uberknowledge

Brian Vecci, Field CTO, Varonis

Is it time for a Consumer's Technical Bill of Rights?

Brian Vecci talks about how freely we give away our most precious assets - not our personal ID but the data on our habits and behavior.

2:07 We get trained to say yes to everything.
2:48 We will never get to the point where consumers actually understand the EULA they are signing.
4:35 Data breaches of names and addresses are old news. People will only sit up and take notice when the data breach is of their Google search history or most visited locations.
4:47 Privacy is different to security. Privacy is the next technical or security leap forward.
6:24 A consumer's Technical Bill of Rights.
07:53 20 percent of all data is open to everyone.
09:11 Consumers don't understand how little privacy protection they have, and businesses don't understand how much risk they are undertaking.
10:58 Consumer behavior won't change, so companies need to quantify risk.
12:12 There will never be enough manual hands to manage all the data and put the controls in place. We need AI and machine learning.
16:44 A great piece of advice for selling in any industry: listen with empathy.
21:09 What is trust in the security environment?
22:65 When you talk about vendor-customer relationships, trust is emotional. Security is emotional and poor security has consequences, perhaps not enough.
24:00 Trust is built within an organization and then between that company and its customers.

Ashwin Krishnan: [00:00:40] Thanks for joining me, Brian, on the UberKnowledge podcast. For the benefit of our listeners can you go ahead and quickly give us your background, before we dive into rich and invigorating topics?

Brian Vecci: [00:00:53] Absolutely. My name is Brian Vecci. I'm the field CTO at Varonis. I've been at Varonis for nine years now. Took a little break and then I came back. Before that I was in systems architecture at a big bank, and I was a developer, a project manager, a systems architect, a program manager. I've worn a lot of different IT and development hats. I wasn't a particularly great developer, which is why I stopped developing relatively early on in my career. But what I was pretty good at was understanding the technical concepts well enough to translate them to … I almost went into my pitching mode to business value.

[00:01:27] What I really meant is, I could sit in a room with a variety of different people and help everybody understand, here's what we're doing and here's why we're doing it. And then about nine years ago I was fortunate enough to land at Varonis, which at the time was a startup. Now we're in that post startup world, and in my role now, I get to be kind of the connective tissue. So, I'm not a salesperson, but I spend a lot of time with our salespeople and in the field with our customers and prospects. I am not a developer, but I spend a lot of time with our engineers and product marketers and product managers. And I don't really run the company, but I spend a lot of time with our executive management trying to help them understand what's going on at the ground level with our customers and vice versa, I explain the direction of the company. Those kinds of things.

Ashwin Krishnan: [00:02:07] Got it. So, one of the things that I found really fascinating doing a little bit of background on you, I'm a social troll as well, is the CNBC interview that you did on data privacy. And I quote you, "We just get trained to say yes to everything." From a consumer perspective, there's just so much being thrown at you, right? A new app being downloaded and the EULA and now with GDPR, it's like storing cookies, just say yes, say yes.

[00:02:35] In your mind, how does this eventually get to a point where consumers don't necessarily become activists, but they become more aware of what they are saying yes to and why. Is there a vendor responsibility as well?

Brian Vecci: [00:02:48] So, there's lots of answers to that question. I honestly don't think we're ever going to get to a point where users have any understanding of the EULA that they're signing or saying yes to. I think it's absurd that we're expected to read a 92-page EULA when we download an app or every time our iPhone gets updated. Anytime we install new software, somehow we're expected to be a lawyer that understands what goes into these privacy policies, that's just absurd. And I think there is no world where that's going to happen. What is going to happen is that consumers are going to start to realize that their data, and it's not just their data, it's not just your name and your address and your social security number — honestly at this point, I assume that my name, my address, my social security number, my telephone number, my e-mail address ...

Ashwin Krishnan: [00:03:33] Is already out there.

Brian Vecci: [00:03:34] It's already out there. It's been part of so many breaches now that, yeah, that's out there. You know what isn't out there though is my personal behavior. There is a wonderful Saturday Night Live skit where Eli Manning is playing an accused murderer. He's in a courtroom and the prosecutor says, "I'd like to introduce into evidence the defendant's search history for that evening." And Eli leans over and says, "I'd rather just confess to the murder."

