, seeing sad stuff, and I'm waiting for my sentencing hearing. And the government says, "We're going to argue that you should get three years in p in federal prison." Uh, I guess I'd still be in federal prison if if they had gotten that. Um there's a process that you go through though for uh before you get sentenced. Uh and that in the federal system is there's somebody called there's a probation office and they prepare a pre-sentence report where they kind of review your whole life. And so it's like it's like a 75page document of everything about me so that the judge can make an informed decision.

And by the time the probation office got through documenting like that Joe's been a volunteer for the federal government 17 different times since he left the government doing all these different things like um and involved in these different nonprofits and helping people in Ukraine etc. The probation office came in with a recommendation to the judge. You should just give Joe probation and let him go live his life. And the prosecutors when they heard that they dropped down and instead they argued that I should get 18 months. But so during that process um I had the most amazing thing happen which was I got these emails and attached to each email would be a letter to the judge. I got over 200 separate letters to the judge sent to me by people who'd worked with me through my career uh by people who were upset about my case. One letter was signed by 60 people in the cyber sec security community, another by 50, another by 40.

It was like this mass uprising of support because they felt that the case was unfair or even if they they didn't know anything about the legal stuff, they they they wanted me to be out and and doing what I do. And so I had a sentencing hearing on May 4th, 2023. So literally 3 years ago and a couple weeks a week. Um, and the judge said it wasn't a cover up. That was the best thing I ever could have heard. Uh, the judge then went on to, you know, basically yell at the prosecutor in some sense, saying, "Why why if you're charging a company, why wouldn't you charge the CEO?" The CEO was in the loop. Uh, CEO supported all the decisions. If we're going to hold corporations accountable, let's start at the top. Uh he uh also yelled at the prosecutor like there was no financial incentive for Joe to do this. Why why do why do you think he would do this? Do you think he needed to protect himself for his career? Stuff like that. He just said, "I've never seen a case like this in my life." And then he sentenced me to three years of probation and a small fine and sent me on my way. So I actually finished my probation a week ago. I got a letter saying I'm off probation. Um, thank you.

I still get secondary inspection every time I come to the country. But, uh, my daughters really enjoyed it. The first time they're like, "Dad, this is so cool." Uh, but yeah, so I I landed on my feet. I started my security consulting business. I still do the nonprofit stuff. I've been working with some VCs. Costanoa made me a venture partner. I've been advising a bunch of C startups. Uh, this slide's actually outdated because well, four of four of these companies have recently gotten acquired and so I no longer advise them.

Um, but I was happy they got acquired. Um, I get to go do keynotes. I I got I get paid to speak all over the world. I this year I keynote at a big AI conference in January in uh Tokyo. This was a very a keynote in Australia. Um,

and so I get invited and and paid to go do these things that I love to do and talk about uh things like this case and and and I just want to like spend like five more minutes on like the cyber security and the world of cyber security has changed so much since I got involved. When when that Uber case happened in 2016, it was like the worst case scenario. Data had left the building. Like in cyber security, that's all we cared about for the longest time.

And then something new happened around 2018 and 19 which is ransomware. So now in 2025 2026 cyber security is still we care about data leaving the building but we also have to care about operational resilience. Does anybody know what happened to Jaguar Land Rover last year? They got hit with probably one of the biggest cyber attacks. It was a ransomware attack and last I I think it happened last August. They literally had to shut down all of production for all of Jaguar Land Rover for three months.

The UK government had to do a bailout of over a billion dollars. A bunch of their supply chain companies. So, you know, a Jaguar is not just all the parts made by Jaguar. They're made by hundreds of little companies. When Jaguar couldn't pay pay them for three months, a lot of those companies went out of business. So like the impact of a cyber attack cost the UK economy literally billions of dollars, billions of pounds and anybody who owned a Jaguar Land Rover during those months couldn't even take their car into a mechanic shop.

