uberknowledge

Paul Vixie, Farsight Security

Six questions, vendor honesty, and the role of the CISO

Ashwin: [00:00:01] So, with me this morning is Internet Hall of Famer, Dr. Paul Vixie. Paul, one of the things that you had written about on LinkedIn that I found really fascinating was the six questions that would make engagement go a lot higher within an organization. So, if you can talk a little bit about the six questions and see if there's a resonance over there to try to bridge the divide between the vendor's side and the customer's side.

Paul Vixie: [00:00:33] Sure. I'm not going to enumerate the six questions, anybody who wants to do that can look it up. What I will say is that it came out of my observation that in personal relationships, in fact in my marriage, we ended up with two people doing the best they could to make a life together and eventually giving up on trying to get the other person to, I don't know, leave the toilet seat down or whatever, and just saying all I'm going to do is add stress if I keep doing that, so I'm going to let that ride. The problem is if you let that stuff ride it has a carrying cost, and so that was my insight into realizing that that was also happening at work. An employee who does not want to change or a manager who does not feel the need to change will end up in these kind of stand offs. Where yes, we're both going to come to work because we're both professionals; we both like our paychecks. There's a lot we're not talking about. And you know, when that builds up to a certain point then somebody leaves or there's just some other blow up.

So, I was looking for a way out of that, a way out of the destructive pattern. Get out of the holding pattern and into a real relationship where you're indicating to the other party: I'm ready to hear what you're ready to say. Let's see if we can

ratchet up both. So, the six questions are really three questions but with symmetry. So, they are repeated mirror image, and they work, they absolutely work. They work in my marriage, or at least they make things better in my marriage, and they work in a professional context.

Ashwin: [00:02:16] If you were to just take those six questions, and for the benefit of the listeners they are: what do I need to know; what do I need to start doing; what do I need to stop doing? Is that something that you think vendors could take to customers and use to really ask the questions? Because I haven't seen that kind of dialogue happen. Being on the vendor side, we would typically go in there with an agenda and tell you how broken you are, how great my road map is, and how sucky the competition is. That used to be the agenda. So, do you even think that this would be something worthy of a shot?

Paul Vixie: [00:02:55] I think it's worthy of a shot, but it's only going to be effective in a minority of situations. The reason for that is the interests are not aligned between a vendor and a customer. One of them is trying to get something done. The other one is trying to make quarterly numbers. We sometimes, and this is rare, and I make it as rare as I can, we sometimes hear from somebody, "We're not going to renew because we never figured out how to use what we bought and paid for a subscription to." And I hate that, it's like, "You could've just called us," and then I realized, wait we should have been calling you. So, if you have a situation where a customer is not as happy as they could be, the customer may not even realize it, you have to go fishing for this stuff.

I'm not going to name names here, but we have a vendor that we will be getting rid of because they have displeased us. I have tried very hard to explain what the problems were, because it's going to cost us to switch and it's going to cost them, obviously, some revenue. But I cannot get them to hear me because they've got this entire apparatus, full of product managers and marketing people and all the rest of it, that are doing what they were told to do. They don't understand why I'm not happy, and there isn't a path for me to somehow get to some key person and say, "You know, I may not be the only person who

hates your product. You should've made the following changes, you should find a way to listen to us." Now we're lucky, we're a small company at the moment of 45 people. So if you talk to any of those 45 people, you're going to get a sympathetic listener who understands what you're saying. But once you have 45,000 employees that gets to be darned difficult.

Ashwin: [00:04:41] You've touched on a really important topic here, which is the vendors' agenda and the customers' agenda are not aligned. We are here at Black Hat with 6,500 cybersecurity companies and growing. You've been here and you've done a lot and seen a lot. So, from your obvious vantage point, what advice do you have for vendors? Again, it's bizarre because I only have this in my framework: start, stop, continue. From your perspective what should vendors start doing, what should they stop doing, and what, if they're doing something great, what is it that they should continue?

