Deloitte.

In this episode of Resilient, Rob Lee, CEO of Dragos, discusses why most organizations, and especially those with operational technology and industrial controls systems, need to act fast to mitigate cyber risk. He also outlines an intelligence-driven approach that can help leaders learn from past attacks to prepare for potential future strikes.

Mike Kearney: There's a saying that I think we're all familiar with: ignorance is bliss. It was coined by an eighteenth-century English poet, Thomas Gray. And if you live by this moment, you may not want to listen to this interview. You know, as a good risk management professional I am very well aware of cyber risks. But I don't think I fully appreciated the cyber risks in our nation's infrastructure.

Check out this quote from Brian Becker of White Hat Security. "Industrial control systems are the wild west of cybersecurity at the moment. These systems control factories, buildings, utilities, et cetera. Most systems have little to no protection and best practices are still being adopted very slowly. They also represent extremely high-value targets, especially from a strategic point of view. A few new companies have entered the landscape, but it is still an extremely young industry."

Today I am in Nashville, Tennessee, and I've got this incredible opportunity where I'm sitting down with Rob Lee, the CEO of Dragos. Rob has an incredible resume. Go online, but here are a few fun facts. First of all, like I said, he is the CEO and founder of Dragos. You'll hear more about Dragos in a minute. He was on the Forbes 30 under 30 for Enterprise Tech in 2016. He's an author and speaker; in fact, actually I think he was speaking at a conference today.

He spent time in the NSA. That's gotta be pretty cool. And he even finds time, which I think he brings out his creativity, to write *Little Bobby*. Go check it out. It's a weekly cyber tech comment. And I have to say I love marketing and he's brilliant for creating awareness and training on this issue.

Dragos is a pretty cool startup that's probably a lot more complicated than what I'm about to say, but I like to simplify things, so here is the problem. And I shared this with you in the stats. There are a lot of cyber threats in industrial networks. And when you think of industrial networks think of things like energy, manufacturing, water, and there aren't a lot of experienced people or tools to analyze and respond to these threats.

Dragos' secret sauce? They have people who have really deep cyber experience in industrial controls. They have a lot of people that have that kind of been there, done that stories, and we're gonna be hearing some of those stories hopefully today from Rob. But they also have some cool platforms and technologies to monitor and respond to these threats. So today when I talk to Rob, I'm going to be asking him things like what is cyber risk in industrial control systems? That's a mouthful. See? I couldn't even get through it. What are some stories to actually make it real? What should leaders be doing to respond to this threat? How is Dragos helping? What has Rob learned about leading through cyber crises? And I'm gonna end like I always do with some good old leadership questions.

Robert Lee: What effectively happened in 2015 in the Ukraine is the adversaries broke into those environments, stayed there for six-plus months learning the systems and then they really just used native functionality in the systems to turn off the power.

Mike Kearney: Welcome to the Resilient Podcast, where we hear stories from leaders on risk, crisis, and disruption. My name's Mike Kearney. I'm a Deloitte partner based out of beautiful San Francisco, although I don't spend enough time there. But my career has been in strategic risk, brand, and reputation. I love innovative new solutions, love creating great experience for clients, and I love what I'm doing here with the podcasts where I get to jump on a plane.

Like I said, today I'm in Nashville, and I get to interview these leaders that have so much to say about what it's like to navigate through crisis, risk, and disruption, what it takes to be resilient. And I cannot wait to talk to Rob. And Rob is at the forefront of this industrial control systems cyber risk, and he is going to share his incredible insights that I think we're all going to benefit from.

Hey, Rob. Welcome to Resilient.

Robert Lee: Thanks for having me.

Mike Kearney: I'm gonna start this out with something that doing a little research just blew me away. But you were one of the first people to report about the black energy attack in 2015 in Ukraine. I want to say most people probably don't know a lot about these operational technology or industrial control technology cyber risks, so if you could kind of just start, what happened there and maybe make it easy for the person that doesn't really understand a whole lot about it would be great.

Robert Lee: Absolutely. So I think the first thing to understand is industrial is pretty much the entire world. So I think a lot of firms these days look at operations technology or OT, or industrial control systems, we call ICS. We look at that and we think power, water, we think manufacturing sites, that's it. But really pretty much everybody besides banks and insurance companies are industrial companies. Logistic lines, everything out there is industrial. And when you look at it from an IT or enterprise security strategy, a lot of people think about patching vulnerability, stopping malware, how do we protect these networks?

What effectively happened in 2015 in the Ukraine is the adversaries broke into those environments, stayed there for six-plus months learning the systems and then they really just used native functionality in the systems to turn off the power.

Mike Kearney: What does native functionality mean?

Robert Lee: It means the grid operators, like the vendors and grid operators are turning off and on power. They have to keep power and electricity running, right? There's just functionality in the systems to be able to open up a circuit breaker or close a circuit breaker or keep the system energized or de-energized. And the adversaries effectively kind of became insiders in knowledge and then just used that functionality that's built into the systems. There's no patch to apply, there's no malware to delete, it's just that's how systems work.

Mike Kearney: They turned it off.

Robert Lee: Exactly, they just turned it off. But they did it in a coordinated, targeted way and they did it across months of time of being in those environments, and that's where the real risk came in of actually being able to do a coordinated effect across multiple regions of the Ukraine. So it was 225,000 customers across the regions that had that impact. And the downside is it happened again in 2016, and we've seen adversaries learn from that as well, and that's typically what we don't want to see is your adversaries getting smarter about how to do these things 'cause then you see a little bit of a snowball effect where you might see these attacks that have never really occurred, start occurring on a more common frequency.

Mike Kearney: How long was the power out?

Robert Lee: Not long at all.

Mike Kearney: It wasn't? Okay.

Robert Lee: I think some people look at that and go oh, it was only out for six hours. No big deal. But the reality of the situation is the systems were destroyed on what we call the SCADA side of the house, so the systems that effectively help automate it, those were out for eight-plus months. And so that impacts the ability to bill, so there's no ability to make money on your electric power at that point. And also that automation provides an aspect of safety. If you're having to manually operate electric equipment, you are very much in a position to get hurt or killed. And so without your systems in place, you could have loss of life due to these types of events.

Mike Kearney: So what has happened since then? Do you think that these companies have gotten religion? Has there been a significant uptick in protecting yourself against this?

Robert Lee: I think the community, especially in electric power, doesn't get enough credit. I think they do a lot more than people realize what goes behind the scenes, but it's still selective. It's not like the industry is doing this. It's maybe your top 20, 30 percent of your power companies are really, really leading the way. Then there's maybe your 40 percent in kind of the middle that are maybe they're doing the right things, maybe they're not, and then there's the bottom portions, which really are just behind.

And I think that's what everybody's a little bit uncomfortable with is, especially when you're talking about electric power and the United States multiple grids that we have, you kind of want everybody on equal playing foot because you kind of have to protect it all.

Mike Kearney: And when you were using those percentages, is that in the US or global?

Robert Lee: That would be in the US. Global is way worse.

Mike Kearney: I'm sorry, I've just gotta say—so if I'm an executive and I knew that this happened, why would I be in that bottom quartile? How do you even stay there? It's hard to get my mind around.

Robert Lee: There's so many reasons this happens. I think one is sometimes it's just even internal cultural issues of board of directors know they want to do something, the executives know they want to do something, but they don't necessarily know what the right investment looks like, and talking between the enterprise security people and what's happening on the operations side of the house, if you don't have the right people along the entire chain, communication issues, cultural issues, et cetera, can really break down very quickly.