So that happened. Uh cyber security became about operational resilience and then also you know what's going on with AI. Uh I I just got back from spending the last three days in meetings in Washington DC uh because I do some volunteer support uh for a couple of government agencies now and um you be like it's weird I'm under I'm I'm on probation and under investigation by one part of the government but I usually am helping a different at the same time. I I have had these conversations where it'd be like in the morning I'm with the FBI talking about something and in the afternoon I'm with the FBI talking about them putting me in jail. It's been it's been pretty surreal. Um but so I was there earlier this week and the amount of pressure the government is feeling right now about AI. You know, I I work with some companies that have access to methos, the the cyber model from or the cyber used model from Enthropic. That's so powerful. And it it it is it is as powerful as everybody says. Like we're finding things uh that are amazing uh and scary. And so the government knows that and really needs cyber security to step up in the next six months because those ma that type of model that's being held close right now is going to be publicly available in six months even if it comes from the open source guys. So that's the future we're facing. All of a sudden every CEO really cares about cyber security. I get a call a day Joe this CEO needs a head of security right now. They need somebody who's like has the experience you have where you could you're comfortable reporting to a CEO, sitting in the exec room, co-running a company. That's the kind of people we need in cyber security right now. And I I don't even have enough people to to refer. At the same time, governments are tightening up on the regulatory side. A lot of other countries are thinking about doing enforcement actions like the ones against me.

So, it's this weird situation where a lot of my peers call me like I hear from every CISO in every bad situation and I also hear from, you know, like they call me when they're like, "Joe, my we just had a ransomware and the CEO is forcing me to sign something to go to all our customers saying that everything's fine and I know everything's not fine. What do I do?" Like, I get questions like that every week from people in the role.

And then the other question they get is like, I'm being asked to take the top seat. do I even want it? Uh because it's really scary to be a cyber security leader in this environment right now. And the thing I'll say is I've been through a lot and one of the things I've realized is that you have to have resilience. And I don't care if you're going into cyber security or what other jobs you all decide to go into, you're going to get punched in the face sometimes. And you got to think about how am I going to handle getting punched in the face. Like you when a boxer goes into the ring, they know they're going to get punched in the face and they think they still have a plan. I think leadership in 2026 and beyond is about that resilience. I these four people like ever since I went through my thing and I've had people say like, "Oh, you're a model of resilience." I started looking. There are a lot of really good models. Like these four people all got punched in the face when they thought they were at the peak of their career and they thought they were at an amazing place and then they end up going 10 times higher in their career and you can find so many people like that. And so the thing I would talk you know I do a lot of work with organizational leaders and I you know I I did like a 4hour how do I prepare for I have like a literally a 4hour program on how do you as an executive prepare yourself your team and your company to deal with crisis before it happens. I'm not going to go into all that stuff with you, but I want you to think about and remember that we don't write into the job description resilience and crisis management. But if you're working in technology in 2026, we're so highly visible, there's so much pressure on us, we have to be ready to get punched in the face. And that means thinking about what are the key elements for success in a crisis. I think the number one element for success in a crisis is actually how well you communicate. Like I I brought up how Cloudflare has handled crisis over the years. They always are on the side of transparency and it always builds trust.

Uh companies that choose like say Uber in 2016 not to be transparent, it leads to this boiling negativity over time. So my last thought for you is this. Run towards those opportunities. Run towards those stressful situations because the more you go through them, the better you'll handle them. I get invited to work at companies, the coolest companies on the planet, because they have confidence that I have wisdom from having gone through the bad things.

If you try and steer your career to never go through bad things, you'll never get the wisdom and experience you need to really succeed. >> So the question is, how did you rebuild your your reputation, which is clearly, you know, world world known? >> Yeah, I um it was interesting. So I I I consider like I consider I lost the trial in the fall of 2022, but I won the sentencing in the spring of 2023. And it was really um my wife who's here in the front row who's a Stanford grad, she came along today. Um she was there with me through it all and having having strong support at home number one. Um was really important. But then I had a lot of support from the community. I got I mentioned those letters. Uh I joke that it was like uh I got to sit through my own Irish wake. you know, the idea that like um I got to hear all these people say good things about me while I was still alive. And I I bring it up a lot with leaders because what you don't realize when you're a leader is how much the little things you do or don't do um your team picks up on. Like I had people write in these letters to the judge talking about things that I I didn't remember at all. It's like I didn't remember. I had lunch with that guy in my team's kid who was thinking about cyber security, but apparently I did. You know, I didn't remember like there were just lots of examples like that. And so, um, so after I won the trial, I reached out to a couple of people. I decided I should I couldn't talk for seven years. My lawyers wouldn't let me talk. So, I was just all negative for seven years. And so after it was over, I reached out and um I reached out to the guy who runs the Defcon conference uh who started it in Vegas back whatever 30 years ago and he'd started Black Hat as well. So they're two of the most

well-known cyber security conferences and I said I'd love to get a chance to tell my side of the story and I um and he he contacted me back a week later and he said at Black Hat we have a CISO summit so like all the security leaders from the biggest companies will be there. uh you can do an off thereord talk there if you'll do an on thereord talk at defcon.