Paul Vixie: [00:05:21] Well, it would help if a vendor had a larger goal besides pleasing their shareholders and having an early exit. Because when you do that, you compromise in all kinds of ways and you end up littering our industry with more debris of, essentially, failed ideas. If an idea has merit then you should be looking to find that merit, make your work as relevant as possible, and the money will come. But it's very hard to explain that to somebody who's got a fresh MBA and they're working inside a venture capital firm. "Yeah, I want to solve a larger problem." "No, we don't want to solve the larger problem. We need to make money for our limited partners. You know, please stick to the script here." So, I think my advice to a vendor is, don't hide your agenda. Whatever it is you're trying to do, tell your customer that's what you're trying to do. Don't tell them you're trying to make the world safer, if what you're trying to do is make your quarterly numbers. Say both are important and then make sure that your actions follow those words. I think if people would be transparent about their agenda, they would have to pick an agenda that they were willing to be transparent about. And that's my forcing function.

Ashwin: [00:06:44] This is an amazing conversation, because we kind of get into marketing. The expo floor is just opening up today and the amount of noise over there in terms of marketing overdrive you have to be AI, you have to be content, you have to be end-to-end. There's this whole machine that, as an entrepreneur or even a large company, if you don't have those buzzwords you're not going to be SEO optimized, you're not going to show up on Google's first landing page. And yet you have this dichotomy, when you go in front of the customer you have to drop your pants and tell them what your agenda is. So, how does someone do this? Frequently what I see is you get caught up in the marketing hype, and being in the product management side, I go in there saying, "Hey we're the best, we're the fastest, we're blah, blah, blah." Versus going in there saying, "Hey you know what, we're just going to take another nine months to get to the release that we promised you and I'm sorry for that." I mean, how does a vendor come to terms with having to regurgitate the noise without which they're not going to survive, as well as being, like you said, transparent in front of the customer?

Paul Vixie: [00:07:51] Well, my marketing team, both in this company and the previous company, has started out a little bit surprised when you say, "Actually, we're not going to say things that we can't support or that are not absolutely positive or true. We are not going to say what other people say just to stay at the table. Because we don't need to do that as long as we're doing something that really is going to make a difference." Then with enough effort and enough time we get success and you know our success has been, I think, guide worthy. I think we're sustainably growing. If I had any venture capitalists on my board, they would have fired me a long time ago.

So, we have booths at the trade show here and at other large trade shows, and what I see when I look at the customers, the prospects, the people who have the ticket to go look at the exhibits or whatever, they're just wandering down the aisle and they have this look on their face like, "Oh my God, it's you again. Didn't I just talk to you at the booth? It can't be the same person." And by the time they reach us, you know in the low-rent district, their eyes are glazed over.

They've heard the same buzz words mixed together in so many different ways. You know what I will only do if I'm doing booth duty, which I still do, even as CEO I think you have to keep your hand in, is I just say, "Aside from the checklist of things that auditors and other compliance teams have said you have to have and that you don't have - essentially a shopping list of stuff you've got to do - what are your actual problems? What is the thing that is making your life harder at the moment?" And if what they say is something we can't help with then I will tell them, "I wish I could help with that, but that's not the business we're in." And if they want to know what this is that we're in I will tell them, but that's real engagement. That's not engagement by the numbers where you get paid for how many cards you can swipe. That's looking for people who still remember what their problem is even though they've been talking to a whole lot of people for the last two hours before they got to go to your booth. But again, if somebody goes into a typical vendor and says I want to be part of your trade show staff because that's going to be my approach. They're not going to get the job.

Ashwin: [00:10:18] So, you have an unfair advantage, or your company has an unfair advantage, which is Dr. Paul Vixie's leading the team. There's an inbuilt credibility when you start talking. Lots of entrepreneurs don't have that, even if they have VC backing, they have to fight their lonely battle every single day. Number one. Number two, is there a cultural issue here? Where I'm Head of Marketing and I'm sitting at the booth and I'm going to be measured by my boss with the number of card swipes I've got. So even if I want to do the right thing, unless the organization is culturally completely reorganized, reoriented towards a goal which is larger than the card swipes, is this thing even viable?

Paul Vixie: [00:11:04] Well, I don't think you can hope that the people in the booth go wild and go sideways and do something the company isn't going to like, that's not a workable strategy, although I have tried it. I think what you have to have is the whole company has to be aligned around some ideal that is larger than what can be measured today. And that's true for all of us. It's true of trying to exercise or eat a good diet or whatever. If you're going to start and

stop measurement today, you're going to be able to tolerate a lot of stuff that isn't actually in your best interests.

