#133 - The Seesaw of Cyber Recruiting (with Lee Kushner)

[00:00:00]

[00:00:00] **G Mark Hardy:** Hello, and welcome to another episode of CISO Tradecraft. The podcaster provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy, and I'm your host today. And I'll have a special guest on board Lee Kushner, who is an expert on careers in this field, and you got to listen to what he has to say.

But before we do that, a quick message from our sponsor. Risk3Sixty is a cybersecurity technology and consulting firm that works with high growth technology firms to help leaders build, manage, and certify security, privacy, and compliance programs. They publish weekly thought leadership webinars and downloadable resources like budget and assessment templates.

Take a look at some of the great information at risk3sixty.com/resources. [00:01:00] That's risk3sixty.com/resources.

Back to our show, Lee. Welcome. Glad to have you on the CISO Tradecraft podcast.

[00:01:06] **Lee Kushner:** Well, thank you for inviting me.

[00:01:08] **G Mark Hardy:** Now, we've known each other, gee whiz, since the 1990s, which is probably the early pleistocene era of cybersecurity careers.

And so I don't want to assume that my audience has the same background knowledge of, of you and your experience and things like that. So could you tell us a little bit about yourself, like where you came from and how you ended up where you're at now?

[00:01:29] **Lee Kushner:** Well, what a long story. So, I mean, I, I actually have a I was an ex-college baseball player and I have a master's degree in sports marketing of all things.

[00:01:38] **G Mark Hardy:** I noticed that.

[00:01:39] **Lee Kushner:** And after I was working with the Dodgers in Vero Beach, Florida doing spring training, sales and marketing and operations for the team that they used to have down there.

I originally from the New York, New Jersey area, and I came up over a 4th of July weekend to go visit some friends and family. And I was introduced to somebody who had an, who had a [00:02:00] recruitment firm. And the recruitment firm was known for placing IT auditors. And he was getting into this new thing called information security.

Which was supposed to be a first cousin to IT audit, and he says, I want somebody to run that business. He goes, well, hackers, and I said, All right. Well, I went to the New York Library and I just, I mean, there was no Google, I just did all this microfilm research on security and there were articles about digital espionage and all these sort of things.

And I'll never forget, like about a week after I started the job, I got a I think it was a cover of Forbes Magazine and The it was either Forbes or Fortune. It was one of them. But the, the, the cover was called Digital Hitman and Jeff Moss was on the cover and,

I

[00:02:50] **G Mark Hardy:** remember that one.

[00:02:51] **Lee Kushner:** Mike Bednarsik was on the cover.

There were some other guys that were on the cover, and I thought it was like serendipitous that my my grandfather may [00:03:00] rest in peace, went to the dentist, brought me this thing, and I was like, This is pretty cool. And I really kind of got into it. I'd seen the movie War games as a kid. I thought I'm, I'm not computer savvy.

Like, the people that I've worked with in place through the years. But always super fascinated and I think that the thing that really kept me in the industry was the fact that. I really like the culture. I like the people and I like the currency of like, either you are an insider and could be trusted or you weren't.

And while that still exists today, if you go back in the cybersecurity time machine for 30 years, those trust communities were super, super tight back then. The world was a lot less open. And getting included and becoming trusted in a

world where trust was the ultimate currency really was something that I took seriously.

I took it as something that was very [00:04:00] special about this industry and special about the people, and I was fascinated by the different walks of life that people came from that came into cybersecurity or information security. There, there is no, whether it was the government, whether it was the the government people on ir, IRCs hacker cons, phreakers, whatever it was, everybody had a different story.

There was no kind of like pure solution. And I just felt the people were so sincere, passionate and unique about what they were doing. And it really kind of melded with like, I, I would say, for lack of a better term, like how I was raised and the thing that I value. So it was very easy for me.

It wasn't easy for me to be trusted. It wasn't easy for me to go to like Defcon three in a suit and people tug on me and say, are you a Fed? It wasn't easy for me in the beginning at all, but as as you're there and as you build credibility and you [00:05:00] demonstrate to people that You're trying to help them versus trying to profit from them.

I felt that that became it just became very easy to separate from a lot of the others who Just didn't understand the true ethos of what drove cybersecurity professionals into this field and what they valued and, and, and really where their ethics were. And that was, I mean, so that's the foundation.

