uberknowledge

Taylor Lehmann, CISO, Athenahealth

A CISO's Journey in Healthcare

Taylor talks about his journey through healthcare security, the unique loss of life challenges found there, and his personal motivation.

03:34	Vulnerability is necessary to build trust, and trust is crucial in cybersecurity.
07:12	Data breaches are not inevitable. We can do this right.
10:49	It's important to understand not just your company's mission, but why the employees come to work everyday, and why customers buy your product.
12:01	A security career in healthcare - finding meaning and purpose in every job, every opportunity.
13:59	Applying a DevOps principle to cyber in healthcare: learn how the system works before trying to solve problems.
18:03	90% of cybersecurity products are devoid of thoughtfulness. Vendors need to learn the industry — and the CISO — they are trying to sell to and be able to show how and where they can help.

Ashwin Krishnan: [00:00:30] With me on the Cyber360+ podcast hosted by UberKnowledge, I have Taylor Lehman. So, Taylor, I know the last time we spoke, you'd just taken on a new job as CISO of Athenahealth. Why don't you tell the listeners about what you're doing right now and your journey, and then we will get started.

Taylor Lehmann: [00:00:52] Great. Thanks, Ashwin. I've now successfully transitioned to be CISO of Athenahealth, which is a large software company on health information technology located in Watertown, Massachusetts. It's a transition, I'm still in the throes of getting to know the organization, but, you know, things are going about as smooth as they as they possibly could.

Ashwin Krishnan: [00:01:26] Great. So, I was looking at your LinkedIn description and I just have to read this out because it's something that is very unique. You say, you believe safety is achieved through security and you value vulnerability and courage over personal comfort and then you help keep things running.

[00:01:45] So that's a very, very unique description, unlike anything that I've ever seen. Can you elaborate on what you mean, especially on the middle sentence, which is vulnerability and courage over personal comfort?

Taylor Lehmann: [00:01:58] Yeah, man, where does that come from? So, I had a great coach in a prior role; her name was Bev Halperin. And if folks are looking for outstanding coaches, Bev was certainly one for me. As part of my development, I would say, Bev introduced me to a variety of texts, some of which came from a very popular author and coach herself, Brené Brown. One of the many things she's done, in addition to TED talks and books, was really talking about vulnerability and the ability to be vulnerable as a powerful tool to not only endear yourself to others, but to help you get control of the things that hold you back, or the things that you live with that you don't need to that create fear and make your life difficult. And behind this term, the power of vulnerability, one of the behaviors I try to model that Brené talks about in her writing is just kind of putting it out there, putting yourself out there, making the conversations personal and leading that way. Perhaps being aware of and accepting of the things that maybe you're not great at or the truth behind a certain set of facts or circumstances you might be in and not hiding them.

"Vulnerability and personal courage are at the start of every day."

[00:03:34] You know, it was really important that to really gain trust and to earn the trust of others — which it is necessary in cybersecurity to be great at because in many cases, you're seen as an adversary for the companies you work for — you really need to be vulnerable. Being vulnerable takes a lot of personal courage. It's not something that people can easily do, to admit your faults, to talk about things in a way that might actually not make you look great, but ultimately, these are the things that people look for when they want to find someone they want to work with.

[00:04:08] And so to me, you know, vulnerability and personal courage are at the start of every day and every conversation I try to have and what I encourage others to try to do; I think it's absolutely essential. In the industry we're in, I feel like if more people

were genuine and focused and authentic and understood maybe that they had some blind spots and that they were working towards them, I think that we'd have better leaders and ultimately we'd have better cybersecurity programs.

Ashwin Krishnan: [00:04:40] Wow, that's really inspirational. You talk about Brené Brown, her TED talk obviously has gone viral, it's "The Power of Vulnerability." For listeners who haven't listened to her before, I encourage you to do so; it's really powerful.