Another issue that comes up is there's a lot of guidance out there for companies. If you're an executive of a company and you're trying to figure out the right thing to do for security, you are at no lack of people outside trying to tell you, well, you must do these five things and you'd be okay or some projections at the end of the year that if you don't do these predictions then you're done. So there's almost a little bit of analysis paralysis that can form for those companies. And then some of them just honestly don't believe it's an issue. I think there was a smaller portion in the US that still existed of people that looked at that and went, oh that's Ukraine. Anything to effectively get it out of their minds.

Mike Kearney: That would never happen in the US.

Robert Lee: Exactly. And unfortunately, that's just not the case. I mean, we don't see power outages in the US. that have occurred since 2015 due to that, but what we do see is nation, state operators absolutely targeting sites. My firm does a significant amount of incidence response around the community and seeing targeted attacks and targeted intrusions by adversaries and we go in power manufacturing, all these different sites, and kick out these state actors and it's not exactly as nice as people would like it. I commonly tell people the risk is much higher than people realize, but not as bad as they want to imagine. You don't need to go read Ted Koppel's book and build a bunker. But on the other side of the house, we've gotta be doing a lot more than what we're currently doing.

Mike Kearney: Maybe just touch on a couple. So we talked about the energy industry. What other industries? You said it, everyone is susceptible. But what would be the top few others that you would highlight.

Robert Lee: Generally when I think of the industries that really need to do a lot more because we have the risk and we have seen threats that we can learn from, I place it in kind of electric power and all the different players across electric power—transmission, generation distribution, renewables, et cetera. I think of oil and gas, even though there's a lot of different aspects of oil and gas. And although it's not fair to clump them all together, I'd say manufacturing is kind of a larger industry, there's absolutely differences between chemical manufacturing, pharmaceutical manufacturing, food and

beverage, et cetera.

But as a manufacturing industry, a lot of the threats and issues they see are actually kind of similar. And unfortunately there's a lot of things that can happen in those other industries, where electric power gets a lot of discussion because we think of state-on-state kind of conflict. But the types of things that you can actually do in the other environments are more numerous in its benefit to the adversary.

As an example, targeting electric power is effectively a military-like action. I'm going to war or I'm not. Or I'm scaring politicians or I'm not. But if I target a pharmaceutical plant, it could have the same type of conflict-like scenarios, but I could also steal tons of intellectual property worth billions as it relates to all sorts of new medicine and research being done.

Same thing with food and beverage. This one's a little bit weird, but we worked with a company that produces lots of chocolate and they were having intellectual property theft issues and it had nothing to do with the recipe of chocolate, it had to do with the molds. And they were doing lots of research around what molds would sell and not sell well and they had a state actor stealing intellectual property of those molds and building them first in another country and stealing sort of revenues. It's amazing how much happens in the industrial world that people just don't realize about.

Mike Kearney: They don't realize. So Rob, let's maybe go back a few years and learn a bit about you. You grew up in a military family, but just tell us what your early years were like.

Robert Lee: Yeah, sure. So I grew up in Alabama and my mom and dad were senior mass sergeants in the Air Force so enlisted family growing up. A lot of fun, but I really wasn't a computer nerd to start off with. I mean, I loved games and playing around, but I think being in Alabama was a little bit more about creeks and running around outside and being a happy little redneck.

And basically there's no great story on this. It's effectively my dad tricked me. But I was going to Auburn. I was gonna have a fun time at Auburn University and go party and enjoy life. My dad had said something to me along the lines of yeah, yeah, well, you couldn't get into the Air Force Academy anyways. I'm like, what's the Air Force Academy, Dad?

Mike Kearney: That's like the Jedi mind trick.

Robert Lee: Yeah, he totally screwed to me. And so I applied to this thing not knowing anything about it. And my dad was a Purple Heart winner or earner in—

Mike Kearney: In Vietnam?

Robert Lee: In Vietnam. And so he had an automatic nomination. You couldn't get in automatically, but you could guarantee that a congressman would look at you, effectively. And so we put my package in and I got accepted. And so I go to this school thinking it's a normal school. Yeah, it was interesting. But I was too stubborn to quit. And then like summers they would send you off and you could go do a variety of things. And my summers I would get to do cool little missions.

I routinely would be—one was working in Cameroon and you'd do control system building and trying to do little microeconomy building. And so I went to Cameroon and helped play around with wind turbines and water filtration units and things like that, and so I learned about control systems before I really learned about cybersecurity. And I just was just really impressed with how much control systems operated everything around the world around us, but nobody knew about them. And everything from elevators in the building to things in your car, the satellites, it was everywhere.

Mike Kearney: Engines on planes?

Robert Lee: And you'd ask anybody about controls—everything. And at that time it was, what are you talking about? Is there gremlins in the system? So I graduated and they said hey, at the end, I mean, I wasn't a perfect student by any stretch, but at the end they had one last pilot slot open up. They're like, do you want to be a pilot? And I was like, no. They're like, what? They effectively hated me at that point. They're like, well, you go be a com officer then, which was kind of like the talk down to you. You go be a com officer. I was like yeah, I'm gonna go back to Africa.

So my actual major at the academy was African studies. I was like, I'm gonna go back to Africa and do control system work. And I get to this news—in route they changed com to cyber and I went to this brand-new schoolhouse they had. They're like, well, all right. You're a cyber officer now. I'm like, what does that mean? We don't know. So they're doing all this training and work and it was pretty in-depth kind of work and training. Then they said, well, what do you want to do? I'm like, what about all these control systems? They're like, what are you talking about?

So for months I was actually teaching them about control systems. And at the very end they said you did really well. You get one of your top picks coming out of here. It wasn't definitely not top of the class but one of the top picks coming out of here is the White House or some Podunk assignment in Germany. I was like okay, I'll go to Germany. They're like no, no, no. The White House. You can do like security in the White House.

Mike Kearney: Pilot? No. White House? No. I think there's a trend here.

Robert Lee: Basically I accidentally walked in. I'm sure I'm destroying any credibility I have in this space. They're like you didn't go to the White House and it'd be good for your career. And I said, but you said Germany and I'm from Alabama. I'm going to go get drunk in Germany.

Mike Kearney: I'm going back to my Auburn days.

Robert Lee: Yeah, exactly. I'm going to finally get the experience. And then when I got there, it ended up being a cover site for the NSA. I'm like oh, okay. What do you want me to do? And they're like, what are you? And I'm like, cyber officer? Oh, okay. Find threats. I'm like, what do you want me to do? Find the unknown unknowns. What are the unknown unknowns? We don't know. Go find them.

So I accidentally fell backwards into building one of the first industrial control system focused NSA missions around threat discovery. So the National Security Agency had been securing ICS before and working on that, but there hadn't previously been a

mission to find what threats were breaking in and learn about them and kind of this intelligence work around these threats. And I don't think anybody thought there was gonna be any. We just started finding states and actors and people we never heard of before.

Mike Kearney: And just put a time stamp on this. When was this?

Robert Lee: This was late in the ages. This was like 2010, 2011. So this wasn't like that long ago. The world of industrial security has been kind of blooming for a while, but this idea of threats to industrial security and actually learning from the threats to do things hasn't. I would say at most companies I go to, if they have an industrial security strategy, they just copy and paste whatever the enterprise security strategy is and then just put whatever doesn't break the industrial environment into the industrial environment.

So effectively you're taking the security strategy that was built off of different threats, different missions, different systems, and you're applying it hoping it's gonna reduce risk, but obviously it's not because it's not the same risk. So that whole aspect of hey, let's take an intelligence-driven approach, let's learn from the threats is completely new in this space.