I started my own business in after spending about two and a half years, three years working for this fella he made a decision to stay with the one client that we were working with. I was getting calls from all these other places because people had left that client, that started going building other things, product services, boutique services.

The industry was growing up. And he made that business decision. I said, okay, well you keep that client. Like, I won't touch them. I'll just go try to like experience the world. And so he got the client and like I went out into the world and [00:06:00] 1999 was when I started my business. And the business started as a contingent search firm.

Really focused a lot on products and services and about I guess about 2010, 2011, we almost became where we were doing about 90% third party products and services. Sales, sales and marketing. Anything in cyber managed services,

the whole thing there. We l we're about 10% end user from like 2011 to the time that I sold the business.

We were probably about 90 to 95% end user. And instead of doing contingent search where contingent search, if someone says, Hey, I'd like you to find me candidate, and we take them, we'll pay you. My firm transitioned in around 2010 to a fully retained model which basically was my firm saying, we are differentiated by our abilities, our understanding of the industry, our candidate relationships, the things that we [00:07:00] know about helping clients build their positions, helping them compensate their positions fairly really trying to build alignment between what their needs were and what they were willing to pay and the appeal of the job in the market.

And working together through that. And my firm's ability to fill jobs very quickly with high quality people separated ourselves. And we worked through that model through 2019 the end of 2019 when I sold the firm to a publicly traded staffing firm of all things in right before the pandemic.

And I spent a couple years working with that firm through the transition period. And right now I've just been on the sidelines thinking about the industry, watching the things that are happening, watching things about the future of work, and thinking about, what. Like what this all means to the cybersecurity professional.

And I just, I, I think it all goes back to like [00:08:00] my roots of saying that I didn't join the industry or I wasn't. I wasn't drawn to the industry because of the customers. I was drawn to the industry because of the professionals. I've always taken a professional first mindset to it. I always thought about if I was the talent, if I was the candidate, how would I want to be treated?

What would I want to know? What kind of transparency would I expect? And it's those things that. Keep me super interested as this industry evolves and, I'm not quite sure if there will be a second act. But if it will be it will be something that will be, trying to make these processes better for the candidates.

That's really I think they're the one, the, the talent is always, the talent is what's in short supply. It's not the opportunities, it's the talent. And for some strange reason, I still don't believe that talent is fairly [00:09:00] represented given how special and rare their skills are. So I, I still think of it that way.

So, a different mark from being at a at a re retained firm, at a retained firm You work where the, the, the better you do for the candidate, the more the client pays

you in a staffing firm, the worse you do for a candidate the better you do for yourself. So it's kind of like, the worlds were very different.

So, it was always better to have our interests aligned with the candidates, even though we were doing a really good job for our clients.

[00:09:33] **G Mark Hardy:** Well, that's a, that's a good differentiation there. I mean, there's a whole bunch of ideas that come to mind. One is, congratulations on beating me to Defcon. My first was Defcon four back in 96, so you were already there ahead of me, and we might have bet there at Defcon back. It's It's possible. I think, well, I might have the wrong day, but the wrong

Did they tear your casino down after the con?

[00:09:52] **Lee Kushner:** Yes, it was the Aladdin.

[00:09:53] **G Mark Hardy:** All right, so that was five I think. Because four was at the

[00:09:58] **Lee Kushner:** Well, I,

[00:09:59] **G Mark Hardy:** brand new one. In [00:10:00] fact, they, they built that one. I've drawn a blank brand, treasure Island. And then once they realized who Defcon Communications were, they tried to weasel out of the contract, but they had to do it.

[00:10:08] **Lee Kushner:** I, I'm, whatever, I think it was 90. I remember having to petition my boss to say, I have to be at this conference.

[00:10:15] **G Mark Hardy:** got to go to Vegas

[00:10:16] **Lee Kushner:** It was 97. It was 97, so whatever that,

[00:10:19] **G Mark Hardy:** Edmond Defcon

[00:10:20] **Lee Kushner:** whatever that was, that was it. And then Black Hat won shortly, followed that a couple years later.

[00:10:25] **G Mark Hardy:** Yeah. Cause I remember I worked with Jeff Moss at Secure Computing Corporation. We came up with the idea, Hey, let's, let's do Black Hat because the suits. Would pay real money for what all of us get. And

back then, I remember Defcon was 40 bucks and 35 if you mailed a check in in advance. And of course things start out that boom, you never know how big they're going to get.

