uberknowledge

Archis Gore, CTO, Polyverse

The CTO Determined to Solve Cybersecurity

Archis shares the story of his experience of Spectre and Meltdown and the lessons vendors could learn from it. He discusses the importance of compliance but suggests organizations go further than the minimum bar. Finally, Archis reassures the cyber industry that it won't become obsolete if it solves the cybersecurity challenge because there will always be more problems to solve.

03:25 Lessons from Spectre and Meltdown: The security role can be a very lonely one when bad things happen.

04:51 In a crisis, where are the vendors? Who is on the side of SecOps?

09:02 Business owners need to accept a cyber breach is inevitable and their security teams need to look for solutions that do more than just prevent.

10:44 Vendors must demonstrate customer empathy and build solutions that focus on the inevitable and varying bugs, breaches, and attacks.

12:24 Instead of focusing on compliance, organizations should take a proactive view of risk and impact. Then they will automatically become compliant because compliance is the minimum bar.

14:47 The concept of Demonstrable Trustworthiness - trust that must be earned in each transaction - is demonstrated by meeting expected behavior. AI and ML can never meet this.

15:57 Trust only happens when there is shared collateral.

17:22 Set minimum parameters for loss then build your system design around those.

18:17 VCs creating evermore cybersecurity unicorns is not solving our cybersecurity problems.

21:57 Solving, creating and innovating will not make cybersecurity obsolete. There are still billion-dollar problems out there. Maybe on Mars.

Ashwin Krishnan: [00:00:44] So, welcome to another episode of the UberKnowledge podcast. With me, I have Archis Gore, who is the CTO of a really interesting company called Polyverse. So Archis, why don't you introduce yourself to our listeners and talk a little bit about the "why" behind Polyverse.

Archis Gore: [00:01:03] Yeah. Thank you for having me on the podcast. I'm Archis and I'm CTO of Polyverse. The really quick version of Polyverse is to solve cybersecurity, and I will explain this in the easiest visual terms possible. If you think of any other industry, we used to have CFCs, now we don't have them. We used to have issues with horse manure. We don't have it today because we have cars.

Ashwin Krishnan: [00:01:32] [Laughs]

Archis Gore: [00:01:32] If we can have one cybersecurity problem that we can name that we used to have in 1985 ...

Ashwin Krishnan: [00:01:41] That we don't have today. Very interesting, yes.

Archis Gore: [00:01:45] That we don't have today, right. So as an industry, as a culture, as a society, cybersecurity does not move forward. It is additive. We had the same problems. We have those problems, and we now have new problems, but we don't solve them. We don't move forward and that's why Polyverse exists, in short.

> "Cybersecurity does not move forward. It is additive."

Ashwin Krishnan: [00:02:07] That's a great way of describing it because you're right. It never occurred to me even though I've been in the industry for so long. Everything is additive, right. We have newer threats, but the old ones never go away.

[00:02:23] So I want to actually bring back one of the conversations we had previously, that I think is emblematic of everything that is happening in the industry today. It's almost like a microcosm of something that you experienced personally. This was, I believe, in your previous job at Amazon. So why don't you talk about how you went from being fully compliant one day to completely non-compliant the next day, and then the challenges that you faced as an individual who had to kind of keep up with these various demands? Through that incident I think we can dig deeper into seeing what other challenges your fellow practitioners face, as well as how vendors can get a look inside a practitioner's world and then talk about how to approach solving a problem that really matters.

Archis Gore: [00:03:15] Yeah of course. What I'm actually going to do is instead of my previous job, which is now four years old, I'll talk about something from one year ago.

Ashwin Krishnan: [00:03:24] Okay.

Archis Gore: [00:03:25] I want to talk about December 31st, 2017. Everyone that I knew across the industry was compliant. They had done everything right. They had done their due diligence. They had spent all their money. They'd done everything correctly. They all woke up; we all woke up on January 1st, 2018 to Spectre and Meltdown. We went from what was secure software one day to, by definition, completely insecure software overnight without having changed anything, without having had agency. We didn't make it insecure; we just woke up to it being insecure. Now that's part one. I know a lot of times people think of us as making things insecure. We don't do anything. We just sit there and yes ... so we've done everything right and we get blamed. Right.

Ashwin Krishnan: [00:04:23] Archis, so let's just dig in a little bit deeper. So given that you were in that world on January 1st, 2018, what happens in an organization when something like this happens? Like you were saying, this is through no agency of yours, something external happened. One of the largest or the largest silicon manufacturer in the world comes up and says, "OK, mea culpa." How do typical organizations react to something like that?