Mike Kearney: So somebody referred to you as somebody with marrow-deep concern for protecting your homeland.

Robert Lee: Yeah, I would say anybody's. And so I sometimes probably upset some people in this comment, but I think nobody should be in anybody else's civilian industrial infrastructure. I loved my time in the National Security Agency. Don't get me wrong. But if I found the National Security Agency in somebody else's ICS, I'd report it. Nobody should be in anybody else's civilian industrial infrastructure.

Mike Kearney: So it's not necessarily the homeland per se. It's just get out of—

Robert Lee: Yes. Don't get me wrong. If you cut me deep enough, I'll bleed red, white, and blue, I'm sure. But at the end of the day, I'd protect the Iranian power grip if they let me. If it's civilians, it deserves to be protected worldwide.

Mike Kearney: So you've seen obviously some crazy stuff. What keeps you up at night now? Or anything? Maybe you sleep like a baby.

Robert Lee: I enjoy life. I got a nine-month-old son. Life's amazing. Look, there's all sorts of disaster scenarios, don't get me wrong, there's intellectual property theft, there's all these big ones. But you know what really concerns me is the fear of it all. I see all these people hyping up the threats. And there are real threats and we must do real things against them. But we don't need to freak out on every little phishing email or something we get. We have to really approach this with some poise and nuance.

And what I'm concerned about is congress, senate, national-level leaders around the world are so terrified of what can be done. You can prepare the biggest military or the biggest economy, everything, and the idea that somebody remotely can turn off the lights scares everybody. And when I did my testimony to the senate, it was probably the one time I felt like the most patriotic ever. Testifying. This is a very cool feeling. And their questions, you can still feel the tenseness. They were really, really

concerned. And my biggest fear is something happens that's really honestly controllable, like maybe a 30-minute power outage in DC.

Mike Kearney: And people overreact?

Robert Lee: And people overreact.

Mike Kearney: Overreaction.

Robert Lee: Yeah.

Mike Kearney: So let me ask you the questions. I work in Deloitte. I'm a risk partner, not a cyber person. I know a lot about IT cyber. The OT piece is kind of new. So I would say even I'm kind of nascent in this area. What do you see in terms of people understanding of this, first question, and then how do you get business leaders actually to pay attention? 'Cause it's hard to get business leaders even to pay attention to traditional cyber risks.

Robert Lee: It's getting better. But, it's getting better and it really is, but I think in my short tenure, what I've seen change the most across the cyber risk discussion at all is having business leaders that have technical backgrounds has been helping companies significantly. So having somebody that we think was a good business leader because of that MBA and then you put them in but then they don't understand anything about tech, they're not really good at advocating for what needs to be done.

And I see that changing a lot. Like, I see the generation of people that are cybersecurity practitioners that learned the business 'cause you can't just be a tech practitioner. You really do have to learn the business. And we're starting to see those move into those positions and I think that's changing a lot for companies. And getting the right outside help to validate that can obviously help a lot. Not just to have a plug, but I'm pretty pro-Deloitte on that piece.

On the OT side of the house, like the industrial side of the house, I think there has to be an understanding that the customer of what you're doing, as well as just the entire mission, is the operations. That's where you generate all the business for your company. And what I found effective at a board level, and I've had the pleasure of going into ten or so boards this past year at different companies and speaking about industrial threats, and what I found to be really effective is helping them understand that a lot of the resource investment has been on the enterprise side of the house, but actually most of their risk is on the industrial side of the house.

And so they just step back for a second and realize the world's kind of flipped. They go, wow, we've been putting a lot of resources, but all the money we make is over on this other side of the house, and what do you mean we're not doing anything? And so it flips a little for them and then you help them understand, but hold on, you don't need to do everything you've been doing. Every IT thing, every IT strategy, every IT product, you don't have to just copy and paste.

You don't have to find the equivalent. With the small focused effort of some smart people, the right technology process and people, you can make huge strides to reduce that risk. That kind of sets them back on even footing of, ok, we can do this. I think there's something that happens, especially around cybersecurity, where you can feel

helpless really quickly. Like, state actors, what if China or Russia or Iran. It's like, you're not going up against China, Russia, or Iran.

You're going up against somebody whose first-time job is the government and they're between the ages of 18 and 30 and they have PowerPoint and management too. You're going up against human adversaries. You can do this. And I think that honestly works a lot for them.

Mike Kearney: But it sounds like in order to really help just a business person without maybe a technical background, almost equating it to, this is how your business is running, you have not made investments in this area.

Robert Lee: I think it's an enlightening thing to see. What do you mean I have unrealized risk across my entire company?

Mike Kearney: And so it sounds like it hasn't been that difficult for you to convey that message to them when you communicate.

Robert Lee: No, not at all.

Mike Kearney: If you were, though, giving advice to a, I don't know, a CSO or a CIO to make that communication simple, what two or three things would you say to them?

Robert Lee: So if the CIO or CSO is trying to talk to their executives, board, plant manager, et cetera, I do think it's effective strategy to simply articulate we have unappreciated, unrealized risk for the company and look at the budget we have, and just show them how little you've actually been putting on industrial.

Mike Kearney: Where you're spending the money.

Robert Lee: Yep, exactly. Follow the money, show them we haven't been doing anything on it, we should do this. And the most effective tool I've seen to be kind of an eye-opener, which is really an in-depth thing, it's not super simple, but a tabletop kind of exercise at the board level of showing them of would you even be able to answer the questions that you need answered from everything from regulatory or liability or communications or just from a general risk perspective?

Could you even have the tools, people, and processes to go and bring the plant back up from a cybersecurity incident? Walking through kind of the what-if scenarios, not based on hypotheticals, but based on what other companies have actually dealt with actually, ends up being probably the most effective tool I see in changing the culture of their company.

Mike Kearney: Well, and the likelihood of them having tested that before is probably very low so it's probably—

Robert Lee: No, it's_____*[crosstalk]*. Every company we go to has an instant response plan. And if there's an industrial portion of it, I would say in well over 90 percent of the companies that we go to, which is, think about it, they're the ones that are mature enough to call us, it's kind of a sampling bias in itself, but well over 90 percent of those, if they have industrial at all in their instant response plan, it's like a paragraph or

a page of, talk to the plant managers. And they're like, what are you talking to us for? We don't know what you're supposed to do with the security piece of this. So no, I think companies are more unprepared than they might realize.

Mike Kearney: So talk to us about Dragos. Obviously your baby now.

Robert Lee: It's been fun.

Mike Kearney: Tell us, if people don't know about Dragos, what do you guys do?

Robert Lee: I think the easiest thing to understand about Dragos is we're the team that knows about the threats the most, and so we're the team that can help you deal with the threats from a technology and people way. What, it sounds kind of arrogant saying out loud, but we have the practitioners. There's not a ton of people in the industrial security community. I mean it's well known that we're talking about in the hundreds, not in the tens of thousands of people, right?

And we've sort of centralized that talent. And so I think the thing that we did well to start with, which actually infuriated all the venture capital community and everybody else, what do you mean you're gonna hire people? No, I want to outsource whatever and let's build product. No, no, no. I'm gonna centralize the smart people. And so we hired a bunch of practitioners and effectively do three things in the company. We have an Intel team, is they go out and figure out what the threats are actually doing and how they're doing it.

We have a services team that does things like instant response around the world, and then we as a company are a software company. But I believe you make better software by having better people. I think we have an issue in our community now where everyone wants to say artificial intelligence and neural networks and machine learning. We can machine learning this away. And we're like no.