But the other thing that I really resonated with me was how you perceive your role and who your true customer is. Because in any staffing environment or hiring decision, there's always two parties and, and often we sometimes think of ourselves at odds with each other. And other times you look [00:11:00] at it as being cooperative, but at the end of the day, You interpret your role as being the person who's going to represent the candidate.

I'm going to get the best possible opportunity for this individual. I'm going to help them find a job that matches their skills, their talents, their interests, and also provides a compensation that's going to work. I mean, you can't pay them too much cause otherwise the first. They get their, they lose their job.

But if they're successful, then you've got potentially a repeat candidate where if they come back to you in a few years and they said, Hey Lee, I'm, I'm ready to move on. You helped me the last time. So does that happen?

[00:11:36] **Lee Kushner:** So, so it's, it's, it's like that. But maybe let me kind of. Maybe pull the cover back a little bit. Right. I mean, so I mean, I used to do a talk with Lenny Zeltzer and we, we, we did this talk called Lenny's Fantastic. And really bright security professional and like, Super interested in careers and which is was great.

And we would talk about [00:12:00] like, the seesaw or like the concept of being on the other side of the desk, right? That there are always two parties to a hiring process and it, it's kind of like, The seesaw. If one party is too powerful than the other, the Seesaw tilts in a bad way. I always looked at my role in the research process as the person who leveled the seesaw and kept the seesaw leveled throughout the entire time.

Because normally when that happens, the parties find that there is synergy. And it normally lends to like good outcomes. But like when it comes down to like, I mean, In fairness, right? Like in any search, right? The client is the one that is making the rules. The client says, well, I want the person here.

I want this skill. They're going to report there, whatever the things that, so the client is allowed to make whatever decisions that they want to, right? We got the client as to what was possible, right? But when you then bring the person there,

right, like you bring the [00:13:00] person there, then you know you're advocating.

The goal is to have the client have some significant choices and for the client to understand the value of the candidate based upon the credentials they have already determined, and then to make sure they're not taken. And then, and then my job is to make sure that they're not taken advantage of.

My job is to like, to make sure that like the client is The candidate is protected because in the end of the day, right, like we're all employees at will mostly, right? And so just because somebody hire, like I could tell you horror stories from like the early, the mid, the late nineties as to what I've experienced.

But I experienced clients that would hire somebody. And then after, like right before a guarantee period, they would figure out that they could hire one of their friends to take the same job. They would fire, our candidate or the person they took, and they would then have the job filled very [00:14:00] quickly because they didn't have to pay the fee.

And there was just look at the saving of money, right? And why you learn over the course of time. And as I became more and more involved understanding that our value to our clients was more of a consultant on staffing and talent issues versus a mechanism or a machine to quote unquote produce resumes.

That was something where, we would screen our clients out and basically say, look, if you want that, we're not your firm. If you want to judge us by how many resumes we produce versus how accurate we are, like, I'm like, we always would say in my office, say that you don't pay for the, I said, you pay for our cutting room floor.

And they're like, well, what do you mean by that? I said, you pay for the people we discard so you don't have to spend your time. You pay for our screening process based upon what you've put together. Because in the end of the day, you only have a certain amount of [00:15:00] time and I'm selling you your time back.

And. I think that most people understand that equation, especially in the security profession when they know that like interviewing is one of the few things that you can spend so much time with and get no yield. You can absolutely have no yield for all your effort and there's nothing worse to know that you can never get that time back because that's time that people can spend with their families to

solve problems, to be with their, I mean, to whatever it might be, to work on their health, whatever it might be.

So like, we are in that business of not a hundred percent, but and, and our ultimate success is not the candidate who gets placed and then we place them again. That would almost be bad, right? Our number one is that we place somebody and they become so good that they hire five or six people from us, and then they're just like, look, I'm now the director.

I'm now the BISO. I'm now the CISO. I'm now the head of security architecture. I need six more people like me. [00:16:00] That was the ultimate success for us.

[00:16:02] **G Mark Hardy:** And that again sounds like a very different view from the other side of the table because oftentimes so, so for me, in the leadership management role, when we're going out to recruiting, there's those who don't understand it. Say, well, why do I have to pay 20, 25, 30% of whatever to this other one? We can just go ahead and run a monster.com ad.