Archis Gore: [00:04:51] Correct, and this is the more fun part. So, as we tell this story over the next two weeks, and I lived through this because a lot of my friends and customers went through this. So, the first reaction is as a security person or even as an ops person, what is the first phone call you get? "Hey, I heard all our machines are non-compliant. Why are you making them non-compliant?"

Ashwin Krishnan: [00:05:19] [Laughs]

Archis Gore: [00:05:21] You're sitting there, and you're trying to explain yourself and it doesn't matter, right. “Why are you doing this?” That is the kind of accusation you have to deal with. You have to take that crap right. So then, you go to the vendors. You know, the vendors are all ... everyone wants to talk about how their stuff could have stopped something, but no one wakes up back then and says, "Oh you're good, you're covered because you purchased us." So the vendors are leaving you out to dry, in a way. And then you have the software providers who still don't have patches. And now you get into this very, very interesting situation.

[00:06:00] And there's two of those. The first is why aren't you patched; why aren't you fixing this? We know it's a problem. Once you know it should be easy, right? And then your upstream, you know, whether it's Microsoft, Red Hat, the kernel, Linux, Intel, IBM, whatever, they're all unpatched. So you can't do anything, but you are unpatched, and it's your fault. And then you go to January 15th, and suddenly patches begin to come out. And then here's the other problem: you deploy the patches, which you have been bullied into doing, and then the patches bring down machines. Then you have to answer the second question which is, "Why did you run untested code, and why did you deploy patches without knowing what they do?" And you're like, who is on your side, who is on my side as the person who has to keep the site up, keep it secure? And that is a very small but very visual graphic situation that almost the entire industry went

> “The vendors are leaving you out to dry.”

through. And this happens almost on a weekly basis, but just because this was so big it became obvious.

Ashwin Krishnan: [00:07:17] Like I said, this is pretty much symptomatic of everything: vendor relationships, talking about what compliance means, and compliance is not equal to security, then there's the blame game.

[00:07:29] So let's talk about best practices and modeled behavior. Given that you have been both on the practitioner side and now you're on the vendor side, there's a certain level of 360 view or balance that you bring to the conversation. So in Archis's mind what should a practitioner be doing? And again, we really don't want to have another Spectre or Meltdown, but we will. We have to be cognizant of that.

[00:07:59] So how much goodwill, what sorts of behaviors does a CISO, chief privacy officer, or even an Ops person for that matter have to be putting in play knowing that, like you said, there's a very small group of people that will come in support of you? How do you make that a bigger group, so that, pardon my French, when the shit hits the fan, you have that support? So that's the first part of the question.

[00:08:22] The second part of the question is now from the vendor's perspective. You mentioned that vendors left them high and dry. What should a vendor's approach be? Let's say you're a vendor, and you have been exposed to a Spectre and Meltdown. You're still working through the diagnosis. You don't have a patch. Yet, you want to engage with somebody like Archis on the other side, on the customer side to let them know that you have their back, and you will be protective of them. So, I'm just trying to figure out, given this sort of thing has happened in the past and will happen again, what is the best behavior to be emulated?

Archis Gore: [00:09:02] I think there are three layers here that we need to really think about. You almost answered your own question, and I will loop back to that. So as business owners, in everything else we plan for what happens when, not if. When a bug comes out, you plan for it. Given that this will be in an accident, you have a chassis that's going to take and absorb impact. Given that the glass is going to break, you design the glass in such a way that it does not create sharp shards. Given that, you're going to have blah, blah, blah. Right. So businesses, in terms of cybersecurity, the business owners need to accept this phrase, "Given that." It's going to happen. Secondly, CISOs need to then look for solutions that not only prevent ... You know, you can only live in fear so long. Right? It's akin to living in a literal bubble or never leaving your house because something might happen. If you think of it from an insurance perspective, given that this is going to happen, how do my systems

> "Given that the glass is going to break, you design the glass in such a way it does not create sharp shards."

respond; how do I degrade; do I degrade gracefully? And there is a lesson from Equifax. When a hack didn't happen, everything was great. When it happened, all their records were lost — not some records, not a few records. And so we went from 100 percent not lost to 100 percent gone.

Ashwin Krishnan: [00:10:43] Yep.