[00:04:53] So switching gears a little bit, when it comes to healthcare and security, it's probably in the news more often than it should be, whether it's the UK hospital system that came under attack about two years ago — 16 hospitals in a ransomware coordinated attack, putting patients' lives at risk — or more recently a server of a U.S. company, I think it's MobilexUSA, displayed the names of over a million patients all by typing in a simple data query. As a CISO of a fairly important organization in healthcare, how does Taylor approach every single day knowing that literally there are medical records, there are patients' lives, there are other sorts of life-changing situations that you might have to deal with? What does it mean being a CISO in healthcare versus, let's say, being in IT or OT for that matter?

Taylor Lehmann: [00:05:47] I think the subject matter is obviously a little different in healthcare than it might be for a bank or for a retail organization. It comes back to understanding your mission and what you're in the business for, first and foremost. In healthcare, some would disagree, but for me, you know, our job here is to ensure health care systems run, it's to ensure patients get the treatment they need, it's to ensure that doctors and clinicians are available to do it, and every decision we make in terms of how we build and deliver software and services and systems needs to be in support of those outcomes. As opposed to, and I think what happens more often than not, is that we get over enamored with blinky lights and tools and laying down hardcore security programs that get in the way of things.

"I don't think it's ok that we have them, and I don't buy into the belief that it's inevitable."

[00:06:39] One very important way to orient yourself in healthcare is, asking yourself what really matters about the work that your organization does? In my case, it's to make sure that, you know, outstanding software allows providers to have the interactions with patients that they need to deliver healthy outcomes. And so, when I think about the strategy that I'm here to build with the team that I have and the resources that I've been given, it's to drive towards those outcomes using my security program as a tool.

[00:07:12] So, yeah, the risks are high. The bad things that can happen in healthcare are pretty bad. Data breaches are obviously terrible things. I don't think it's OK that we have them, and I don't buy into the belief that it's inevitable. I'm a very firm believer that, not just for healthcare but for others, we can actually do this and we can be successful at it, but I think it starts with mission orientation.

[00:07:43] Anyway, back to the point. Confidentiality of data is one really important risk in the healthcare industry. You know, this stuff is worth a lot of money. People want it. They're willing to go through steps to get it. The threat actors are sophisticated and they're focused. But for me, the outcomes I'm really trying to avoid in addition to data breaches are the ones that put the systemic delivery of care in our country at risk. We've got a variety of wonderful tools. Our software is used in a number of different places. We have a major role to play in the delivery of care to patients in this country. To me, when you think about what that means, it really plays out into the resiliency of a system; it plays into integrity of data; it plays into availability of the system. So in addition to confidentiality of the data itself, and yes, it's our most important asset, there are other really important things that we need to focus on in cyber in healthcare, which I think are fairly unique.

[00:08:51] Yes, you want the bank to be up so you can process your check, but maybe that's an 8 to 5 sort of thing. For healthcare it's 24/7 and the outcomes that we're protecting here against in some cases are life and death. You know, you can get your account back and get a new credit card. You can get a new driver's license, but you can't replace when somebody gets hurt because a piece of connected equipment malfunctions or the refrigerator attached to the blood bank goes down because it's been ransomwared or, god forbid, the implants to chest pacemaker, cardiac defibrillator gets ransomwared. Those are outcomes that are unique to our industry and that we need to be focused on preventing.

"Those are outcomes that are unique to our industry and that we need to be focused on preventing."

Ashwin Krishnan: [00:09:33] Going back to something that I found really inspiring from somebody who's as public as you talking about not just things like security and privacy, but also — exactly how we kicked off the whole discussion — about vulnerability. There was a post that you shared about four months ago sharing an article that first appeared in The Washington Post about how an amusement park worker had an autistic child who had a meltdown and was lying next to him as he was kicking and screaming. And you challenged the LinkedIn readers with this really powerful question asking, what is your mission, and then making it easier for them saying, you know, your mission is really to be better and see how what you do serves someone else.