Well, as you had indicated, yeah, you could run an open ad like that, you might get a hundred responses. Do you have time to interview a hundred people? And if you go through an organization from, with your experience now, you've seen an off lot. I remember coming to you a long time ago, so that was back in 2001 when I was offered to go run the Wall Street security practice for Ernst and Young.

And at the time, I, I knew what I was making and I was looking to say, Hey, is there something else that is this offer should be about here or here. And you're saying like, no, they're, they're big. I think six, five and a half, wherever they were back then, they're in New [00:17:00] York. This is your ask.

And I'm like, really? Okay. So I went in and said, this is my ask. And they said, okay. I. Now it wasn't okay. Like it was a laydown. It was well that was at the very top end, but you already knew from your experience how to better represent. Cause if I came in too cheap, let's face it, if you go to a, a, a wine store and you say, I need a nice bottle of wine, but I don't know a lot about wine, but I'm trying to impress somebody, would you go for a $40 bottle of wine or a $4 bottle of wine?

Even if that one here is spectacular, you, you'd never know it by the cover. So as you represent people and you help them, Fit into the market, both from the skillset, corporate fit, and then financial. How do you overcome things such as

people who really are good at what they do? But let's face it in our line of work, not everybody has a degree.

Not everybody has advanced degree, and yet they might be in the job description almost all the time. How do you help bridge that gap?

[00:17:58] **Lee Kushner:** Okay, well that's, [00:18:00] I mean, that's a very fair question. So if you go back into the time machine, like in the nineties, late nineties, mid nineties, late nineties, early aughts degrees were super important. And what a lot of companies didn't understand is that some of the best cybersecurity professional they could have taught the classes in college.

So like, it wasn't like, you weren't going to teach really bright security people on how, Linux and Unix really works because they know how it works, because they know how to take it apart. They're not, they at those times, they weren't going to learn that in those schools unless they were going to like very advanced CS programs.

Right? So, People didn't understand that. So I, I always looked at, my job as a level of education of like what the market truly is. So it would start with something like degrees, right? And then you would counsel a client and say like, look, how important is it? Like, and just tell me why it's important and if it was important because of.[00:19:00]

A cultural thing, we would just say, okay, well that's the search and that's a non-starter. You've set that rule. If you say, Hey, look, you're open to it under certain stipulations. Okay, let's talk about what they are. So, that's when you know that's the difference between working with. Somebody in executive search that knows an industry and that understands the composition of the industry versus when somebody says, well, like, just give me a job order and I'll fill what you can because you could push back like as we progressed.

Right? And this is something that I think is very, very relevant today. Because there's a lot of great look, the amount of like females and underrepresented populations in the market. Now as cybersecurity professionals is significantly different than it was 25 years ago. However, it still probably represents somewhere between 10 and 15% of the [00:20:00] overall census of security, and a lot of that 15% is not necessarily in the highly technical areas.

So if you put in compliance and risk, you probably of that 15%, you probably have more, 75 or 80% of that 15% are in like risk or non-super technical

professions, and you have a much smaller in engineering. So if a client would come to us and say like, we really would like an underrepresented. Population.

We could say like, look, we could build a diverse candidate pool, but we're not going to be able to promise those things because they just don't exist and they exist in balance. And I think that a lot of people, there are a lot of organizations that have taken security because it's an area of growth and because there's definitely an overall kind of an understaffed nature of cyber.

Talent and in cyber organizations, what they've basically said is that this would be [00:21:00] a very good place to kind of balance out or add to create a more diverse and equitable workforce or inclusive workforce. That said They're making a already difficult problem, more difficult. And if you really wanted to solve that problem, we need to go back to the high schools and we need to have more girls who code, like my son who's a coder and he's in Python and he's doing his stuff and like in addition to other things, but he said to me, he goes, dad, why?

Why is there a girls who code? Why is there no boys who code? I said, Brody, I said, There's a lot of boys who code and it's disproportionate to the math I said, and look around your math classes. Look around your computer science classes. What's the population of females? So I think that that's the thing that has to happen and companies want to fix that right now.

And a lot of times that's becomes an unfixable problem. And [00:22:00] recruitment firms that aren't really, that if you're not, don't really know the industry or the industry composition and you don't have a very even relationship with your customers. You can't tell them, Hey, look, your design is bad. Or this is what your design is going to yield.