So, what I tell people is, you're shooting for the renewal. I'm going to be very happy if some deals come out of this trade show, because we have some costs and I'd love to have some profit to offset against that. But what I'm going to be concerned about is that you sold somebody something that they didn't understand because you had the right smile, and you used the right phrases, and you reeled them in and so forth. That's not what we're here to do. If you don't think these people are going to use the product, renew the product, maybe expand their use, maybe add other products from our portfolio in Year Two. I don't want to start down the path with that customer and they know that. And so that doesn't mean that their boss isn't saying, "Hey, I got to have some card swipes." But that does mean that if that's all they do, they're going to know that they won't be with us long and again the whole company has to be aligned to that.

Ashwin: [00:12:36] That's actually a good point. I'm quoting something you've written about, about securing something you don't understand. From a knowledge perspective, except for a few large vendors who have the breath of portfolio, most people are trying to solve a very focused unique problem, right. So, what you mentioned earlier, I haven't seen any vendor do, which is go into a conversation saying, "What problem are you trying to solve?" and then self-select out because you don't solve the problem. Most of the times it's like, "Yeah, yeah, we can solve that too," and go back to HQ and change the road map and pretend you have. How does that culture transformation come about, where you can go in and say, "No, we don't do this, sorry," and walk out of that conversation?

Paul Vixie: [00:13:30] There probably comes a time when you can't. If you've got 45,000 employees, that is an incredible payroll beast you've got to feed every two weeks, and at that point you probably have to be a little bit less selective. But, you know, Google is that size and they seem to be doing just fine on growth.

I don't think anybody is confused about what they do, or what they can help with, or what they can't help with. So, I hesitate to say that some people shouldn't be doing this because there's clearly a lot of money to be made in our industry. Why wouldn't we want other people to come in and cooperate with that and participate in that?

When it comes to the understanding gap, the thing you were just quoting, if your fundamental problem is not the one you thought you had, was not the one you're walking on the show floor thinking you have, if your actual fundamental problem is that the attackers know more about your network and more about the devices and the vulnerabilities in those devices than you do, you're probably not going to be able to pave over that by spending more money on more complexity that makes your network even harder to understand. That may take certain attacks off the table, but it won't change the fundamental deficit of understanding.

So, you know I've got a number of friends who have done a number of other companies, Tenable being an example, where they're not trying to sell a whole bunch of machine-learning snake oil, they're selling a bunch of, well not a bunch of, but some of what they sell is pretty non-sexy.

It's like we want to come up with an inventory of everything you have so that you can integrate that with your BYOD policy, if any, and your network architecture about who's inside and outside what perimeter. So that when Shellshock comes along or whatever it is, some vulnerability that's in some open source thing you've probably got a copy of, like the refrigerator in your in your break room, it'd be great if you can be sure that you had found and updated everyone, but we don't have that because most people don't want to spend their money on something that isn't sexy. There's no screen in the security operations center that is visible through the glass wall behind you that is going to say, yes this is our inventory, and there should be. Because one of the things that I remember thinking about James Bond when I first started reading the very first Ian Fleming novel from the 60s or 50s or whenever that was, is this is not how

trade craft works. If you're actually in the intelligence service, you don't have a lot of glamorous women running around in bathing suits and you're not shooting people, you're sitting at a desk doing stuff that's fundamentally not very sexy. You can't make a movie out of real intelligence work, and I have a feeling you can't make a product out of a lot of the real security work that must be done.

Ashwin: [00:16:21] So that leads me to the question that CISOs have to contend with, and the more interviews I'm doing with CISOs, the more I'm realizing that there's a need for them to show up every single day. But also there is a need for them to tell the world around them, their VP of Marketing, their CEO, their Ops person about what they do. Every single day. So there is that mind shift that needs to happen which is, yes while the vendors are trying to push AI and MA and all these other whizzbang terms, and you might actually even get budget for that because the board is asking you, "Hey, what are we doing in ML, but you really have this long tail of hardware and software that you need to take it on. How does a CISO or VP of security operations deal with what gets attention, what they have measured against and how do they really reduce the risk?