And so those were the first two times I was talking about my case. It's funny my dad emailed me the other day cuz he found the defcon talk and watched it uh three years later and um and he emailed me about it and I was just reflecting on I was so nervous. I was so nervous because a friend of mine I went who lives here in Palo Alto. He'd been on the early Facebook team with me. I went walking with him and he'd said, "What are you going to do if you get booed?"

And so I mentally going into the speaking was worried that I was going to get booed. Uh but I just did it. I got up and went and did it. It was the same thing as like in January of 2018, the first time I went to a security conference after getting fired on Global News. I felt very sheepish and awkward and uncomfortable, but I got through it. When I spoke at Black Hat at that CISO summit, I got ended up getting a standing ovation from like my peers, the best security leaders in the world. And so that just gave me the confidence and courage to to go forward. Uh I started my own consulting business and then I had success doing it. It was mostly what I've learned is that I was mostly able like large companies can't be associated with a felon. Um although I do work with some large companies but they prefer that we keep it under NDA. Um and so I started embracing working with startups even more because startups don't care. They just want to have the best security they can get from somebody who understands them. So I just I just been building it ever since.

>> Good. Next question. >> So the question is what are the security issues around Vive coding and what should we be thinking about? >> Yeah. I actually joined the board of an appseac company uh last fall and and with at over at the VC we've been looking a lot at how application security is evolving and I've been thinking about and the uh the companies that I advise and work with are obviously in different stages of of um embracing it. Financial services is really slow on embracing it, but some of the other companies I work with are really deep in uh like a large percentage of their code is being generated through um these tools. U the the first challenge is just the sheer volume of code being generated uh has gone through the roof. Uh like one small southeast bank that uh we work with uh they went from like 250,000 lines of code a month to like 1.25 to five million lines of code a month in in like a two-month period after get uh so challenge number one is the sheer velocity of u of code. Challenge number two is that uh one of the other companies I work with here in the Bay Area they're um their CISO called me and he was like we just had our the first marketing person merge into production and there was a vulnerability and we tried to kick it back to marketing and they don't know how to fix the vulnerability. So like you know whereas an a software engineer would actually like okay here you know security could send them a proposed fix and then they would typ the typical appsac model is the security sends a proposed fix and then the the engineer actually looks at it and thinks about the bigger context but it's somebody from marketing you can't really do that. Um so that's the second challenge. Um the third challenge is um it's not just a vibe coding but like cloud co-work for example is I mean which is really claude code with a rapper um co-work uh it's getting non-technical employees to be even more ambitious with connecting externally and the way that they'll solve problems is if they don't have the API key they'll go out and try and you know literally they'll go try and set up their own remote external server so and create their own API key and you're like there's No way an

engineer would do this. So we're seeing all kinds of crazy things. There is no one silver bullet solution. I'd say companies are walk are coming at it from two different directions. Some companies are doing YOLO and then trying to clean up. But a lot of companies and smart companies in particular are are starting out with pilots and constraining to just software engineers who who know better and then are slowly adding um different groups. I really believe that we can't solve um we can't solve the headaches the security headaches of agents inside our environment just by putting guard rails on them because it's not you can't say okay you can have access you can have right access to my email for purpose A but not purpose B. It's like we just can't do that. And so we have to have um kind of like anomaly detection around. I think of it like um agents inside companies are like toddlers in inside a house. They're running around. They can run, but every so often they're going to, you know, if you ever seen a parent of todd toddlers, they're kind of running next to them. It's like real time runtime. Um and that's what I think we're have to get to in in um Agentic Solutions. It's like we'll put some guardrails, but it's not that they have access, it's what they do with the access that we have to pay attention to.