And we could do it everything your way, but like, there's a lot of things right now where people are saying, well, you don't need technical people to do security work, and we should be hiring less technical people because there's enough opportunities for non-technical people to be security folks.

I'm not going to disagree that there are probably some jobs that you don't need to do a lot of technology in the job. Like you could be very good at awareness, you could be very good at policy, you could be good at a lot of different things. There's your the, there's your assistant. I see. But while that's the case, when it comes down to like very difficult engineering tasks or solving technical problems or protecting somebody's [00:23:00] environment.

Understanding the underpinnings of how computers work and being able to code and write scripts and do what's necessary to protect applications and to protect networks. Those are technical issues. And if we believe that we're going to solve a problem by under hiring or under skilling for roles, roles quite frankly, it's going to just create more problems in the future.

But, I, I, I think what it comes down to is that it's. When you're trying to solve a people issue, which is very much a moving target, right? And you're dealing with a lot of variables. Understanding the bigger data sets and understanding like who these roles appeal to, who you might be able to attract, what might be the roadblocks, how you have to design your roles.

That's really where the value of a search firm would come in. And that's why I think now there's a lot of. There are tons of firms now that are saying, oh, [00:24:00] we do cyber. We do cyber because it's hot, it's new. There's a big difference between the people who are newer to the profession who do cyber versus people who've actually taken time to learn about the profession and.

The recruit, the cybersecurity professionals are super bright and they're super intelligent and they could sniff charlatans coming from all sorts of, miles away. So it's just one of those things is that, one of the things my firm was able to do, and my team was able to do really well because they understood the industry and cause they took the time to try to get it was to be able to was to be able to, be able to mobilize a highly qualified workforce fairly quickly because they understood that value, right?

And they understood how to present that value. And, to your point before about, your experience Candidates [00:25:00] have to understand their value in a fair way, and they should spend some time. Every cybersecurity professional should try to figure out what their most valuable skills are, why they're valuable, to whom they're valuable, and like what those skills might then, morph into as the industry evolves.

[00:25:25] **G Mark Hardy:** And, and that's really kind of a long-term career growth because when I started doing this, there really was no career. And when I told people I'm going to go do computer security, which later became infosec, and now it's cybersecurity and who knows what'll be next time. But it was like, you can't make a living out of that.

And I said, well, just watch me. It's going to take a while. And it's like going, Hey, it's 1822, I'm going to go to California and look for gold if I live long enough. I'll find it in 1849. But for the folks coming in today into the career,

there's a couple things they're looking at. One is of course the first question for a lot of people, how do I get started?

Getting that first job is [00:26:00] tough when your, your resume consists of, well, I had a paper route. I don't even know if kids do paper routes anymore. I worked at the food service at college. I, I. Whatever it was, and that's not really work experience or let's get 22 or so coming out of college or even let's, if, let's say you've been working in a non-degree area, but you still got some experience, then you also got people who, let's say, do a term.

Of duty in the military did four years or six years, and they come out and then there's a translation of how do we take this military terminology and responsibilities and map it so that a hiring manager or an HR person gets it? Because if they don't have a military background, they're not going to understand what the responsibilities are.

And then lastly, how do they position themselves for expectations that if I'm starting out in this area, What kind of money am I looking at? And again, this is theoretical because I'm not asking you to help me find a job. But for somebody starting out, what are some of the reality checks in there? And are they going to be able to pay off the student loans that they've picked up getting a [00:27:00] cybersecurity degree in a reasonable period of time?

And if so, that's kind of a good reason to take on debt because it's sort of like a mortgage on your professional career, which once you pay it off, you get to enjoy the benefits for the rest of your life.

[00:27:14] **Lee Kushner:** Yeah. I mean that's, that's a lot to unpack, but I, I think that that is a really, That in itself is a very good starting point, right? I have a 15 year old and a, a four-year-old, so it's different conversations, but like, I'm always talking to my 15 year old about making choices and that down the road that those choices are going to matter at some point.

And I think that when you start talking to young people, right? I mean, one of the first choices I always say like, is your kid a video game player? Are they a video game builder? Because we have a lot of video game players, we don't have a lot of video game builders, right? So, I, I, I think about that, right?