Archis Gore: [00:10:44] And so vendors can then play their role in building solutions that focus on "Given that" and then the second part of it is customer empathy. Put yourself in the customer's shoes and actually call them proactively as opposed to being theoretical. If Intel had made one phone call and said, "Hey, you know we get this, we understand this, this is the impact. We're with you every step of the way."

Ashwin Krishnan: [00:11:20] Yeah. And as you mentioned, in fact quite the opposite happened. I remember that the then CFO or CEO went on record saying this doesn't impact, it's very minimal. So it's almost like the lawyers and the litigators are the ones that are given voice to say how do we minimize the shareholder impact or the shareholder value etc. Versus doing the right thing.

[00:11:42] So is there another consideration here? I know we talked briefly about compliance, and you've lived through both sides of the house. It's a bad word in most connotations because it means budget, it means distractions, and so forth. How have you seen compliance evolve over the years, and is it finally starting to make an impact in terms of it's not just checking the box anymore, it has higher value? And if so, have you seen progressive organizations take a much more proactive stance to compliance than just the check-the-box once-a-year audit?

Archis Gore: [00:12:24] I think, yes and no. I don't think compliance will ever be better. And that's because, by definition, compliance is your minimum bar. So it's not that you shouldn't be compliant, you should always be compliant. What happens is compliance is almost rhetorical always. right. It's always backward looking. If you know what a seatbelt is, you go back 100 years and you just know how obviously stupid these people are because they don't have seatbelts. But if you had come up from horse and buggies into an automobile, it's not as obvious. And so I think the right way to think about it is insurance. How can I insure a certain degree of loss? How can I insure what valuations? And that's a very uncomfortable conversation. You'll notice that the insurance industry doesn't actually have compliance as much as they have models for what the impacts will be. And that informs how they insure you.

"Compliance is your minimum bar."

Ashwin Krishnan: [00:13:41] Got it. So in your mind, if organizations take a proactive view of risk and impact, they, by definition, will become compliant because that's a much lower bar.

Archis Gore: [00:13:53] Correct.

[00:13:54] So switching gears a little bit, again this is something you and I talked about some time back, this phrase called demonstrable trustworthiness.

Archis Gore: [00:14:04] Mm hmm.

Ashwin Krishnan: [00:14:06] And again, this is an interesting phrase, I haven't ever seen those two words juxtaposed in that fashion. We hear things like zero trust, and we hear things like two-factor authentication, but what you talk about is a little bit different. And the demonstrable trustworthiness that you talk about, it's in context, which means I can trust Archis today, but if something changes in your behavior tomorrow then you have to re-establish your trustworthiness with me. So, talk a little bit about how this evolves. Are the tools and the solutions keeping up with this?

Archis Gore: [00:14:47] Correct. So I think we're teasing that slowly in terms of behavior analysis, all the analytics that's happening, but we're still not fully there. And so first of all, I look at everything as a Turing test. There are things that I can control, which is basically just me, and everything else I cannot control. And so, what I do is I put everything around me in a risk bubble, and I call it a side-effect bubble. Anyone from functional programming will absolutely relate to this. If I call a certain function, what it does doesn't matter, the traditional way of doing security or introspection is to nitpick, is to drill down, is to be clever. Right? I hate all those words. Now, what I actually focus on is what should it ever, ever, ever in the wildest dreams have to touch or get to do? So my laptop should never be allowed to log into your laptop, just never. Right. That is a hard rule. There is no scenario.

[00:15:57] So by putting systems and situations in that bubble, you create these sandboxes, and then you know whether the behavior matches those sandboxes. And the minute it doesn't, I don't lose trust — basically there is no trust to start with. It is demonstrated by meeting the behavior that I expect. And AI and ML get it wrong because they study the behavior of a system that has already been built. It doesn't help. You have to start by saying, what can this ever, ever in my wildest dreams be able to do and then constrain it. And then when it breaks, go ask it why or just shut it off. And so that's part one. The other part is trust only happens when there is shared collateral. Like in bitcoin. It works because I have some bitcoin that I want protected and you have bitcoin that you want protected. So it's in our interests to protect the network. Right? But it doesn't work when there is an asymmetry of collateral.

Ashwin Krishnan: [00:16:51] Got it. Now the thing that you mentioned about the baseline behavior and trying to mimic that. A lot of it is also because people want a fast start or they have built so many data sets over many, many years, let's give the AI model a jumpstart. And what you are suggesting is something different, which is always going back to the drawing board and redefining what it is that you want to have happen and not happen and use that as a baseline. Correct?