>> Interesting. So, so the question is what would you have done differently if you were back leading security at Uber? >> Yeah. So, from a technical operational side, my team, my team, I was so happy that we actually got to get to the trial so that the world could see what my team did technically. Um, I think everything we did I would do the same. I wish we had more documentation. I'm actually an adviser to a company now called Breach RX which uh creates a platform that forces legal and um communications to work more directly with security and I started working with them uh before they even got their seed investment because I really believe that it is about how you get the different teams inside the company to work together on transparency.

um like in the middle of a security incident, the security leader doesn't have the credibility around communication or legal issues to say we should be public about this. You have to work through that stuff ahead of time. So, operationally, I wouldn't change anything. We should be paying those researchers. Um we should be uh fixing things. We should be working with legal. Um I think I spend much more time now educating the other executives at the companies I work with Not just the security team. Like there's when you become a leader of a company, you don't actually work on your team anymore. You work on the leadership team of the company. When I mentor a security executive, I always start out with a question that's actually a trick question. The first time I'm meeting with someone new, I say, "Tell me about your team." And they immediately start talking about, "I got this team that does detection. I have this team that does application security. I have this."

I'm like, >> "No, no, I mean your team." They're like, "What do you mean?" I'm like the other executives at the company. >> When I was at Facebook, I had an exec coach and she told me that I should be spending 50% of my team with the other executives instead of with the security team. And I actually think for a security leader, it needs to be even more because our world is dark and scary and confusing. It's not very measurable by metrics and you only hear the bad stories. And so it's our job as security leaders to get out and really build trust with the other executives at the company. so that in the crisis moment they'll trust us more.

>> Yeah. >> The question is around quantum cryptography. >> I'll tell you that uh this comes up all the time like I was in Florida last week for a closed dooror group of like 20 security executives including from a bunch of the large um ga uh gas and energy world oil gas energy world. And we had a whole session talking about like what

are we doing about the quantum risk and opportunity. For the most part companies are not doing a lot right now. I think the reality is that we could you know if we look at how the pace of AI uh has like sped up from predictions uh quantum seems like it could be here by 2030. And so arguably we should be doing stuff but for the most part when you think about uh where cryptography exists in our environments I think that um most of the work that needs to be done needs to be done at the Googles the AWS um like the biggest risk probably to most of us right now is that um agencies of governments have vacuumed up a lot of historical communication data that was been encrypted by non-quantum resistant uh encryption. And so if you're part of a terrorist group 5 years ago, you might have some trouble in 5 years. Uh that kind of stuff. Um like the quant uh most of our environments that are the main infrastructure companies supporting them are going to be quantum resistant. Um, and also if you flip it around, it's a little bit like the Mythos situation.

Once we get quantum, it's not like going to be like all of a sudden every data center is a quantum data center. Quantum machines require extreme cold and all this other stuff. So, it's going to be like a few people have quantum before everybody has quantum. And then there's going to be a period of time >> uh and so hopefully it'll be the good guys get quantum before the bad guys. And then they can do kind of what Andropic and Open AAI have been doing with their new cyber models.

>> Actually, just I have a question on those models like with the mythos like what is your opinion on how those tools should be released early and and kind of like what what's the right kind of process there do you think? >> I I have seen it's funny the cyber security community is very critical self-critical and and loves to jump all over each other. So like the first I I think on a mainstream level, Anthropic did an amazing job from a brand standpoint around you know they're coming out of this fight with the deal department of war and then all of a sudden they're just like being noble and helping the world around cyber security.

They nailed that >> um from like communication standpoint and then there was this little backlash in the security community of like >> I don't have access to the model. I don't believe it kind of thing and uh this is all hype and why haven't we seen a bunch of CVE submitted and documenting it. >> Um what I can tell you like I said uh one of the companies I work with uh was given access on day one and it's just been um incredibly valuable for them. Um when you get um but when you get when companies and organizations get access to these models it's not like they can just snap their fingers point the model at their infrastructure. you have to have built the harness and kind of like the uh the technology around the models.

So I think every company should be building those harnesses right now so that and and honestly you could take some of the other existing public models if you have the right harnesses you can find a lot of the same things if you're intentional about it. So um I don't think I I'm not critical of Antropic in the way they've done it. I will say that um they went public with the names of like eight companies >> and I think that there was some intentionality about that because they imagine you're in their shoes. If you decide to give the access to one gas company but not another >> or one bank but not another, you're it's almost like you're picking winners and losers.