And I think about how easy it is to play a video game and how hard it would be to even create the simplest video game, whether it was a mind sweeper or, [00:28:00] checkers or, some sort of if then program or whatever it might be. So, I, I think about like what goes in, right, and, and I think that, the one

shortage that comes across the board, or the one common denominator that will exist in careers now, 10 years from now, 20 years from now, is going to be a technical foundation.

Which is probably more important than a course of study. So when I say a course of study, like there's a lot of kids that have cybersecurity degrees but have not taken any cybersecurity. They have no coding. There's no programming. There's no networking, there's no lab, there's none of that. Right.

And I remember some of the brightest young people that I placed that they were like non-technical majors, but they worked in the computer lab. They, did you know they did capture the flags? They like on their own, like, Say, look, I've been studying, I've been studying Python for two years.

I can do [00:29:00] certain things. I have to get paid, whatever it is, right? So it's all those things that are completely available that don't necessarily have to map to like a traditional course of study. So like you don't have to be a computer scientist. However, the entry level things that everybody needs somebody to do is like, How the computers talk to each other, make the software work.

How are we reporting? Like, what are we looking for in an, in an iso, right? What are so, so you have all these things that are there. There's some basic technical things that not everybody has. So that's your differentiator to start. I think that anybody who doesn't have like a differentiator, if you go to a career fair and you see all the kids that are running around with marketing degrees, right?

And then you see all the kids that are running around with. CS degrees or like who have, who are in the computer club or are doing the things that whatever it might be like in [00:30:00] those worlds of technology. Like those are the ones that are attractive. Like in, in like, Going back to me, I worked in sports.

I love working in sports, but I realized very quickly there were a million people who wanted to work in sports and there were not many like, and unless I became the GM of the Dodgers, it wasn't going to work out for me, or I was going to become the head of scouting at some point. So when I realized that that was a journey that might be super crowded, I said like, look, let me go try to do something that nobody else is doing.

Let me try to learn something about it. Right? And that's just my story. But I challenge people that if you have true technical skills to lead with that, and that

in itself creates value because that is where it's shorter supply, higher demand. We don't need tons of kids running around with marketing degrees.

We don't need tons of kids who are video game players. We need kids who are video game builders. So I think that's kind of where it starts. So I get a lot of calls from [00:31:00] parents, kids have graduated, I don't know what to do. I heard you do what? Cybersecurity. That would be a good thing. So I get on the phone with the kid and say, Hey, like tell me about the last time you coded something.

Like, I don't do that. I'm like, well, would you be interested in teaching yourself that? No, that's too hard. Okay, next career. How about sales? Right? So. I, I, I think that people have to understand that, right? They have to start building skills where the value is the skill and the supply of the skill is short, and the demand of the skill is high.

And once you do that, you start creating a level of value. And then once you get in doing technical work, you could apply that technical work to security challenges. You can always go to the security team, say, look, I'm in, computer support, or I'm in, I'm a sysadmin I'm in a I'm in CI/CD kind of role or whatever it is, but I'm really interested in security.

Do you guys have any extra work that I can, like, sorry, I've never met a [00:32:00] security apartment that doesn't have extra work, and I've never met a security apartment to tell somebody like, Well, your technical skills are too strong to work here in security. So I mean, there are plenty of roles, application development, infrastructure, whatever it be where you could actually liaise with the security team.

And that's another good way to kind of get in. And internal postings are fantastic. So like, you could create that value like When I was old, when I was younger, and I was starting people to come up to say, well, what do you want to be? And, and, and this older fellow would say, it's not, what do you want to be?

It's what, how, what do you want to become and how do you want to become what that is? Right? So becoming right, not to use a Michelle Obama term, but becoming right is really the journey that you're taking yourself. And, and, and you need to ask yourself, if I invest my time, What might be the logical outcome and is that an outcome that I, I'd like and that outcome might not come right?

But if it's a [00:33:00] logical outcome, right, you're able to expect some. Typical results for typical effort. And when you start increasing that effort, then

you are able to expect some additional results for that additional effort. So that's kind of how I answer that question to young people, because there are plenty of ways to become involved in cybersecurity.

Some of them are traditional, some of them are atypical. Go to a cybersecurity meetup, go to a 2,600 meeting. I know they still exist. Go to an OWASP meeting, go to go to a B Sides. Right. Just. Getting to know things. Go to SchmooCon, like whatever it is, figure it out. We, we just saw each other at Thought Con.