[00:04:01] Our really private information is our behavior, right, and our location and our search history and things like that. And I think consumers are going to start taking much greater notice when we start to see data breaches — not of names, addresses, and phone numbers, that's happened, nobody cares — when we see data breaches of your Google search history and it's linked back

to your email address, and you start … Because I get threatening e-mails, I'm sure you get them too, "This was your password." Yeah, it was my password, a thousand years ago before I used a password manager. So, I don't really care, but here's the thing that you searched for on Google yesterday, here's your Bing search history, here's a list of the 10 places that you were most commonly in the last month.

[00:04:47] That starts to open up my eyes, right. And so, privacy, which is different from security, is, I think, the next technical or security leap forward. Here's what I mean by privacy is different from security. If I hand you something valuable, I've got my passport here because I lost my driver's license — really, I shouldn't admit that on a podcast — but I lost my driver's license, so I've got my passport here, if I hand that to you, you can tell me, "Brian, I've got a privacy policy. I am not going to do anything that you wouldn't want me to do with this very sensitive information." And then you go out and you throw it into the middle of the street, and you just leave it there and you turn your back. That's how most companies treat this kind of data. They have no idea where it is. They have no idea who could potentially look at it. They have no idea who is looking at it. So, they don't have the security controls in place to make sure the data is kept private. And I think what is going to happen, to bring this back to the question that you asked, is we're going to be in a situation in the not too distant future where consumers and especially businesses are going to demand privacy. And it's not so much that I don't want my data to be breached, it's that if I give you something valuable like my location, access to my photos, access to my browser history, access to any kind of behavior that can be linked back to me which is, by the way, what the GDPR says, it's not just name, social security number, credit card number, things like that, you have to treat that as if it's something valuable because you're deriving value from it. You're, this kind of sounds like a negative term, but you're exploiting that information for your own benefit, otherwise why are you collecting it because it represents some risk.

[00:06:24] I think what we're going to see soon is privacy policies, EULAs, all the things that we click on without thinking that stuff is going to have to go away at

some point. And there just has to be some sort of, call it a version of net neutrality — which is a whole different issue — but call it a consumer's technical Bill of Rights. Here is what we as people in an interconnected world demand of the entities that are gathering information about us. Here's what we demand they do to keep that information relatively safe and private. There is no such thing as perfect security. Security is a journey.

[00:07:02] I got raked over the coals for going on CNBC and beating up on Marriott for their breach a few months ago. And that's fine. Marriott got raked over the coals much more than I did, and their excuse or their explanation was, "It wasn't us it was Starwood." My response to that is, "Yes, but you bought Starwood." Starwood had a certain amount of risk that you did not quantify or at least you didn't quantify properly or if you did then don't get mad at me for getting pissed at you for letting that data out. Right? Yeah, it was Starwood's fault, but you bought them. You brought them into your network. It's Marriott's name now, and every company that does that just like every consumer that knows ... Listen, you bring a stray dog in your house — and I love dogs and I've rescued a couple of them — but you bring a stray dog into your house, it might have fleas. You buy a company, it may have security issues that you don't know about.

[00:07:53] A big part of the problem is that not enough companies are doing the basics to understand the risk that they've got on their data. Again, 20 percent of all data is open to everybody, most companies don't even know that that's the case. And I know that because we do risk assessments, and we will show that on the screen, and I have legal in the room looking up at a presentation that I'm giving saying, "What do you mean we have 335,000 folders that have GDPR data and are open to everybody in the company? There's no way that that's possible."

[00:08:23] I'll tell you another story. We had a team go into a meeting with a prospective customer that we had done a risk assessment for, and on the way in one of our engineers said to the CISO, joking, "Did you know that the

receptionist, who is very lovely, that just let me into the building, she has access to your salary information and the salary information of everybody in your executive team and actually everybody in the company?" He looked her in the eyes and said, "No, that's ... ok listen, I get you're trying to sell me something. I get you're trying to give me some shock and awe, but that's absolutely impossible." He said, "I'll bet you dinner." So, they went back to the receptionist's desk and because we had done the risk assessment, we knew exactly where this data was, we knew that it was open to everybody who was an authenticated user, went whack whack to the file server, opened it up, brought up the spreadsheet. The CISO was blown away.

[00:09:11] This is so common that what it says to me is two things. Consumers don't understand just how little the privacy protections are for most of the companies that they give their data to. And most companies don't really understand the risk that they're undertaking by having this data and having it so exposed. I've been talking for way too long.