That machine learning model has never experienced this. Let's use machine learning and really smart technologies as an amplification of smart people. But let's not pretend that you can remove smart people from the process. So let me take the insights that the experts have and make better software, and then yeah, sure, go after that and do whatever you want to amplify it.

Mike Kearney: Anything you're innovating now that you're excited about? That you can share?

Robert Lee: Yeah, I think the technology that we have is cool 'cause it's not only giving visibility into the assets and inventory around the environment. It's kind of fun to see people's face light up when they've never seen how much has been in those environments. They assume we've got a couple of turbines and a couple of manufacturing lines or whatever and you turn it on and there's all these devices and they're like, what is that? And like yes, it's been here, man. Or it's very common for companies to think their air gapped. Very, very common. We're segmented from the Internet. No you're not. Guaranteed. I'll save you the assessment. You're not segmented. And they start seeing these inner connections. They're like, where do those connections come from?

Mike Kearney: What would lead them to believe that they air, I've never heard that term air gapped. So that's separated from the Internet.

Robert Lee: Yeah, it's separated. Yeah. I think it's a very common thing that just everybody in the community, I don't know where it originally came from. And people even talk about, well there's IT and OT convergence. It's converging together. No, it's not. That happened a decade ago. You're just now figuring it out, but it already occurred. You've got cloud-based applications reaching down to your manufacturing lines today. You've got Internet-connected processing that's helping you produce power more efficiently. You have a highly connected plant, highly connected industrial environment. They don't realize it.

Mike Kearney: Is it that they don't, they literally just don't realize it?

Robert Lee: They don't realize it.

Mike Kearney: Wow.

Robert Lee: 'Cause if you think about it, there's so many things happening in that environment—maintenance, operators. In an enterprise environment, you have vendors but you don't have vendors that you really rely on. You have Microsoft for Windows. But it's not like your entire system is built by somebody. Maybe like ERP would be an equivalent. But the industrial environment, they build a portion of the plant. And so as you have all these different equipment manufacturers building giant portions of it, more and more they've been connecting it up over the years for maintenance and purposes and people have been signing off to go yeah, I want to reduce that cost. It just happened to people and they didn't realize it.

So from a technology piece, what I get excited about is one, turning it on and people are like, wow, all right. And two, that's when we start doing the threat detection piece, which is let's show you that you have issues. And I don't want to say this flippantly, but it's a little bit like shooting fish in a barrel of you have an environment that you've never really done much with before. It's a pretty high chance that some stuff is gonna be in there.

It might not be the Russian nations there, but you're gonna have something going on. So helping them realize that things have already been occurring and you can kind of get a quick win right off the bat is always nice. And then we have in the technology playbooks. I think that's the piece that I think is the most fun, which is I don't want to make a technology that solves the problem. I don't think that's really possible. There's no silver bullet. What I want to do is enable people to develop their own experience and expertise.

So instead of trying to sell a silver bullet, it's really just checklists and info from my people of here's how we would have dealt with this situation. Why don't you do it? And so it's kind of this guided experience for your security people to then go and actually do it themselves and then they feel super proud, they're excited, you see the lightbulb come on. So you're kind of growing the community at the same time that you're actually getting them to do the work. That's all fun. And then it's always just fun being involved in these cases where I think we're a little bit different than most firms where we don't want to talk about the attacks.

Mike Kearney: I was gonna ask you about that. I read that somewhere and I was like wait, so that

insinuates that other firms like to talk about the attacks.

Robert Lee: Yeah, I think we're kind of pseudo famous, if you will, for two things. One, we don't tell the media about the incidents and two, we don't do attribution. Even if we can. Even if we know who did the attack we don't do it. And journalists, it used to the mind-set was journalists wouldn't cover you unless you were willing to point the finger at Russia, China, whatever. So we were one of the few firms who were like no, we're not doing that.

Mike Kearney: Why?

Robert Lee: It doesn't help anybody. And so if I tell you—

Mike Kearney: So it's almost more of just bringing awareness to how great you guys are more than anything.

Robert Lee: More than that. It's like if I tell you it's Russian or China or Iran or North Korea or whatever else, it's distracting. It doesn't actually help you do your job better. And you can argue about oh, it helps with priorities. No it doesn't. It's legitimately distracting the people doing the mission of actually defending. You should care about how the attack occurred and how to defend against it and not who did it. And I think it's been very self-serving in the industry to do all this attribution stuff, so we don't do it.

It's been interesting because originally we thought it was gonna be a decision that hurt us. And then the journalists are like wow, these people don't do it. It kind of became a thing. There was even a *Washington Post* article about us lately. They were like, "Dragos, who famously doesn't do attribution," I just kind of laughed at that. So we don't do that and we don't talk about our cases, and I think for most firms you do. You want to.

Mike Kearney: Meaning like here's work we did, like cases.

Robert Lee: Yeah. If it's an incident—

Mike Kearney: Yeah, when you're a consultant, that's your everything.

Robert Lee: Absolutely. That's how you prove that you know what you're doing. And in most firms it's really important to be in the *New York Times* or *Washington Post* or whatever else we're talking about. We just did this big investigation, and we refused to talk about something unless it's already gonna be made public somewhere else first.

And the reason for that is if you're a power company, manufacturer, whatever else, the last thing you want is the stuff in the media because people freak out about it. Everybody cares about our industrial infrastructure. Your local community cares about power. It's our infrastructure. So when these attacks get publicized, it generates so much noise and hype and craziness that none of the defenders ever get to do their job. They're just answering emails and taskers from everybody.

Mike Kearney: That's a fair point.

Robert Lee: And so I view it as our responsibility to help them do the actual mission, and we've

actually found stories that were going to get out that we killed to make sure they didn't get out just so that people can actually do their job.

Mike Kearney: Where does that philosophy come from, do you think? Is it kind of your own value system or somewhere else?

Robert Lee: I don't know. I think it's—maybe—that's a good question. Maybe there's an element to the National Security Agency of don't talk about it. And the only reason we even talk about the National Security Agency stuff is because so much stuff got leaked and my name ended up being tied to some stuff with Russian websites and all this other crap, and I was like well, all right.

Mike Kearney: It's in the press.

Robert Lee: It's in the press now. It's not like I can come out and be like that doesn't exist. But I think maybe it's a little arrogance in it too, if we really want to get down to it. I think from a National Security Agency perspective, you took pride in being that silent defender of, I'm holding the wall but nobody needs to know and I can't even tell my spouse about it. It's almost like not a romanticism to it. And so the idea that you're this community partner and taking care of people, I don't need the credit, maybe there's a little arrogance. But I think it also comes down to by being practitioners, by actually being in the community, you realize how much it hurts the community. If you actually want to make these companies successful, then even if you think the ends justify the means, you just don't.

Mike Kearney: So talk about talent. So you said that there's not hundreds of thousands, or even thousands of people with this experience. What are you guys doing or what does the industry need to do to cultivate more people?

Robert Lee: So there's a couple of ways I look at that problem. One, even before I started the company, but I saw this problem at the agency. I have this ICS mission that was growing and because it was successful, the government kept throwing money at it. Let's build it out more. There was nobody to hire. There was nobody to pull over. And what I found most successful is building internal training classes and brainwashing them into our way of thinking about it. And at the time I realized that that didn't scale. And what happens if I get hit by a bus?

How am I gonna make that scalable? So I actually ended up going and creating the first ICS instant response class at the SANS Institute. So it's like a big training provider around the world. And so to this day I still teach. That's where I came from today was teaching there. And so even though I'm running Dragos, I still think it's important for the community for me to get out and teach a couple times a year. I want to try to at least build up this skillset. Training alone is not gonna do it. You gotta get experience as well. But I think what's important for the community is having access to training and also creating a buzz around it. I think there's a lot of interest in cybersecurity, but there's an importance to show that ICS security is this cool defensible, wonderful thing to be in, and then you draw in new people.