Paul Vixie: [00:17:23] Here we end up with almost a warrior king attitude. If you think about the early days of electronic mail, when companies were first moving from paper that was stuffed into everybody's mailbox by the elevators to having everything on computers, there were people, we called ourselves postmasters but really we were sysadmins who were responsible for making sure all that worked. And we had essentially the computer equivalent of godlike powers. We could see anything, we could see everything, but it became quickly apparent that we must never use those powers except for good.

I've let the staff of every company I've started, this is number five, know that there are some things that you know are wrong. And if somebody asks you to do them, even if they're up the chain from you in the org chart, you have to say no and they know they've got my backing on that. So that just works. That's a trust that we all have. Right? Edward Snowden proved to the world that you have to be able to trust your sysadmin, and if you can't then you have problems that no

amount of security apparatus is going to solve for you. And I think the CISO needs to be like that. He has to have the power, or she has to have the power, to say no. Sometimes for the company's best interests what we need is to get this product into the market as soon as possible, because the area under the curve of our time in the market is going to dictate what the total profit is. And we don't have time to test it. We don't have time to hire a red team and see if it's got trivial...the CISO needs to be able to say, or the product security person or the V.P. in charge of all of that, needs to say, "I'm not going to do that. We're not. This company is not going to do that as long as I'm here, because I don't want to put stuff out there that's going to give us bad headlines and make our customers less safe. That's not what we came here to do." And the power to say no does not automatically come to these positions. And it has to.

I've seen a lot of chatter on LinkedIn and elsewhere in recent years about what should Boards of Directors do about cyber security. Should there be a specialty, some board member, instead of being an accountant or marketing person or whatever, that's what they do? And the answer is obviously yes, except we don't have enough people to make that work. So what we're going to have to do is use the people we have and give them the power to influence decision, because sometimes the best thing for the company to do is not going to be the best thing for this quarter's results.

Ashwin: [00:20:05] Right. So that leads me to one last question which is, is the persona of a CISO, which is steeped in technology, now need to change automatically to be more business-focused, more outcome-focused for lines of business, for the Boards of Directors? Which is a different job definition than what we've seen traditionally in the past. So is that a little bit beyond being able to talk a language which is non-tech and still conveys the ordinance of what's being done and the impact of not doing their job that could have on their business?

Paul Vixie: [00:20:47] I think if you're a CxO that's got to be true. And you know I've even noticed that in the pure engineering side of the house, at a certain

point the person who's championing some product and who's got the vision and can explain it to anybody and is there pushing for it, for it may even be her idea, has to be able to explain it in terms of the profit. There has to be a business plan, and they have to be able to write it and speak to it. If you can't do that, then you're going to remain a senior engineer rather than a distinguished engineer, at least in my company. I expect people to have the full spectrum of business capabilities which includes technology, but it also includes some other stuff. I think for CxOs that has also got to be the case.

If what you have in your CISO position right now is a very good-hearted, very brilliant geek who can't get up in front of a Board of Directors, and not so much just say no, but explain why no is the right answer, then you need to get that person some media training, because that would make you blind in a very important way. If I was going to leave you with one thought, it's that a bank used to be a building full of money that had in it somewhere a room full of computers. And that has reversed. Banks are now I.T. companies. Their principal job is to secure their customers' transactions not to secure the physical money. And in the last ten years a lot of banks have turned around and they have their own patent portfolios. They're competing in college job fairs. They're not just buying off the shelf, they're doing integration in-house because they recognize that if their DNA doesn't include cyber-security and cyber-operations they're going to be out of business. And I would say that that was obviously true for the banks. It's less obviously true for the rest of us.

Ashwin: [00:22:47] I think it's a great takeaway. It's been a fascinating conversation, so thanks for your time, Dr. Paul.

Main discussion topics:
02:16 The six questions you need to ask in any relationship
05:21 Client agenda versus Vendor agenda
07:51 The importance of vendor transparency
11:04 Measuring sales success while maintaining credibility
14:45 Security technology isn't sexy

17:23 CISOs need the power to say no

20:47 The importance of the CISO as a communicator