Ashwin Krishnan: [00:09:31] No, no. It's interesting that you bring two sides of the puzzle. One is consumers: should they become custodians of their data? Which is a kind of a newfangled concept of who do I give my data to and at what price. Then from an enterprise standpoint, there is the classification of data, how many primary, secondary, tertiary backups and just the magnitude of what that entails. Do you see either side doing anything about it or are regulations the only place to look for getting people to act?

Brian Vecci: [00:10:11] You're gonna laugh at me when I say this.

Ashwin Krishnan: [00:10:12] Ok, I'm laughing right away!

Brian Vecci: [00:10:14] On the first part, I don't see consumer behavior changing all that much because, honestly, the price of admission to get somebody's data is to have an app that they care about and that people download. I challenge anybody, if you really want to go through an archaeology project, you can go

— at least I'm sure you can do this on Android, but I have an Apple, I have an iPhone — you can go to the App store and you can look at every app you've ever downloaded. You can scroll through, it'll take you hours to scroll through. My first iPhone was a 3G, so I've downloaded thousands and thousands and thousands of apps, potentially all of those apps still have some of my data. So, I don't see consumer behavior changing all that much. I honestly don't see consumers starting to think of their data as something that needs to be paid for because it's already seen as something that's valueless, at least initially.

[00:10:58] I do see consumer behavior, at least I hope, I'm not sure if all consumers are going to behave, but it's like the bike lock analogy — you don't have to have the best bike lock in the world, you just have the better bike lock than the guy next to you. And so, I'm seeing a lot of password managers becoming more common. People are being way more careful about the permissions that they grant to apps. Why do you need to access my location history all the time? The platform vendors, Apple and Google, I think are doing a much better job of exposing some of those controls and they continue to make better choices. But the second side of that is do companies really understand or are companies properly quantifying the risk? The reason I talk about risk is, risk is a business issue not a technical issue. Technical risk is how valuable is the asset, what's the probability that something bad is going to happen to it, what's the potential impact of a loss or misuse. And what we know is that companies have not been able to properly quantify the risk to data. And here's where you're going to laugh at me, because the problem is so big, it's going to take automation to do it, which is where AI/Machine Learning works has to come in.

Ashwin Krishnan: [00:12:12] Laughs.

Brian Vecci: [00:12:12] There is never going to be enough people, there's never going to be enough manual hands to do the kind of work necessary to put these controls in place. That's why you need automation. And the only way to do automation at scale these days is with lots of data and really good algorithms, and I've just described what AI and machine learning are. So, that's

where I think that has a place. Now that said, we're at RSA where everybody is talking about AI/machine learning. It's like, I'm going to make you a better peanut butter-jelly sandwich with blockchain. How are you going to do that? Doesn't matter, here's some VC money. And I think that's where separating the signal from noise. I don't envy CISOs these days. I know how hard it is. It's hard enough for me to separate the signal from the noise just in the vendors that are trying to contact me. Let alone if you've got a CISO title. I can't imagine how you're trying to separate real value from science experiments, and that's not to say one can't come from the other, but who's got time for science experiments these days, unless you're one of the big banks and you've got a hundred thousand people that you can really build a data lake and build all the stuff yourself. Very few companies can do that, which is why, I think, we're seeing time to detection for incidents is going up, and time to response is going up as well which is not an encouraging thing. Insiders are more sophisticated, attackers are more sophisticated, and because of the depth of technology that almost every enterprise has to deal with these days, the ways in and the methods that you can use to remain undetected are just growing. Which should be scary which is why we need automation that actually moves the needle and makes a difference.

Ashwin Krishnan: [00:13:52] So, getting you back from AI/machine learning to …

Brian Vecci: [00:13:56] Please do, pull me back from that precipice!

Ashwin Krishnan: [00:13:58] So, I'm going to do that now, try to do that. On your podcast on the Varonis website, you talked about something which is not very common: listening and empathy. We had a brief chat before the podcast and I quote you, "Learning how to shut up and listen, have a little bit of empathy and think about the people that you're talking to and what they care about was one of the hardest lessons for me to learn because it's something that I'm not naturally good at, but it's something that stuck with me for eight years and something I continue to work on." Number one, kudos to you for admitting the fact that listening was really hard.

Brian Vecci: [00:14:33] Thank you.

Ashwin Krishnan: [00:14:36] But in this day and age — and we're at RSA right now and the noise level is really, really high — how does somebody change the way a customer conversation happens? And in your role, being the connective tissue, you have a little bit of leeway to do that, but think of the average sales person on the street trying to make a quota number. How do they change their behavior and actually stand above the rest of their competitor sales men and women who are trying to do their thing?