So we, like at Dragos we've had success in three ways. One is pulling in the small community that does exist around ICS security practitioners, and we all used to get drunk at the conferences together and go what if we all just did a company together?

What if we just got the 20 of us and just, forget consulting, why if we just did it together? We always used to joke about that, but that's what we did.

Mike Kearney: That's what you did.

Robert Lee: We just pulled all of the friends together, which helped in the startup aspect of reduce the Stormin' Norman aspect. We've known each other for years. The second thing we did when we exhausted that talent pool was we looked at really high-end, really professional IT security folks that had the community drive. You can see that they are always out teaching, they're always out speaking at conferences and B sides and whatever else.

Not only is that person sharp, but they really care about community and that's a very industrial—I don't want to say that enterprise security doesn't care about our community, but that's a very industrial thing. And so we pulled those people in and we make them junior people at our firm. We say I'm glad you were a top tier instant responder everywhere else. But here you're gonna sidesaddle with our people, and we treat it like a journeyman program and then transfer that knowledge.

We've been very successful about it. And to give her a lot of kudos, Lesley Carhart's a well-known incident responder in the community. And thankfully she didn't murder us for doing this, but we treated her like a junior person when she came in and now she's amazing. She's probably one of the best ICS incident responders in the community now 'cause she transferred those skills over, was humble about it, and then went off and did amazing things.

And then the last thing we do is we take just straight-up interns and young people, right out of college. They haven't been taught the wrong things.

Mike Kearney: Does it matter what their background is? So like if I'm a kid in college—

Robert Lee: I don't care. I want somebody who's excited, who's hungry, who if I can sit them down in front of the TV show *How It's Made* and her face lights up, that's your person. We take those folks. One of our better analysts was at the Navy Academy. Everybody makes wrong choices in life. He was the Navy guy instead. It's unfortunate for him. But he was a Naval Academy person and they kicked him out for having diabetes, which—

Mike Kearney: They didn't know that when he went in?

Robert Lee: Didn't know it when he went in. And you can actually be an officer in the Navy and have diabetes, but you just can't graduate from Annapolis and have diabetes. So whatever. We were pretty pissed for him. And we didn't know this kid, but he started showing up one day and said hey, can I just do some work around the office while I pack up my things, settle my stuff with Houston I then I'm going to go home. It's like sure, no problem.

And he just dove into it so much that I walked in one day and found him sleeping on the couch so he could be there early enough in the morning to sidesaddle with the analysts to be able to go do stuff. I'm like dude, you're hired. Stop. Go home. Sleep. And he's one of our better analysts now. He's so entrenched in it that he's become

amazing.

Mike Kearney: You know what's great about that story? Is that it's actually a great little lesson learned for kids trying to find a job. When you have that grit and just I'm going to make this happen. Those are the type of people we all want to work with.

Robert Lee: I think you can get burned out in this industry really quickly, but I think you have to show you're hungry. And the balance is really, it's a really thin line to walk, but I think it's important. Especially if you're gonna come in when the bar's kind of stacked ahead of you, any time of going into places like power generation stations and gas turbines and oil refineries. It's not exactly like if you crash a Windows system everything's okay. You're taking some real responsibility. So you've really gotta prove it. And we found that a lot of the young kids coming out, they're really showing some awesome aptitude.

Mike Kearney: How do you think your intelligence background helped you?

Robert Lee: I think it helped us a ton. And the reason I say that is we're the only ones that are actually doing what we're doing, and I still think this is the next area in common I'm gonna make. I think we're years ahead of our competition because of that. They're all buying into this narrative of let's just bake a machine learning model. Then it will highlight anomalies. Then what? What do you mean then what? So you have something weird on the network. Now what are you gonna do about it? For us, we dealt firsthand with these attacks.

Name your major industrial attack and somebody at Dragos has worked on it. And that shows us that here's what does and doesn't work in these situations. And the intelligence side of it helped us go okay, it's nice to get an alert, a notification that something is wrong. It's even better to have context around why it's wrong. Context of what you're supposed to do with it. An understanding of where it's happened before. And that understanding of what intelligence can deliver I still think is an issue even in enterprise security.

Most people think of intelligence as a data feed of data that gets delivered to you. That's not intelligence. Intelligence is context and understanding and knowledge about what you're supposed to do in any given situation. We built that mission out for industrial so it didn't even exist before. Again, I think we've kind of set up a little bit of a monopoly on that component of the industry. And so it's done very well for us and we've grown very quickly. We've started the year with 22 people and we have 104 employees now.

Mike Kearney: That's what I was gonna ask. I wasn't even gonna go there. Are you, concerned is probably not the right word, but you obviously have significant growth opportunity. You're the CEO. How are you managing that? That's gotta be—

Robert Lee: Culture, culture, culture. And I know that every CEO says that, but I've awoken to that of yep, that's right. I think every time I've heard some businessperson be like it's about the culture, like okay dude. What is it really? What are you actually doing on a day-to-day basis?

Mike Kearney: So what are you doing on a day-to-day basis?

Robert Lee: So from a day-to-day basis, effectively, I've kind of had three different companies in the company, right? You have an intelligence team that's off doing their own thing, you have a services team that's off doing their own thing, you have a product team. Just keeping those three in line is enough. I focus a lot on what are we capturing from each, for like the voice of the customer. Since I've been in the community a long time I like teaching them. I kind of have almost like this product officer view on what the normal user needs out of what we're doing.

And then as silly as it might sound from a marketing and sales perspective, we're a highly technical practitioner shop. We're always oversensitive to snake oil marketing and sales tactics. We've all lived that. If somebody came in and sold the CEO on a silver bullet and we had to live with it. It is a daily work. Luckily I have a good sales and marketing leader, but it's a daily struggle working with them to help them understand here's what you can't say. What do you mean I can't say that word? Well, that word has been abusive before and here's why. I know it seems kind of silly but—

Mike Kearney: No, that doesn't at all.

Robert Lee: But really focusing on how we communicate to people externally, how we capture communication internally, what values we really focus on, what we walk away from has been interesting.

Mike Kearney: That probably says more about your values than anything, right?

Robert Lee: There are companies we go to and we're like we're not the right fit for where you are. You need to start somewhere else. Usually you need to go get a handle on your networks, you need to go build a security culture. We're who you come to in maybe two to three years after you're thinking about this, for some of them. And so I think it's important to know what we're good at because more important than anything, and again maybe it's a thing of arrogance, but more important than anything to me is the Dragos brand that is trusted and people know that we'll take care of them.

And so I don't want to be in a position where we're not gonna be able to be the best in that situation. And it's funny too 'cause I'll tell people that we have 100 people and we'll have these giant firms sometimes that we deal with, and they're like it's a small company. We're the largest ICS incident response team in the world. We have more incident responders at Dragos for ICS than the Department of Homeland Security. It's a think scale in terms of what the industrial community is.

Mike Kearney: Right. And focus.

Robert Lee: Yeah, exactly.

Mike Kearney: You know, it's funny 'cause I always think of, and it's kind of maybe cheeky, but Tony Hsieh at Zappos, how he sold his first company 'cause he hated his culture, which I think is fascinating. You build your own company and then you hate it.

Robert Lee: And I don't want to be in that position. 'Cause you can only do it once, though.

Mike Kearney: There is a trend almost starting with where you went to school and then what job you picked and then when you went to Germany. You almost do exactly the opposite, but it's actually it some regards it made you who you are today.