>> And so they have to be very careful. They gave access to more than they said they gave access to. like I know

of organizations that have access I know multiple organizations that have access that are not on any of the lists that have been public. >> So do I. Yeah. >> So um so it's interesting they they're doing a very public part but they're doing some behind the scenes and then we do hear like some European leaders complaining we don't have access stuff like that but some of their peers in Europe actually do have access. And >> it's it's one of those things where maybe transparency would be better.

Maybe this and now I think the the the government is really uh this administration is now thinking a lot harder about how should we get involved in these? Do we want >> like what if next time it's not anthropic, it's somebody else. Um and they're not as intentional about the roll out. Um so >> out of curiosity, where do you sit on that regulatory kind of uh topic? Yeah, I've I mean I've I've spent 20 years being the face of companies like I've testified before Congress multiple times on these topics of like should we come regulate PayPal or Facebook because of um >> I think we need to have smart regulation. I'm not anti-regulation.

like a lot a lot of Silicon Valley companies and a lot of the companies I work with in general like the whole public policy team's job is to prevent any regulation at all because stupid regulation definitely gets in the way of innovation. Um, at a certain scale though, we need to have regulation to protect people cuz it's not in the best interest of companies that are just pure existing for money uh to take care of everybody who has access to their product.

>> And and a lot of products get used in a lot of ways that the companies don't anticipate. Uh like when I was at Facebook, I worked with a lot of um dissident groups in Africa in you know countries that had governments that were very oppressive and the only way they were able to stay in touch with each other was through Facebook and yet uh and they were using the product in ways that I never imagined that they would use it and it wasn't built for and it was putting them at risk and then they were like can you build some other features for us to reduce our risk but there's no economic incentive for us to do that as a company. Uh so you see these weird situations all the time where um governments can make like social media for kids.

>> Yeah. >> My daughter who's 23 now is like dad you should have regulated us way more. Um and so like there's no easy answer on it because a lot of the time government shows up and they don't even know how to turn on a computer and you're like how could I let these people regulate me? Uh, I mean the good news is, you know, like we have a lot of smart business people going ever since the second Obama administration when they had that um they really started promoting getting people from the private sector into DC.

This administration's doing it too. Like we we were talking about Emil Michael who's the person at the Department of War who's negotiating with Anthropic. There's no person I would rather have representing the Department of War in a negotiation with Anthropic than Emil. >> I agree. >> Yeah. >> Right. >> Yeah. >> Because he's like I worked with him here in Silicon Valley. He understands this world and he understands that world. >> Yeah. >> And and we need to have people in those roles like him.

>> We're going to have actually a meal for office hours later in June just as a as a future speaker. Next question. I think it yes it is very difficult for any company to put full security around everything they're doing. Um I I work

with a lot of um startups and the number one thing they're worried about is theft of intellectual property. Uh it's that's a big difference between the the companies I work with and a lot of other organizations. A lot of the world thinks about security. Intellectual property theft is a huge risk uh for a lot of different reasons in Silicon Valley companies. And so um you know can we fully vet every employee that we hire?

We cannot like we can't do the level of background check. We can't know if you have relatives back home in another country who are being held hostage by the government. I've I've had situations at companies I've worked at and with where we have known that the employee would was put under pressure when they went home and it was like hey you know your your parents have a nice retirement right now but you know we have this luxury suite in Siberia um that if you don't start showing some patriotism like that pressure happens all the time. I've had like um I've had employees uh arrested by governments overseas uh and held in expectation that the company would cooperate. Uh to the point you said about saying that he was worried his hand is cut off. There have been executives at cyber at crypto companies whose hands have been cut off. There are lots of these like well you think about like if you could get access to the the vault of of like one of those crypto banks. Uh, and a lot of times like the main keys are literally like two people's fingerprints have to be involved to be able to unlock it. Um, and so they'll collect the fingerprints.