Brian Vecci: [00:15:09] Well I'm going to be careful in how I answer that question because I'm not a sales person. And I want to be careful and be a little empathetic with salespeople because that is a hard job, especially in enterprise sales, especially in security sales. It's an incredibly hard job and I would never presume to tell anybody any kind of silver bullet that is going to make you better. I'll tell you the piece of advice that I got that changed my thinking about it.

[00:15:34] So the first thing, and I learned this later, but I worked for a company that sold software that people didn't know about, so we had to do a lot of teaching and evangelizing in every meeting that we did. Varonis? Who are you? What do you do? Why do I care about this? That means by default we were doing a lot of speaking. There's this concept of, I think it's called the idiot curve or some sort of curve, think about a parabola, like a bell curve. You start out in your sales career not knowing anything about what you're selling. So by your very nature, you ask a lot of questions because you have nothing else to say, right? And asking a lot of questions, I think any sales person would tell you is a very good strategy. Then as you learn your product suite, you learn your customer base, you learn your value proposition, you get so excited to talk about what you're doing. And your knowledge goes up in this kind of bell curve, so you spend more time talking than listening, more time saying than asking. Then eventually over time, you get to a point where you realize I know what I

know, now I'm going to use the knowledge that I have to ask good questions and elicit good responses.

[00:16:44] The one piece of advice that I got — and this was from our chief marketing officer, who at the time was Director of Technical Marketing, he was an SE at Varonis and he had hired me. I was going into a bunch of meetings on the West Coast. I was traveling for the first time. He said, "Brian, here's what I want you to remember: Make the meeting about them, not about you. It's not about you. It's not about whether you know what you're talking about. It's not about whether Varonis is right for them. Just make it about them." When you go into a room, and your goal is to understand and make the meeting about the person that you're meeting with, I think it changes your approach a little bit. It's really easy as sales professionals to think, I've got an agenda, I've got a playbook, I know what I'm doing, I'm going to go in and nail my presentation, I'm going to get that next step, I'm going to get a risk assessment, I'm going to get an evaluation, I'm going to get a purchase order, whatever it might be. But if you flip your mindset a little bit and think, all right what does Ashwin want out of this meeting? What is it he really wants to get, and oftentimes the answer is I don't know. Then you can start to ask some questions. What would a good meeting look like for you? One of the things that I've started doing in almost every meeting is asking permission to ask questions and then asking the people that I'm meeting with, "Listen, if I start talking about something that you don't feel is very relevant for you, would you feel comfortable telling me to shut up and move on?" and I've never gotten a "no" to that question. What it does is it tends to lower the tension level a little bit because now this is a, to use a broad term, a bidirectional conversation.

[00:18:26] I am fortunate enough in my role that I don't have a sales role. I don't have a quota to meet. So, I'm not living and breathing on the outcome of these meetings. I'm living and breathing on did the person that I'm meeting with feel better about me, Varonis, themselves, their goals. Do they feel like they're in a better place now than they were an hour ago or a half an hour ago or in some cases four hours ago, whether it's an executive briefing or something else, and

that ends up being my goal. And I found what that's done is force me to listen. Empathy is about listening, empathy is about putting yourselves in somebody else's shoes. And I think the sales professionals that aren't as successful tend not to do that. The ones that are, are the ones that really understand I'm here as a representative of a company that's trying to sell them something, but if I make this about Ashwin, if I make this about you and you getting some value out of taking time out … look how busy we are! I mean, you mentioned before we started talking, who's got 25 minutes, right, even to listen to a podcast? God bless all of you that are still listening.

[00:19:39] If I make this about you, I'm putting myself in a much better position to be successful and success really is, did you care at all about what I had to say? And having been in a lot of sales calls, the answer to that question far too often is, no. We're in a very ... it's a quota-driven culture and that's just the way things are.

Ashwin Krishnan: [00:20:01] This actually gets to the last point I want to talk about. We talked about security; we talked about privacy. The last part that you talked about is customer empathy which actually leads to probably one of the most-used phrases in RSA 2019: trust. If ultimately your secret sauce of actually building and maintaining customer relationships and eventually customer data is about building their trust and becoming that ...

Brian Vecci: [00:20:29] Safe advisor.