Robert Lee: Chased beer and didn't like flying. So good job.

Mike Kearney: Yeah. Hopefully my 19-year-old son isn't listening to that. So just to cap off this conversation, if I'm a business leader, no technology background, what advice would you give to me based on everything that you've said?

Robert Lee: Look to see if you have industrial in your company.

Mike Kearney: Which you basically probably do.

Robert Lee: You almost guaranteed to do. Make sure you're getting the right answers internal to your company. 'Cause it's a very difficult position to be in for people that have never dealt with it before and now they're on the hook to provide answers, but make a culture. If you're an executive, make a culture where you can go to your CIO, your VP of technology, whatever it is, and let them understand that if they don't have an answer for industrial it's okay. You're not gonna penalize them for not having an answer to a complex challenge you as a company has never looked at before.

Take the time to get it right. And my general advice is don't worry about all the hypotheticals. I think it's very common for people in security to look at research that comes out at the DEFCON and Black Hat conferences and stuff and go, well, how would we deal with this? Well, hold on, stop. What is actually happened before? Did Ukraine have a cyber attackattack that led to a power grid? How did those things occur? We want to know at a board level that we can reduce risk against what's real and has occurred before, and help me understand where we can prevent, detect, and respond.

Don't put everything in prevention. Where we can prevent, detect, and respond to those types of incidents. Make sure we're good with that. Effectively, and I've said this to boards before, if the Russian state, and we just pick on Russia all these days, but if the Russian state throws everything they have at you, and that's never how it actually is. But let's say they just throw everything they have at you and it's all novel and no one's ever seen any of this before, no one's gonna hold the board accountable for that. But if what happened last year to a similar company identically happens to you, you should probably go to jail. You've definitely not done your job to reduce the risk.

So, in essence, start by building the culture around accepting new thoughts of how this needs to be done, learn from what's happened in the community before to guide your security investments of what right looks like, then start thinking about being innovative and how you can cover down future issues.

Mike Kearney: I also just love how, 'cause there's probably a lot of organizations that haven't thought about this, don't go, yell or implicate your CIO because they haven't done anything, work with them, which I think is a really healthy way of approaching it.

Robert Lee: Yeah, it's a hard job to be a CIO/CSO these days. CSOs are scapegoats with every

breach we see. When the CSO doesn't own the risk, the CSO is the advisor in the organization. And I think many times they get beat up and it's kind of funny 'cause they're the ones that are jumping up and down before, like we need to look at this. Then you see them leave.

Mike Kearney: High-risk, low-reward job.

Robert Lee: Exactly.

Mike Kearney: I think we've got a lot of insight into this. We're gonna pivot to kind of some leadership questions but I think we've got a lot of insight into who you are. But how would you describe your leadership style?

Robert Lee: I try to empower my team as much as possible to make decisions without me. I sleep better knowing that if I get hit by a bus, they can keep the company going and they wouldn't miss a beat. They probably wouldn't like to deal with venture capitalists as much as I have to, but they can do the rest of it, right? And so that comes down from everything from lack of meetings, like we try very hard not to have to have meetings around give me an update with PowerPoint slides. I don't care. Go do what you need to do, come to me for help, and it comes down to even like hiring.

Mike Kearney: I was gonna say, the lack of meetings, the need to kind of micromanage probably has made it a lot easier if you have great people.

Robert Lee: Absolutely. And if you can't trust your people then maybe you don't need to be going with that team into the game anyway. Even with hiring, it probably is counter cultural where the idea is I'm a good CEO 'cause I've met every person we've hired. I completely believe that was said. I want my team leads to build their own teams, just like I got to build my team with them. And so I am not bothered at all if I don't interview or talk to that person coming in and out.

I'm gonna make them feel welcome when they come in and make sure I interact with them and all, but I'd rather my team leads choose the team they're gonna go play with. So I try to empower my team to make as many decisions as possible. We have a company handbook and we literally have one corporate policy. And that one corporate policy is don't be an asshole. And as long as you stay inside that guideline, 'cause we all know what an asshole is when we look at them, right? As long as you stay inside that line, I don't care. My flight got delayed and can I get a hotel? I don't care, dude. Go. Do what you need to do.

Mike Kearney: Do what you need to do.

Robert Lee: I'm going on a long 20-hour flight. Can I upgrade to business class? Yeah, that makes total sense, dude. Just do what you need to do. But don't be a jerk. There's a balance there. I'll tell you what. Probably the thing I like the most, and this is gonna be inappropriate, but the thing I like the most is coming from a government background, it took an act of God to fire somebody, and everybody knows we don't deal with assholes, no matter how good they are. And there was an employee we had that broke that rule.

And effectively harassed one of our female employees. And she was so nice and

followed up with him and said, hey, could you please stop? And then he immediately did it again 'cause he thought it was funny and he was fired two hours later. And the ability to have that flexibility inside the company made me feel better. But what I didn't anticipate is that it resonated with everybody else, and culture was amazing after those kind of cases.

Mike Kearney: I was gonna say if there was a culture score, it probably went up 20 percent after that.

Robert Lee: Yes, it all comes down to I've built the team with people I trust. I think I'm a decently intelligent person enough to hire people smarter than me, and then I let them go and do the same thing after that.

Mike Kearney: But I think you said something that's really important, because one would argue, though, in your industry that the premium on technical skills probably outweighs maybe those interpersonal skills. And I think what you're saying is—

Robert Lee: No way.

Mike Kearney: No. They both have to be there.

Robert Lee: You better—especially the type of work we're talking about, our tagline is there again. Our tagline is "safeguarding civilization." You can't come to play with that and have jerks on your team. You have to actually take care of the community.

Mike Kearney: So what's it like dealing with, well, you're a venture-backed startup, so what's it like dealing with your investors? And I'm guessing there's probably a lot of positive because they're very focused from a business perspective. You guys—

Robert Lee: Oh I'm sure it's—

Mike Kearney: Tell us how that's going.

Robert Lee: I'm sure this is gonna sound so fake. Oh, I love my venture capitalists. Of course you do, right? I'm mean, but—

Mike Kearney: So let me pivot to people. So obviously you've talked a bit about what you do to get your people excited, to encourage them for you to build the right culture. But what is the one thing you do to motivate them? So that's the first question. And then the second one is what do not do that would demotivate them? Which actually may be more important in some regards.

Robert Lee: I'm gonna give a very tactical-level answer to that, but what I do to motivate my people is realize why they joined and empower them in all the ways possible to let them do that, and that is the mission. So I remove as much as possible from any barrier for my people so they can focus on the mission. How we do benefits. This is totally not normal startup stuff, but we do a 6 percent, 100 percent match 401(k), we do health, dental, life, disability, vision, everything, 100 percent covered for you and all your dependents. Don't worry about anything. We got you.

Every possible thing we do, provide lunches for people, every possible thing we do to take every minute back that we can give them to do the mission and we let them go do

it. And recruit for us. We don't have a recruiting problem. We put out a job announcement one time. We had 480 applicants in 48 hours. We don't have a recruitment problem.

Mike Kearney: So beyond that, it almost sounds like you also take away kind of the bureaucracy. Is there an example that you see in a lot of organizations where you said we are not doing that here? Meetings was one.

Robert Lee: Management that cannot do the mission. I do not agree. And this is a very—

Mike Kearney: What did—say that again?