[00:10:20] So clearly, that must have been ... you mentioned a few people in your life, but if you can elaborate a little bit on how your journey has taken you to where you are right now, where you're comfortable in your own shoes talking about being out there and going outside the standard definition of your job and really connecting and being empathetic with people around you.

Taylor Lehmann: [00:10:40] Yeah. It's an interesting story, at least it's interesting to me, it's probably boring to everyone else in the world, but I'll tell it.

Ashwin Krishnan: [00:10:49] [Laughs].

Taylor Lehmann: [00:10:49] As you know, I'm still in my first 90 days of being a CISO at Athenahealth. I've got a lot to learn here. I'm active in meeting our customers and our teams and really spending the time up front to understand not just the mission of the organization, but why it is that people get up to come to work every day to work here and why our doctors and our clinicians choose our software? And that's a process, it is going to take time, but it's important because often that process is overlooked and not taken into consideration.

[00:11:26] I would say a lot of the empathy and understanding that I've built has, I think, brought me to a level of awareness around what it is that I do and why I do it, and why I say some of the things that I say or take positions on the things that I take is because of that. That sense of understanding and empathizing is never over; it's something that you have to do. So in my first 90 days as a CISO, given the importance of such context setting and learning and listening, it's effectively the thing that leads to those outcomes and perspectives.

[00:12:01] But I will just go back to say I started my career in 2002 as a consultant at PWC working in healthcare industries: young kid, didn't know anything, saw healthcare as a major problem in which I'd be gainfully employed for a long time if I learnt the business and found innovative ways to solve problems. This is when HIPAA was new. I then took a job after losing a family member back where I grew up in western New York at a health insurance organization, which was the first time I'd say I really got into the industry and understood it from the perspective of the health insurance payer, which was new to me. I had preconceived notions about why they mattered and what they did. You know, in addition to paying claims, health insurance organizations are really interested in making sure the health of its members is taken care of and handled. And it was the first time there that I saw the work I do here enables that mission. So, if I can understand more about why security and passwords and two-factor authentication connects to the outcomes I'm looking for, maybe I'll have something.

"The mission of these organizations is about treating patients … it's not just about money."

[00:13:09] From that point, I went to a bank to see how a bank did the same thing. I didn't find the same amount of personal enjoyment as I did in healthcare. So I went back and worked on a payer health IT system at a company called HealthEdge, which gave me the perspective of supporting a health plan on the vendor side. So having been one and now becoming a vendor to one and understanding why my clients pushed me in a certain way to make sure my software and my product was outstanding, that gave me amazing perspective. I got to go and work and see and talk to outstanding people from all around the world in many, many major large health insurance organizations who really lived and cared for what they did. It really brought me back to the mission of these organizations is about treating patients and getting to outcomes that are beneficial; it's not just about money.

[00:13:59] From there, I took a gig at Wellforce, a large hospital system here in Boston. And this was the experience, I think, where I was finally able to start putting some of these things together to understand deeper exactly what connected my work to my outcomes. One of the most powerful things that I experienced and will continue to do now, because I understand its importance, is rounding with physicians. Literally following them around so that I could see how care delivery worked. To borrow a DevOps principle, the first thing you need to know and to take into account in order to start solving problems is to understand the way the system works: systems thinking — **everything flows to production, left to right, in a software development lifecycle. While in a hospital, everything flows to patient outcomes**. So that's every step of the way: it's registering; it's getting in; it's getting screened; it's finding the doc; it's getting the medical records updated; it's getting the drugs delivered; then it's saying goodbye when treatment is over.

[00:15:09] The best way to understand the systems that you're in, especially at a hospital, is to go and see and watch the work get done. So we round. Rounding not only taught me really what mattered, but I could see it because I could see my customer. I could see the pain they were going through. I could see my users and the pain they were going through in using the systems. From that perspective, I gained so much in terms of not only empathy for why we do what we do, but back to what the goals I was trying to hit were. It wasn't getting a more secure system. It was facilitating, how can I make sure that that note the doctor is writing is accurate, that it doesn't get deleted accidentally by some system glitch or some password protection I put on the screensaver. It doesn't get done if, like I said, the wireless bed that patient who just had spinal surgery is on malfunctions. It brought me to an awareness around why we do what we do and how I played a role in that, because I could see it.