Ashwin Krishnan: [00:20:30] Yeah exactly. I mean, I don't want to use that word! Is that something that you see becoming center stage right now? Yes, we need to secure data. Yes, we need to keep data private, but ultimately, it's about building that trust. So your customers, your prospects actually believe in you. And I've heard this a number of times in the podcasts I've done this week. It's about the people behind. Good salespeople, as we talked about earlier, could go from Company A to Company B and customers would still buy from them

because it's "Mary" you're talking to. I don't care what product you have behind it. What thoughts do you have on trust?

Brian Vecci: [00:21:09] People buy emotionally and then rationalize it later. I think when you're in a role where you have to be a technical person, we deal in technology, we deal with engineers, we deal with code which is very rational. But people make investments. People give up money. People put their neck on the line, right? Making a major investment in a new technology is, to use my old financial way of thinking, it's a change-the-bank exercise. And you don't change the bank unless you're confident you're not going to break the bank, right?

[00:21:44] My first job in IT was as a help desk analyst. My job was: I can't print, I can't do this, I need access to this. And I think everybody in technology should work help desk for a year, right?

Ashwin Krishnan: [00:21:56] [Laughs]

Brian Vecci: [00:21:57] I think it's the best training ground you can possibly learn in. But my boss told me be careful when you start making changes. You go into someone's workstation, and you go into a file server and you go onto whatever. The fastest way to get fired is to fix something when you don't know what that fix is going to do. Trust is an emotional thing, which is interesting because we're at RSA so there's also a technical concept of trust. This concept of zero trust or trust but verify. But when you're talking about vendor-customer relationships, trust is emotional and with security there is a lot of emotion behind security. That poor security or poor privacy can cost you your job. You can cost a company their brand, their bottom line. I think there's an argument to be made that there's not enough of a cost. I mean, Equifax seems to be doing fine, and Marriott's going to be fine and, to bring back that SNL skit, a lot of companies would rather just confess to the breach than have to pull up their skirts and show the controls that were there.

Ashwin Krishnan: [00:23:04] Yeah.

Brian Vecci: [00:23:04] I think it's a really good question. I think trust is built on vendors, and especially salespeople, having empathy for the people that they're selling to. Trust is built on good listening and good questions and on standing up for what you believe. Good salespeople, you mentioned, will move from company to company and sell anything, but the really good salespeople, they go where they know that they trust the company that they work for, they trust the culture of that company. You've written and talked a lot about diversity and listening to different voices and how powerful and how important that is. I think trust is built within an organization, a sales organization, a technical organization, in the company as a whole, and between that company and its customers.

[00:23:55] Technology aside, you can have technology that works or doesn't work, but trust is built on people. And at the end of the day, we're all people and we need to interact with each other in ways that build trust. I kind of went off the rails. I hope that makes sense.

Ashwin Krishnan: [00:24:11] No, it does. So final question, we are at day two or day three depending on when RSA started for you, what would success mean for you at RSA 2019?

Brian Vecci: [00:24:25] Success for me here is ...

Ashwin Krishnan: [00:24:27] Good swags?

Brian Vecci: [00:24:29] No. I used to love the swag because my wife's a teacher and she could put it in her prize box — Hi Olivia, I love you — her prize box for her students. But really for me, it's when I go back through my notes. I meet with press, like you, I meet with media, I meet with customers, I meet with prospects, I meet with other technology partners, and I meet with our internal sales and executive teams. I'm going to go back through 30, 40, 50 pages of notes. When I

look at each of those various stakeholders, I'm in this wonderful position where there's lots of people that interact with me and I can say I know that this sales team is better off because I've met with their customers and their prospects and I've moved the ball forward on those deals. These customers that I met with feel better about Varonis because they met with somebody who looked them in the eye and said, "I'm going to help you get more out of what you have." Period. It's like anything else. What you got, I can make it more powerful and more valuable for you. And they feel better and they're going to take my phone call in a month or two months when I said that I'd follow up. Our executive team is going to look and say we are getting leads from the booth or we are getting leads from the media appearances.

[00:25:42] Basically if the people that I meet with here feel better about the show than I have done my job and that's what success is for me. For me RSA is about everybody else that I'm meeting with. There is no metric for me. My metric at RSA is how many people did I meet with. Did those people feel like those meetings were useful and did they feel better about themselves, our relationship or Varonis as a company or especially our technology - I'm the field CTO - do they feel better about our technology, who we are as a company? Then I've done my job.

Ashwin Krishnan: [00:26:15] Cool. I don't think we can we can top that. So, on that note thanks Brian for your time.

Brian Vecci: [00:26:20] Thank you so much. It's been a pleasure.

Ashwin Krishnan: [00:26:22] Thank you.