uberknowledge

Chad Holmes, Optiv

Supporting and Educating CISOs

Ashwin Krishnan: [00:00:02] So welcome, this is day one for me at Black Hat, and with me I have Chad Holmes. I'm going to do a quick intro and this is going to sound a little bit over the top but it is over the top because he has achieved a lot at a young age. He has been feted as one of Business Magazine's 40 under 40. He's been educated at the Harvard School of Business and has a philanthropic bent which is really interesting, I want to dig into that a little bit. He's bonded with the Boy Scouts, mentors young entrepreneurs, and is an advisory board member for the North Texas Crime Commission. So, with that intro, Chad, we're here at Black Hat and we were chatting just before the official recording of the podcast about what brought you into cybersecurity and how your journey evolved over these many years, and why has it come to Optiv at this stage?

Chad Holmes: [00:00:54] Yeah, it's a great question. I would say cybersecurity has been a passion my whole life. I've been focused on how to make a big difference with organizations and I started, it's funny, I started my career in building architecture. My Dad was a general contractor, and then I went and was an architect. Then I started managing and owning different systems from an I.T. perspective. And it was years and years ago, 20+ years ago, I started working for an organization where I started taking over some of their I.T. infrastructure and I realized there's a huge gap around cyber and it's early stages, right? At this point security was really just how to manipulate different processes and hack in and exploit vulnerabilities. So, what I started to do, is probably spend a third of my life in, really, security operations. Helping organizations and on the ground every day working from finance to healthcare to other organizations as a CISO, trying to help that organization secure themselves from all the threat actors at

the time. Through my career I started realizing that, yes, I'm influencing that individual organization but there's an opportunity to influence a whole market.

Ashwin Krishnan: [00:02:00] Yeah.

Chad Holmes: [00:02:00] So, I made a transition of going from operations to actually working for product vendors. OEMs, you know, if it's Intel or Checkpoint or Core or McAfee. Finally, I ended up as the CTO at FireEye and really helping organizations develop products to address some of the major market issues that we're running into. Then going through that exercise and really helping organizations out from a development innovation perspective. I started realizing something really quickly, probably the last three or four years, and that there's tons of different investments going into Cyber because we're trying to solve the big cyber issues that nobody can solve. So, tons of investments, tons of new startups, tons of new vendors coming out, and what we started doing is the race to the market. Who can race out to the market fastest, who can put the most marketing budget around it to drive a new buzz word to the market? Now it became less about providing an outcome or a value to our clients than it was just driving market price.

Ashwin Krishnan: [00:03:05] So, let me interject a little bit over that. Did you realize this while sitting at a vendor or was this realization after you stepped out?

Chad Holmes: [00:03:15] No, it was definitely when I was working at a vendor. As you know, I started working with clients and we were creating new industries, creating solutions to their problems. But it was an isolated problem. We started running into different competitors in the space. So, it really wasn't competitors, it was more market competitors. It was more marchitecture and we were like, they are not really a competitor. So then, I started seeing the collapsing of the market a little bit. And then you started seeing organizations lack of going IPO and start doing consolidation. So then I was like, well I still want to help organizations solve some of the biggest challenges, how do I do that in a larger industry? Well, maybe not be focused on the individual product.

So that's when I kind of jumped out and started doing consulting work, large-scale consulting work. I went over to Ernst & Young and was running their cybersecurity practice for a long time. Then recently I made that transition to the Chief Services Operations Officer at Optiv, and it really blends both my operational background, my product world, OEM space, and my consulting world into one company and really can drive a larger outcome or a larger solution for a customer on both sides of the world.

Ashwin Krishnan: [00:04:27] Got it. I mean that's great. The capture of your journey and where you've got to. So, a few questions. Forgive me, I haven't even got to the show floor, I'm not even sure I want to go to the show floor, but if you were to say, what's one of the most under-hyped security issues that should be getting attention, but is not?

Chad Holmes: [00:04:49] You know, I have a very interesting spin to it because I would say we're not spending a lot of investment in VC funding right now, and we're underestimating the impact it does have on our security posture for most organizations. Probably the under-hyped one I'm really focused on is, as organizations go through a business transformation they're seeing this major movement around new innovative companies - like Tesla putting a strain on the automotive industry - and they have to rethink their business strategy, right? You're seeing organizations transform, and when they start transforming their business models it starts putting more pressure on the security industry and the security buyer. We're actually seeing a growth, about 40% of security spend not being dictated by the CISO anymore. What does that mean? That means you have different personas, digital officers, risk officers, assurance, cyber-resilience people influencing organizational security budget.