Um, yeah. So I like I built executive protection programs in the physical security side and I've seen a huge ramp up in executives needing to be worried about that. I mean, we heard the story of what happened to Sam Alman recently. I um there are lots of stories like that that don't get as much attention. I could there I you know you could go back 20 years ago one of the co-founders of Adobe was kidnapped here in Silicon Valley and held hostage um like in the East Bay and the FBI went and rescued him like nobody I know that story because I was around then but most of the world like we've been dealing with this type of stuff for a while and it's real because our companies are the most powerful companies in the world in 2026 and and the technology is scary. So okay, that's the first part. We can't uh we can't do perfect security and there is a risk. I do still think that we should be moderating the release in the spirit of doing the best we can to manage the risk of the release and I think that's what an entropic and open AI have been doing. Um could we critique them? Is there could they do better? the more transparent they are about the releases, hopefully over time we'll figure out what are the like it would be nice if we could say here are the five best practices for rolling out the release of a model and like we we we will prevent these organizations and they will have signed the right agreements and stuff like that. Uh I think we're walking but not running in that direction and we'll get better and better at it over time. Um and governments are going to get more and more involved because they need to. Um what are the other question?

>> Open source >> and then open source I okay on on the open source point I don't think we I don't think there's I don't think anyone knows what the ideal or real world of what models are going to be the best models three years from now are like I don't know if LLMs are going to be the center of our universe like they feel they are right now. Where do world models fit in? Where do small language models fit in? Where where are vertical models? It's like there's so many different things going on in so many different startups around models. Um like are we going to get to a place where the models stop, you know, these large language models stop making leaps every few months? Are the leaps going to get a lot slower? Are the open source ones going to catch up? Um the economics don't make sense to keep going forever on these large language models.

So I I feel like it's going to be a couple of years before we um even know what like the steady state is enough to debate it. >> So So the questions around shiny hunters and the canvas and ransomware. >> Yeah. So uh it's interesting ransomware um like let's look at what's the history of ransomware. Ransomware actually started uh through state sponsored attacks. It wasn't for money. It was for political reasons. If you go back, the the the biggest early ransomware situations were not ransomware. They were destructive cyber attacks. Saudi Aramco was taken out by Iran. Uh the Sands Casino was taken out by Iran. Uh North Korea took out Sony. Uh that was actually my team at Facebook that uh showed that it was North Korea that had taken down uh Sony in 2012 or 13. And then uh we shared that with the FBI. Um and there were um and so it evolved uh from those attacks into private sector attacks. And right now there's literally so much uh infrastructure built around the business of ransomware. Like a lot of companies hire a ransomware negotiator to have them on retainer just in case they get ransomware.

I like the idea that there was actually a business profession of like I negotiate ransomware solutions. Um it's a thing in 2026. Um and it's a best practice to have one of them on speed dial. Um >> I think that it's uh we're in the bad state because government didn't do enough to react and understand the implications now that governments like the UK government are doing all these bailouts. Now that it's hit companies like healthcare companies in the United States. If you like the first time cyber security really impacted American citizens was the Colonial Pipeline one.

A whole bunch of the northeast of the United States. People were lining up and filling up their cars with gas and they block long lines because of a cyber ransomware attack. The government is finally in the last couple years realizing we got to get involved. We can't allow these like organized groups whether in Eastern Europe or in Asia or in the United States itself. Uh governments have to get involved. So law enforcement is starting to do a lot of takedowns and now some other branches of government are thinking about how can we go after those gangs. So how do we go after them before the attack rather than after? Like if you think about the FBI's role in cyber, they don't prevent cyber crime. They try and do arrests after the fact. And so we need more government involvement on the prevention side. It's just been hampered by the fact that, you know, when our government goes to meet with the leaders of the governments in these countries, we're often negotiating more about like the war in Ukraine or, you know, or Taiwan and the cyber stuff is not getting to the top. But because the economic because the CEOs are now so worried about ransomware, our government is starting to become more proactive and there are starting to be a lot more like if you pay attention the White House uh cyber in the last year he's talked about allowing companies and organizations to go on the offensive. Uh and that is really a scary thing but also an interesting thing because it's like >> like what's your plan when you get punched? you want to be able to punch back. And some people say, you know, the best way to win a fight is to punch first.

>> Uh that was a quote from one of my CEOs. I won't tell you which one. Um but like you you um you've got to uh be more proactive than just waiting until the ransomware starts to happen to you. >> Great. Thank you so much. Uh it's fantastic.