Archis Gore: [00:17:22] Correct. You define the side effects. And so, if you start by saying when I get hacked, I must not lose more than 10 records at a time, then your system design is fundamentally different. You're not talking antivirus and scanning AI and ML, you're talking systemic design. We say that this building must withstand an earthquake of four point six and above. Right? And then we build it to withstand it, then we don't go back. Now we might test it, but we start with that ask.

Ashwin Krishnan: [00:18:00] Now that's a great point in terms of just, like you said, defining what is not acceptable, and then defining the sand bubbles, and defining the acceptable behavior, and making sure that everything stays within that.

[00:18:17] So finally I want to come back to something you talked about earlier, which I want to hear your thoughts on. We talked about the nature of the cybersecurity industry which is additive in nature. RSA 2019, we just finished up 10 days ago with the largest ever attendance, both in terms of exhibitors as well as attendees, is just more indicative of the fact that there's a ton more venture capital funding, as well as IT and OT industries grabbing after cybersecurity. In your opinion, have you seen a sense of it is no longer acceptable putting more and more products and solutions out there, and this long tail continues to plague us as newer threat vectors challenge us?

[00:19:17] So I mean, is it only Archis talking about this, or have you seen more industry leaders really embrace the fact that we need to think differently and just creating more startups with billion-dollar valuations isn't going to cut it?

Archis Gore: [00:19:33] Yeah. It's not as much as I would like to see, but it's not zero. You know people are beginning to latch on to that idea over time. I think the big cloud vendors get it the soonest because they cannot fail. And so, for Amazon it doesn't matter whether it's their fault or not, it matters that their customers are affected or not. So they, for instance, use this formal verification thing internally called DLA+. They study their systems, and they use a lot of very old-school control theory, old-school reliability analysis, and they go back to basics. I'm pretty sure Azure, Google, they all have that.

[00:20:27] When it comes to enterprises, I think we are at that ... Let me put it this way. We know that a lot of people acknowledge that it's a problem. But I don't think we've gotten to the part where we can actually take a collective deep breath and just say the solution is simple, if we accept that this is a problem, and what we're doing isn't working. I think there's two camps right now. One camp is doubling down, and it's almost like, you know, all that's wrong is that we aren't throwing enough money. So maybe instead of a billion, we need to throw five billion. Right? And then there are some split-offs which are basically saying maybe this can be done for ten thousand dollars.

"The solution is simple, if we accept that this is a problem, and what we're doing isn't working."

Ashwin Krishnan: [00:21:17] Yeah and it's very interesting you mention that because one of my podcasts at RSA was exactly that. There is a reverse or inverse economic incentive, or disincentive depending how you look at it, for cybersecurity vendors to not continue doing what they're doing. Because like you said, if it's ten thousand dollars, then how am I going to make money and make my shareholders happy?

[00:21:33] It's been a great conversation. So, any final parting words? I know we talked briefly about Polyverse, but maybe you can just shed some light on how your journey has been and where you think the company is going.

Archis Gore: [00:21:57] So here's an uplifting note for vendors. I think even in the computing industry, as much as we like to talk about coal miners becoming irrelevant, a lot of people in our industry fear if we move, if we solve, if we progress, then we become irrelevant. Here's my parting thought. In 2015 when I was trying to hire someone in Amazon, they asked me if my team had enough problems, enough sexy problems ...

Ashwin Krishnan: [00:22:34] [Laughs]

Archis Gore: [00:22:34] I started writing down a problem as fast as I could write, and I told him if he wants to take up the entire hour that's fine; I will keep on writing a problem as long as he doesn't ask me to stop. I had a backlog of two hundred years. Now, I have a backlog of about 50 years. If there is one guarantee I can give you, it's we're not running out of problems. If we solve this for ten thousand dollars, there are still billion-dollar problems. How do we secure space access software? How do we secure Martian software when we establish that Mars base? There is a lot of opportunity that we're giving up in protecting some compliance spreadsheet today. And so that's my hopeful, uplifting part is we're destined for the stars. We should be on warp drive securing computers of galaxy starships.

Ashwin Krishnan: [00:23:31] I don't think we can we can top that! Martians and space and space x as your parting thought. So again, thank you for your time, Archis. Always a pleasure speaking to you.

Archis Gore: [00:23:43] Yeah, same here. Thank you.

Ashwin Krishnan: [00:23:44] Thank you.