Why does this go to the question you asked? Where I see that we're understating certain areas is, really people are creating 4, 5, 6,000 chatbots to automate some people's action to get that return on their investment. But who is building the security for digital? Who is managing that security element through

that entire life cycle? Yes, we're doing some desktop stuff, we're doing some apptech stuff, some are doing some red teaming and A&P work, we're doing some other strategy work associated with it. But imagine if you have 20,000 chatbots running around, doing different things, taking action, how are you managing that? We talk about compromise and organization and doing lateral spread, and a hacker comes in, he's trying to get lateral, he's trying to get data. Well, with organizations very mature around using robotics, is that an avenue that they would go after?

Ashwin Krishnan: [00:06:48] Right.

Chad Holmes: [00:06:48] Can they lateral spread faster? Do they have different chain instructions or automated playbooks, digital playbooks, that could take action maliciously for them? So, we get to really up our knowledge around what that new vector looks like, as an organization. Instead of just, you know, all the different campaigns and crypto-aware and all those different things. Ransomware is important. But insider threat is now a new vision of insider threat, because it's not an individual as much as it could be a computer.

Ashwin Krishnan: [00:07:21] So, this is a very interesting conversation because it also leads into two things. One is the cyber skills gap that is getting exacerbated. But what you're talking about, you mentioned CISOs and security architects need to be retrained as well, in terms of needing to broaden their scope of what the attack surface is. Especially in non-traditional tech industries, whether or not things like industrial IoT and other kinds of sensor devices, where does that knowledge come from?... First of all, they need to understand this is a security issue, second, like you said, being aware of what the components are inside a robotic arm and being able to see whether the software itself is hardened? Is it even practical to say we need to do it from ground up, and where do you get the skills for that?

Chad Holmes: [00:08:17] That's a great question. I think it's a fundamental shift in how the market looks at it too, because if you look at the spend ratio it's drying

up a little bit for the CISO. But why is that? Why is the CISO still not the head leader for all things cyber? And I think a lot of it is to your point around talent. You look at talent and it becomes, historically our CISOs have been very much a technologist, a focused technician, they're technical individuals, but now security is a business challenge. How do they go from a technician to a business person? Because what we're seeing is the CEOs and the boards losing confidence in the CISOs. And that's why they're giving the risk officers, internal officers, or other people domain focus saying, "Hey you can take ownership of the cyber element for our business. Right?" So, it's more of, yes we have a talent challenge, yes we have a talent shortage, but we also have an educational shortage. How to make that transfer from technical to business. I can tell you, through my career, my life, my career path, that's probably the largest challenge I ran into, because you don't want to give up that technical knowledge because you feel you're not relevant anymore.

Ashwin Krishnan: [00:09:31] Right.

Chad Holmes: [00:09:31] But there are so many different aspects of what relevancy really looks like. So yes, you want to be technical at a certain level. Can you keep up with all the trends? No. And still maintain a business presence and understand the business challenges? It's almost impossible. So, we have to really take a look at how we organize security in a way to maintain both sides of the fence. But it goes back to my original question. Look at how I.T. has done it. In the last couple of years, I.T.'s gone from enterprise workforce I.T. CIO to industrializing the shadow I.T. organization to make them the digital officer, or the CMOs, or the digital officer, or branch of the CIO. What they've done is they've separated the roles a little bit. If you look at the bigger international, a CISO role has been separated, they'll have a business CISO, or a line-of-business CISO, or a big corporate CISO, so they have different levels. But I think that separation or bifurcation of the two different structures is important for us to be successful.

Ashwin Krishnan: [00:10:34] So that actually leads into another question, which is advice for fellow CISOs. I think you touched upon the technical talent that you have, knowledge that you have is critical and important, but if it comes at the expense of understanding where the business is going and how they need to be educated, then you're probably on the losing side. But the other thing you mentioned is this bifurcation, so are there other choices that CISOs would have to make going forward? Like which line do you want to be - number one. And number two, if you're incapable of transitioning into that business-focused mindset, is this even a job for you? Is that conversation happening in CISO circles?