Come there, you're going to meet people, you're going to see people. You're going to learn something and you're going to talk to people. And you got to learn that. That's part of it. So, I mean, those are the things that I would say. And once you get in the foot in the door, then the world's much easier because you start building a reputation and credibility.

[00:34:00] You start building real skill. You can talk about solving real problems, and then the world kind of opens up more.

[00:34:06] **G Mark Hardy:** Yeah. And I think that's a good point. I, I talked to a young man a couple weeks ago, just got his bachelor's degree in cybersecurity. Just you're talking about technology. And I said, okay, let me just open up with a couple simple questions like, well, how many bites in the TCP header? What's the TCP header?

Okay, what layer is tcp? What are the layers? What's the name of the model? And he, he didn't know any of this. And I'm thinking but you have a degree in cybersecurity. Yes. And I said, and with all due respect, I don't think you got very good value for your money. And he said, oh, it was all a scholarship was paid for.

I didn't have to pay for it. And I said, then you got your money's worth, which is basically nothing. And I had interviewed a, a lady. Couple years ago who had her master's degree with honors, and again, had no idea what the OSI stack was like, had no idea how networking worked, how protocol headers, and, and these are not down into the weeds, and I'm not interviewing a CISO because typically at a CISO [00:35:00] level, these are things that probably were in your background at some point.

But definitely when you're coming in at a manager level or a technical level, you should have some inkling of what's going on. Behind the, that curtain or inside the wire. But if you had mentioned Thought Con, I really enjoyed the talk

that you gave at Thought Con and, and we're discussing that before the show, how it's kind of nice sometimes to, to have a non attribution environment where you can speculate on things.

And if you come up with ideas that are a bit radical, then so what? Because you can. Banded them around over a beer. But things that are on the record, so to speak like this, we are going to stay a little bit closer to home. Which makes good sense because the last thing we want to do is give somebody just enough information to make a mistake with, they have to really have enough information to make an educated decision.

So a couple kind of predictions. Where do you see the cyber? Security career path going in the next few years? Are we going to be overcome by generative ai and all our jobs are going to [00:36:00] be sitting there on the sidelines watching it? Are we going to have a greater requirement for security? It's going to be more management versus technical.

And then how do CISOs and other security leaders position both themselves and their workforce for this future world?

[00:36:15] **Lee Kushner:** I mean that. That's a, that's a podcast in itself. Put alone part

[00:36:18] **G Mark Hardy:** we have six minutes. Let's go.

[00:36:20] **Lee Kushner:** Well, look, I, so here's, I mean, I think, to answer your question, the best part about cybersecurity is that when I started recruiting, like if I found somebody with some firewall experience, that was a big deal. If somebody had ever done a penetration test on a network that was huge, right?

Or they run a Nmap scanner, that was a big deal, right? So, The best part of security is the technology keeps evolving and every new technology, whether it's cloud or AI or what a edge, what iot, there's always going to create more security concerns. So I don't think that we're running out of problems to solve and I don't think we're ever going to run out of problems to solve, right?

So normally security lags [00:37:00] technology by anywhere between 18 months and two years. It's probably getting a little bit closer, but. That's kind of where we're going. Right? So number one number two is that I think that companies are, they're spending a lot of money on their managers and their leaders.

And they have higher expectations for their managers and leaders that are becoming more in line with their expectations for manager and leaders in other disciplines. What. The one thing I will say, and it kind of dovetails into the thought con talk, right? Is that like the, the number that I don't necessarily agree with, but it's the one that all the media outlets pick up.

As they say, there's 3.4 million unfilled cybersecurity positions worldwide, and there's 750,000 openings, current openings in the United States and cybersecurity. Okay? If the numbers were half that or a quarter of that, it would still be a lot. fact is, is that those positions that are open, they're open because there's [00:38:00] technical void, there's open because there's lack of technical competency, and there's open because there is a dearth of people who truly understand how to solve cybersecurity issues.

And the reason they're not many entry level jobs purely in cybersecurity is because cybersecurity. Is really a combination of a lot of skills. It's a mindset, it's engineering, it's working with other people. It's kind of a glue to the organization. It's understanding risk. There's so many components of that role that you know, quite frankly, it's the people that have those skills that are super high demand.