"The best way to understand the systems that you're in, especially at a hospital, is to go and see and watch the work get done."

[00:16:07] I think that whole concept of getting on top of machines and watching production workflow get done, which is a very popular way, folks who focus on manufacturing efficiency figure out how plants run because they watch the work. This is something that the Toyota production manufacturing team does, they stand on top of buildings and watch work get done. Same theory applied to healthcare. It's really bringing yourself back to getting closely connected to your work. And for me, you know, it was adding up of many experiences over a number of years to then finally being able to sit there and watch the work and understand it at all steps.

Ashwin Krishnan: [00:16:46] Wow, that certainly gives perspective, which is interesting because it leads into my next question. I think I know the answer, but I want to ask it anyway. It's something that plagues a lot of security vendors, but also the broader IT vendors, again going back to something that you had commented about on LinkedIn: the FUD marketing flowchart. As you're talking about how products are getting built and how marketing jumps on a few buzzwords, and then it gets

marketed, and then salespeople start harassing you through emails.

[00:17:16] Clearly, this antagonizes CISOs, and you guys are obviously a very close-knit community, so it's not just affecting a single buyer but rather your coterie in the buyer community. So, two questions: number one, why do you think the vendor community has not changed tactics knowing that this not only does not work it actually jeopardizes relations? Second, have you a few instances where you've seen vendors operate using a different blueprint that actually does wonders to build connection and empathy?

Taylor Lehmann: [00:17:55] So this is really around how vendors are engaging. Is that the question?

Ashwin Krishnan: [00:18:00] Correct. How they are, and how they should be.

Taylor Lehmann: [00:18:03] Yeah. I think it goes back to, and I've said it in some of these posts, vendors who reached out to me to try to sell me their project get put on the email blacklist and blocked on the firewall - specifically those who could give less than you know what about what it is that I do and what my day-to-day is and how what they do fits into helping me. 90% of the stuff that I get, and I consider myself a sophisticated buyer, 90% of the stuff I get is completely devoid of any thoughtfulness. There's no effort put into building and understanding what I do and then reflect that back into how a product or service can actually help me accomplish that goal.

> "There's no effort put into building and understanding what I do and then reflect that back into a product or service."

[00:18:48] The vendors who actually care or the ones who get it, and there are many out there who do, they actually spend time learning my industry and they come to me with real examples of how they created value at their customers. They also do important things like show up to events that I'm at. They don't chase me; they find a compelling way to make me find them. But, you know, unfortunately or fortunately, I guess it depends on how you look at it, I might be a harder person to seek and make contact with than perhaps some of my peers or others who really do respond favorably to getting spammed and called 24/7 and love to show up at the booths and get the free squishy or pen or the T-shirt.

[00:19:39] I mean, you know, there's certainly a lot of people who like to do that. And to each their own, they can do it. Again, it comes back to it's very important to me that everything we bring in, everything that we're adding to our environment, which will increase its complexity in some way, it actually helps me deliver care and ensure safe outcomes for our patients. I'll never ever buy a product or spend a dollar or take a pitch from someone who doesn't understand that and a set of products that don't care. It's just not something I'm willing to invest my time in. Because, you know what, every other minute of my day, I could be doing that.

[00:20:25] Ashwin, I have to peel it here. I'm sorry to cut our time short, but I think we're

going to be doing a series of these going forward.

Ashwin Krishnan: [00:20:33] We are, yeah. I appreciate your time. We'll be doing this on a monthly basis. So Taylor, this is the first of many. Again, appreciate it, I'm looking forward to the future conversations.

Taylor Lehmann: [00:20:41] Yeah. Look forward to it.