Chad Holmes: [00:11:16] I would say there is a lot of mentoring going on. If you look at some of the bigger organizations, mature organizations, that have the big time CISOs, the guys that have been there, made that transition, understand the complexity of that transition, are having conversations about how to do that. Now is it a mainstream topic that we talk about? We talk about talent shortage in cyber, but most of that is the technical capabilities and that the domain and the attack surface are growing faster than we can keep up with. But we don't spend a lot of time to talk about how to transform the CISOs. Even when I was at EY, we spent a lot of time of building educational systems on the career path, and I'm doing it at Optiv also. How to transform the technical technologists into more of a business technologist. And I think that's really critical as you look at career growth opportunities. We got a new age of millennials coming in. You get new people coming in and they behave differently. We have to take that into consideration: the gig economy approach. So, you get a gig economy, new millennials coming in and we still struggle with the transference of technical to business. We have to eventually overcome that or what we're going to collapse on ourselves.

Ashwin Krishnan: [00:12:34] That's a great lead into my next question, which is advice for vendors. As we talked about earlier, having come from the vendor side and you as well, I do feel for them - just in terms of being able to connect with the CISOs - but is there opportunity for them to step up and start helping the

CISOs get to this business-focused mindset. Is there a vendor play, where you're no longer trying to outmarket each other? I have this analogy, at the #RSA conference I was talking to Giovanni at Lastline and he made this amazing analogy that stuck in my head: how a CISO's job is like a goalkeeper in soccer. If the score is 0-0 you're not feted. They don't lift you up and say "Yeah, yeah!" But if you're 0-2, you're out. So is that a vehicle for a vendor to come in and say, "Hey, 0-0 took x amount of shots against the goal and he or she saved every one of them." From a vendor perspective, could they actually step in and start helping the CISOs bridge that gap, or is it purely a fight that the CISO has to do him or herself?

Chad Holmes: [00:13:47] Well, I would say historically, I've seen trends. I mean if you've been in this trade long enough, you've seen trends of the I.T. side going from green screens to a more client base to cloud, and now we're coming back to green screens model, right? I use the analogy because I think security is doing something similar. Five to seven years ago, when I was at McAfee, we talked about going to platform plays, and how to bring platforms and be more holistic for our clients. We looked at data exchange layers and how to exchange and communicate different platforms in an ecosystem. Now with the rise of orchestration automation interconnecting those technologies to drive a better outcome, it is something the CISOs and teams are pushing. So yes, we have the marketing teams and everybody, especially for a startup, is trying to get mindshare and they're trying to get the next cool widget to drive that.

I would say most of the vendors now, the more mature vendors now, are really thinking about how to solve for that outcome, how to try to quit because I think really the CISOs are forcing the conversation, they're saying, "Guys, I can't." I think there's an average of over 100 vendors a CISO has to operate. They're like, "Well, the spin is going to dry up, the talent doesn't exist, I can't manage it. So, what I'm doing is having all of these consultants come in - yay for the consultants - to help me manage my day-to-day operations." Now you have organizations and CISOs saying that's their business model. They're really third-party risk management. Then they are really managing the security of the organization.

When you start looking in it, I would say the vendors are trying to come together in certain areas in their domain to try to provide a larger outcome. At the end of the day though, are they really? You know that's the question because of how much effort they really are putting towards it. They still have to drive a product release, they still have to drive innovation, they still have to drive market share adoption.

There are lines of friendly fire. But when it comes in a day, you know coaching their marketing teams has to become really important. They may believe that, and believe it into their culture, but they don't educate their marketing teams and marketing teams go to market a different way. Then you have what we see at #RSAC, we see it all the big conferences, Black Hat, where everybody seems to be delivering the same message.

Chad Holmes: [00:16:11] It's like, "OK, I know for a fact you do not do that, you do not do artificial intelligence (AI). So why even put that on a slick? What does that really mean to you?" Well, it means something different to everybody. So, my advice to the vendors is continue to evolve, focus, but also don't lose focus on the business challenges they run into, and then work with organizations like Optiv and others to help you bring a single message. If you can't do it by yourself we're here to help you do it and bring that message, because as specialist consultants we're here as an advocate to the client and some of their business challenges and we want to provide whatever that outcome looks like. So, make their APIs friendly, keep them standard, don't change them all the time. If you really want to build an ecosystem, you can't modify your instructions and your API every day. You've got to control some of the development maturity of your technology if you really want us to provide a platform-based security solution to our buyers. That would be my recommendation, fix marketing, fix your API management on the development side, and have really mature development processes.