Robert Lee: Management that can't do the mission that are leading. I know this is maybe not resonate with everyone in the audience, and I understand that I'm a small company, but the idea that I can put a person and expect management to be a skill is ridiculous to me. There's no such thing as management as a skill. Read all the books, Peter Thiels' book and all his other crap, they all boil down to don't be an asshole. So that's why I just made it a company policy. I don't view management as a skill.

I view being so good in your position that you can coach and lead others as the skill. So my vice president of services can go do the incident response case, so he can lead that team. My vice president of marketing, she gets every aspect of it, so she can lead that team. And so one of the things we're really careful of and one of the things we really try to avoid is nobody gets a pass of, well, they're really good at this business thing or whatever else. So we'll put them there even though they might not be good at that. No, they have to be able to do what their people are doing.

Mike Kearney: That is fascinating. What about advice for an up and comer? So if you were to go back to when you were in the Air Force Academy, you put yourself in this situation of a kid that's in college, what advice would you give to that individual irrespective if they're gonna go into cyber or not?

Robert Lee: I think there's no excuse to not be empowered in your journey. And what I mean by that is regardless of the technical skill you want to develop, even if it's not cybersecurity, I don't know I can give completely broad advice, but especially in the world of tech-ish anything, there's so many online resources and free resources and everything else that you can self-educate on so many wide topics. Harvard has free online classes; MIT has free online classes. I don't think everybody starts from the same position of privilege in life to be able to actually go do anything.

But to actually teach yourself to be able to do those things is a different discussion. And if you are afforded the luxury of a nice life where you could go home and check out Netflix and hang out for a couple of hours and you come into the job interview and you don't know a technical skill, and you'll be like I hope you can teach me. Well, why don't you teach yourself? Did you have the opportunity? If not, that's different. But if you had the opportunity and you didn't take it, why do you want to do it on my dime? I completely agree with taking your people and training them into whatever else.

But if you are a young person and you want to get into this field, you better show that you are able to take advantage of your own path, that you're able to actually take care of yourself, then we'll amplify it. Then we can unlock the gates for you. But you've got

to actually show you can get after it.

Mike Kearney: Hustle. And it's be ready. I totally agree with you. So I've been dying to get to this because I think it is so fascinating, I'm curious why you started *Little Bobby*.

Robert Lee: Oh, gosh.

Mike Kearney: And the book that preceded it. And what I'm really curious of is, what inspired you? But I also think that there's potentially some creative genius, and maybe not, but of explaining really complex topics in a way that people can get.

Robert Lee: So I'm afraid that the story is not gonna be again setting the expectations of you think it's an intelligent story.

Mike Kearney: Maybe explain what *Little Bobby* is first.

Robert Lee: So *Little Bobby* is a comic I run every week. Every Sunday Jeff Hass and I do this. Jeff Hass illustrates it and I write it. And it's a three-pane comic explaining some complex security topic or a lot of times a fair amount of snark or something about it.

Mike Kearney: It was like somebody said I think I read *Calvin and Hobbes* was your inspiration?

Robert Lee: Yeah. So we modeled it off of, like my inspirations were *Calvin and Hobbes* and *XKCD*. And so I did it focused originally on industrial and it's been the larger topic. Where it came from is a little bit dicier. The original book, so effectively, at my time at the National Security Agency I was asked to go explain to another team how to do SCADA, so industrial offense. And I was completely against the topic. And it was this combat and command team. No, Rob, you will come brief us on how to do SCADA offense stuff. We're the—we are the SCADA offense team and you're gonna tell us what you know about these environments.

I was like okay. Salute sharp, move on. So I go down there and I prepare a two-hour briefing on if you're gonna do this, don't do that. Here's how you get into that person's electric grid, all these things. At the end of the presentation, no questions the whole time. At the end of the presentation, one guy raises his hand and goes, so what does SCADA stand for?

And so I left and I wrote *SCADA and Me: A Book for Children in Management*.

Robert Lee: And people actually liked it so we self-published it on Amazon and it sold, I don't know, 20,000 copies or something around the world. It just went crazy. And I was having engineers call me and be like I can explain to my son what I do now. This completely snarky, cynical book ended up being this extremely important thing to people. And so it's like maybe we should keep doing this. We just had our 205th week or something and so every Sunday I publish it out. And then we published another one that was *Threat Intelligence and Me: A Book for Children and Analysts*. And that one's a little less snarky and more educational.

Mike Kearney: I'm sure you get the fact that there is brilliance in it because there's so many topics that people just can't get their mind around. But by putting it into that comical, whimsical way—

Robert Lee: It very much helps educate people. I wrote an article for a bunch of congressional staffers explaining why backdoor as an encryption and blockchain were all stupid. They didn't get it until I put it into six comics and they were like I totally get it now. I'm like okay, we're good.

Mike Kearney: You have a second career now. But do you think, in all sincerity, do you think by doing these comics it's increased awareness to actually help you with what you're doing at Dragos?

Robert Lee: I think it does. None of these things are ever, teaching at SANS, maybe doing comics, none of the community stuff was ever like I'm gonna build a company and it's gonna be awesome. But what I find is everybody we interact with, they see *SCADA and Me* on an engineer's desk or something in a company I go to. Or I'll be at a conference speaking and I'll be, how many of you have taken one of my classes or seen *Little Bobby*? And like 60 percent of the people will raise their hand. Well, crap, it's just a lot further and wider than I really would have expected it, and it's very humbling.

Mike Kearney: Has it influenced your marketing at Dragos?

Robert Lee: No, I try to keep them separate. My marketing leaders are like, can we use *Little Bobby*? I'm like, don't bastardize it. Please don't leverage—

Mike Kearney: But has it influenced the way you think about marketing and telling your story to clients?

Robert Lee: Yeah, okay. Absolutely. 'Cause I know no matter how much I think I'm not just drizzled in technical jargon that I know even on the podcast when I'm trying to be like, oh, let me talk about risk, no, it's massive technical jargon. And so I always remind myself by thinking about how would I put this in a comic. My board slides, I really made board decks and I had five slides in a comic and it's been the best board deck ever for these other companies to understand.

Mike Kearney: I honestly, and I'm not just trying to kiss your rear, when I was reading those prepping for this, I was like, oh my god, this actually may influence, maybe I'm not a Little Bobby, but just the way that it's described and the humor that's in it, it almost allows you to take any really complex topic and convey it to people who may not understand the underlying technical nature of it. We're getting to the end. What's the best part about being the CEO of Dragos?

Robert Lee: There's internal and external, right? So internal it's seeing people go do things they never thought they were able to do. To be able to be invited into a nuclear reactor or be invited into a manufacturer of a global food and beverage company, those are crazy things. And to know that we built something that if you're really doing intelligence or certain response work in this community, you will come through our doors at some point. That's just cool. Externally, it's the customers.

And I know that's a very CEO answer, but you go to their sites and there's a buzz around security and they're like hey, we never had access to the plants before but now we can communicate with our operations folks and deliver value. Oh, man, and you kind of just feel like you're making life hard for the adversary. I want to know that there's some Russian or Iranian, whatever team that spends millions of dollars and

years in training and develop the capability and then they go up against one of our customers and some dude that's got a GED that he worked hard and he didn't have the luxuries of life, he worked hard. He didn't have a million certifications and a PhD or whatever, but he got after it. And he's sitting in front of our technology and goes no. And he just stops it. That to me is gonna be an amazing feeling of Russia's finest against Bubba. And Bubba destroys them. And I'm so excited about that.

Mike Kearney: Well, there's a theme of this empowering people that's kind of consistent throughout this entire conversation. What about the most challenging?