And it's the ones that are open, right? So you are going to see cybersecurity becoming more and more like structured functions within corporations, but you are going to see the gap in technical people continue to grow because we're just not producing people fast enough. And I think that [00:39:00] really brings an interesting, like, it's an interesting like, Question, which I'm not sure is ready to be answered yet, but you know, do those super technical people who are in such short supply and high demand ever receive fair value?

Because I would argue that it's easier to find qualified security leaders and managers than it is to find a highly skilled security architect in any of the variable discipline, the disciplines application, network and for cloud, whatever it might be, web, anything, that it would be much harder to find somebody with that blend of technical depth and understanding in these sub domains than it is to find the person.

Who can understand the umbrella. So the specialist is always more, and that's at all different levels of specialists, right? And if you are a big pharmaceutical company, you want to build new [00:40:00] drugs, you don't want to have recurring cybersecurity costs. You want to just know it's dealt with and the regulators are fine and you're not act and everything's good.

Well, you have managers for that. I don't know if people are going to feel that the value proposition for working in corporations is going to be truly fair, especially with like remote work and with these layoffs that are happening and then people being overpaid in a reset of the market. Like, there's a lot there.

And I'm not sure where it goes. But I don't believe the four point, I don't believe the 3.4 million number. It's nice to keep it, having said, but I, I, I really worry that we're creating like a system that just becomes super unfair. To the people who skills are truly valued and don't want to be managers.

They just want to do great cybersecurity. And I don't think that our HR structures that [00:41:00] exist in most corporations enable that or allow for that. And I think that's where we're going to start seeing some real friction in the in the future. But It's, you're, you're never going to lose by investing in your career as a cybersecurity professional, but invest in the technical skills to start.

If you could do that, people will listen to you a lot more. If not, you just kind of have an opinion.

[00:41:24] **G Mark Hardy:** Well, that's some very good insight. I think some of the best stuff in the show are the last five or six minutes of there where I'm thinking, I'm going to replay this myself because you've got a lot of wisdom there, but you've been doing this. For about a quarter of a century, a tremendous amount of gain knowledge.

Just a handful of people that were doing what you were doing back in the nineties are still in the game, and as a result, the insights that you have are incredibly valuable. Now, you said you'd sold your company, you're off kind of, doing stuff. If people had more questions, if they wanted to get in touch with you, they said, Hey, this Lee guy looks interesting, but G Mark didn't ask a question.

I really wanted answered. Is there a way that they should get in touch with you? Do you want them to come through me? [00:42:00] Contact you directly? What's the best way to do that?

[00:42:02] **Lee Kushner:** Well, I mean, the only really external presence I have is my LinkedIn.

[00:42:05] **G Mark Hardy:** And LinkedIn works well.

[00:42:07] **Lee Kushner:** Lee Kushner, that's, I mean, and I'm, I would say, I wouldn't say I'm an open networker, but like, if you're in the world of security, I'm a networker, so that's fine. You reference, you heard the podcast, it's perfect. If they have questions, I want to direct them to you and you want to forward them to me and you think it would be good for another follow-up podcast that made some sense.

I'd be happy to do that. I used to do this thing where we would kind of do it like a Dear Abbey. I called Career Advice Tuesday, where we would just answer a career question that we got and make it publicly available. And that might come back at some point in time. But yeah, I mean this world's ever changing and I really hope that, I hope that, I just hope that people feel that they're treated fairly by their employers.

I think that like, They are the talent. They should always remember that in the end, you can't replicate talent and you definitely can't replicate great talent. So, yeah, I appreciate you having me on. This has been a blast. It was so [00:43:00] cool to kind of reconnect with you, like, yeah, we know each other, I guess we're old 25 years or so.

And it's. It's interesting to see the next generation kind of come up or to just just to continue to be involved or see like how wonderful this industry has become. And I'm still amazed by the people. And I'm amazed by the passion that people have for their craft. And that's just, it's still wonderful.

So.

[00:43:23] **G Mark Hardy:** you for being a part of it and actually helping to build it. So we're out of time, but I want to thank you again, Lee Kushner, for being part of our show here at CISO. Tradecraft. I'm your host, G Mark. Hardy. If you're following us on LinkedIn, please continue to do so. Or if you're not, That's a good place to find us.

Please subscribe on our YouTube channel or follow us on any number of podcast channels that are out there. We want to make this information available to as many cybersecurity professionals as possible to help you and them in their careers. So thank you for listening, and until next time, stay safe out there.