Ashwin Krishnan: [00:17:21] One thing you touched on earlier is, at least for the smaller companies, the challenges because they have to raise money and they

come up with this extremely strong technically-oriented deck. Then, like you're saying, marketing comes on board, but marketing is typically non-technical. And then the technical guys have to make that marketing leap and say, "OK, we just can't continue to pitch technology the way we pitch to the VCs to get funded, to customers." And marketing, the kind of cyber skills that we're talking about here is, a new kind of marketing needs to evolve which truly is more about not vendor over-hype or jargon, but maybe telling a story. Like you said, maybe working with consultants and seeing where things fit, and being able to take some of the harsh feedback back to sales and HQ. Is that a mindset shift that you would recommend inside the vendor community as well saying how do they look at things differently?

Chad Holmes: [00:18:27] I would take it even further and say it's more than just marketing, transformation around marketing. We need to see a transformation around entrepreneurs. Because being a technical expert and creating a unique idea, really, we don't have unique ideas, it's whoever can get to market faster and have the most VC funding behind them. So, I would say, especially the organizations where I see technical founders not giving up post as they grow, when they don't bring in a business CISO to really drive business outcomes, bring in the people that can tell the story. Yes, technical capability is important, but everybody has unique technical capability. And you could probably put five vendors in the same room and say, "Hey let's have a debate," and everybody would have their spin and why they're better. So everybody, especially as they grow, has competitive teams to help them differentiate. Everybody's smart, everybody's technical, everybody thinks they're great. My recommendation is we have to see a transformational knowledge. Let's start thinking bigger, broader picture business issues and figure out how we change that dynamic. Solve a bigger problem for the buyers, and not try to figure out how to take a widget and go to market and then drive VC funding around it. I mean everybody can do that. I could probably start five companies right now while we're sitting here. But the value is, is it driving personal revenue for myself, or is it making a difference in the industry? That's the bigger question.

I always say some of the stuff that really makes industry differences gets understated and undervalued too, and it's because we like the sexy, we like the hooks, we like the oh this whatever. And that's why marketing teams rally behind it. So I would say, and I may even go broader and say, the VCs and the PE firms need to think differently on how they do funding because, are you funding an organization because they have some interesting tech spin, they can grow, or are you just giving money to a serial entrepreneur that you have confidence in now?

There's a little dynamic there, and I think it goes all the way back to how we fund startups that influence how we solve and then change how we do security. And until we change that dynamic and get the entrepreneurs to think a little differently we won't never get to a point of changing it and addressing the bigger market. Now, you could do the late stage elements of changing how marketing looks at it and you stay in your lane and build a story that makes it important, but does it really grow to a billion-dollar organization, do you become a unicorn through that process? Probably not. You want to do everything for anybody. So, there's expectations on entrepreneurs and expectations on the industry. I think it fundamentally goes back to the funding source, in my opinion.

Ashwin Krishnan: [00:21:31] I think that it's a great takeaway because we never talk about the funding source and what drives them, and ultimately entrepreneurs going after where the source of the money is and what their thought process is. Any final thoughts at the end of our interview over here, it's been fascinating, anything that you expect to see at Black Hat, good, bad, ugly?

Chad Holmes: [00:21:57] Well, hopefully I don't see more of the same. I guess it's my expectation. It's always interesting, you say Black Hat, DEF CON, and all these other big industry conferences. These conferences I've been coming to, as you, DEF CON, 20-plus years; I've seen evolution. When marketing companies take over big conferences, you see a dynamic change. But my ask is that we'll

see some interesting spins on how to circumvent certain controls. You know to drive theses and white papers and stuff, which I think is interesting. I think what we'll still miss is solving some of the bigger business challenges. So, hopefully we'll see that. I doubt we'll see it. We'll see probably more of the same to be honest. Hopefully we get to a point in the industry and say, "Okay guys, more of the same? It's just not going to get us there anymore." From an Optiv point of view, we're very focused on how to solve some of the business challenges and it really gives us that opportunity to sit on both sides of fence. Working with the vendor community and working as a consultant, ask how do we balance the two? And my goal is, while not having great conversations like this, hopefully I see not more of the same.

Ashwin Krishnan: [00:23:20] That's good, 'not more of the same.' That will wrap up this podcast. Thank you, Chad.

Chad Holmes: [00:23:26] Thank you.

Main discussion topics:

02:30	Cyber industry has become less about solving problems and more about driving market price
05:01	The most under-hyped security issue – the pressure placed on the security industry by changing business models
07:12	The new vision of insider threat
08:29	Tech skills and business skills in the CISO role
14:05	CISOs pushed to their limits and the search for talent
16:24	Advice to vendors – bring a single message and make it relevant.
18:27	Transformation is needed - in marketing, entrepreneurs, and funding
19:30	The biggest issue: driving profit vs making a difference.