Robert Lee: Most challenging is telling people no. You love them, you want to empower them with anything and everything, but standing as the gatekeeper going, you know, engineering team, I know you want ten more headcount, but if I look at the burn and I look at what we're doing and I make that choice for you today, it's gonna impact in what we can do in 18 months from now, and I'm sorry but you've gotta do the job with what you have for today. Let's talk about it next quarter. And standing in front of your team that you love and telling them that you can't empower them on something, it's a hard choice.

Mike Kearney: So I started asking this next question, which I think is my favorite question, and so I'm really curious to hear your answer. So I'm gonna tell you what the cliché question would be and then I'm gonna ask my real question. There's always that, hey, how do you define success, which I hate. But when you define success, what would you not include in your definition that most would?

Robert Lee: What would I not include in my definition of success?

Mike Kearney: So, one would argue like money or whatever, but when you think about success and how you define it, what would you not include?

Robert Lee: So, especially from a venture-backed company perspective, I don't think being the market winner is successful. So I hear every venture capitalist, every Gartner analyst, and I say that lovingly to Gartner, but you gotta pay the tax. No, I say that lovingly where I see all these pundits come out and go, who's gonna be the winner of the industrialists? Dragos is on the way to be the winner. And I actually think we're doing the community a disservice if we're the winner.

I think there should be an ecosystem of players. And don't get me wrong. I want to beat my competitors like crazy. I don't want to hear the lamentations of their sales engineers. Don't get me wrong. That being said, if it's just Dragos in five, ten years in this space, in what we're doing then we haven't built a community. If we're truly educating and training other people, then there's gonna be other companies nipping at our heels and it's gonna force us to be better. And so I think being the winner in this space is not what I would define as success.

Mike Kearney: Wow. And would you extend that to even personally? Meaning it sounds like what you're saying is, it's not just about me. It's about the team like you're talking about.

Robert Lee: I think with the industrial community there's a place and a risk, where the IT security and competence and businesses think that ICS is an add-on. We can throw in a dissector for traffic analysis and some other product. Or oh, we can just give this to IT to deal with. And if you don't really defend the industrial space, there's gonna be a

future where people get hurt. This isn't about missing a patch and having a breach. This is about people dying.

There was an attack in Saudi Arabia in a petrochemical facility where a state actor literally tried to kill people at that plant by removing safety functionality from the systems. This isn't the normal game. And industrial isn't a segment in the market. It is an industrial world, and I think if you're not careful of how you build that community, it could just slip into, oh yeah, we can handle that with our normal strategy and people get hurt.

Mike Kearney: I'm keeping that question. That is one of the best answers, so thank you. Last question, although it's two-part. The question is, what do you think are the most important attributes of a resilient leader? And you've seen a lot of, I would imagine, people that really demonstrate resilience. And then the second is, is there somebody that you would call, it actually can be an organization, it can be whoever you want. But is there somebody you say that person is resilient?

Robert Lee: I'm gonna be cliché on the second one. But on the first one, the first part of the question, I think, and it goes to resiliency, but I think anything that you're doing and you're doing well and it's worth doing is gonna be lonely at some point. And I think it's gonna be an incredibly difficult thing, and you just have to be ready to be knocked around. And I know that's a cliché kind of answer, but if you're gonna be a resilient leader, you have to understand that you're going to piss off people in what you're doing.

And you have to understand the path you take isn't going to make everybody happy. Otherwise it wouldn't be a path really worth taking into finding kind of a new success strategy. And at the end of the day, getting knocked around in that way could even, again, very cliché, but could even lose you friends and peers and people that you wanted to hang out with and be at the ending line with. And if you're going to really get after it, you have to stick the course. And I think that's a harder thing to do than it is to obviously cliché kind of say.

On the who really inspires me, who do I think about, my super cliché answer is my dad. I have Vietnam veteran, Desert Storm veteran, kind of always took care of the family, was always there for us, was always present. If I look in the business world, I don't know, it always changes. But there's various characters that you don't know that you like. Like Mark Cuban is the kind of guy that's seen like this on a swagger aspect of it.

I think you see political figures that you really like. I think everything politics these days pisses people off. But I always liked Condoleezza Rice and how she spoke to the American public. I would just say that there's nobody that you could probably idolize your entire career after. But when you see people that are kind of those silent leaders in their space that don't necessarily need the Twitter fame and everything else, you want to be more like those people.

I'll give you an example. I would never give him the card to be able to have me call him somebody I look up to 'cause he would harass me forever about it. But I'll give you an example. I come into this world of I'm protecting critical infrastructure, I'm in cybersecurity against state actors, this is starting like I'm not protecting a bank. I'm

protecting the industrial world. It's sort of like a-ha. It's kind of hard to feel bad about what you're doing. And my director of intelligence, Sergio, and his wife, Sherri, they do all that and then Sherri built a nonprofit where she does data analytics to identify human traffickers. And last year alone, they freed a thousand women. And I'm like, dammit.

Mike Kearney: You've one-upped me.

Robert Lee: Yeah, I thought I had something. And not only are you're protecting industrial but you're freeing people in modern slavery? God, it's beautiful. And it's just absolutely beautiful. And so I think it's important to constantly have people that you feel are one-upping you and that's fun.

Mike Kearney: What an awesome way to end it, Rob. Thank you. This has been great.

Wow, that was incredible, Rob, thank you for your time, thank you for visiting our offices, thank you for educating me, educating the listeners, and likely educating a lot of our clients. This is something that if you have industrial control systems in your organizations, you absolutely need to be getting ahead of. And I'll be honest with you, some of the things that shared with us kind of scared the crap out of me, but that's a good thing. Because we need to be aware of these risks, and there are three key things that I'm taking away personally.

The first is like traditional cybersecurity, organizations that have operational technology have to act fast. If you're on a board or if you're an executive and you have operational technology, you better start talking to your CIO and your CSO to understand what plan they have in place. The second is, just because you are a cyber professional doesn't mean you have operational technology experience. So if you're a company looking to engage somebody, make sure that they've got the right experience.

And then finally, and this is the half-glass full, if you are out there, if you're going through college right now or if you're looking to reinvent yourself, I would say look at a career in cyber. There are so many unbelievable opportunities, and there are so many opportunities out there. I know from personal experience that we can't hire cyber people fast enough. And now with this industrial control opportunity, it's even greater.

Now let me thank everybody that's out there. Listen, this podcast wouldn't exist if you guys didn't listen, so thank you very much for listening to Resilient, a Deloitte podcast produced by our friends at Rivet Radio. I love saying that, our friends at Rivet Radio. Because, in fact, they do such an incredible job supporting us, producing it, everything. If you're interested in finding us, you can find us at deloitte.com or you can visit your favorite pod catcher, iTunes, SoundCloud, Google Play and even Spotify, keyword Resilient, and check out some of our previous episodes.

We have great interviews with CEOs, board members, and other leaders. If you liked my conversation with Rob, go back and check out my conversation with Jackie Rice, a good friend of mine. And she's got some leading-edge perspectives on modernizing risk. And as you may recall, she was the first CRO at Target following their cyber breach. And if you're enjoying these conversations, do me a favor. Give me a rating. That's all I'll say about that. And if you really want to provide any feedback, go to LinkedIn or Twitter. LinkedIn is just Michael Kearney, last name is K-e-a-r-n-e-y. On

Twitter, mkearney33. I love recommendations for guests. I love hearing what you had to say about this episode. So visit me on social media.

And now that we're done, I just want to pause and I just want to think about what Rob had to say. And I want you to make sure that you understand what your plan is that you have in place to protect your organization from these cyber threatsthreats in operational technology. And if you're not confident that you do, go figure it out quickly because this is a significant risk.

[End of Audio]