"There're still folks out there that want to run a really punitive program and really advocate for that, and they swear by it, because if you train to a very specific behavior and you have stiff consequences for noncompliance, it's going to work, you're going to get that specific behavior. I don't argue with that, but I think a lot of CISOs will tell you that what they want to see is engagement, and if you run a really punitive program, and your materials aren't engaging, and you're not inviting people in, you're also not teaching them how to think."

MARCH 23, 2020

The Demand for Soft Skills

Presenter: Lisa Plaggemier

Summary

The current global industry talent shortage proves to be a tough challenge and while having impressive technical skills are important, showing skill in creative problem-solving and communication may put you above the rest. Join Brian and Lisa Plaggemier, CSO at MediaPRO, as they discuss a new perspective on training and awareness, the difference between training to solve a specific problem and thinking critically, and the secret to engaging your employees.

Transcript

Brian Contos:

Welcome to the Cyber Security Effectiveness Podcast, sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve, and communicate security effectiveness. I'm your host, Brian Contos, and we've got a really special guest today. Joining me is Lisa Plaggemier. Welcome to the podcast, Lisa.

Lisa Plaggemier:

Hi, thanks for having me.

Brian Contos:

Hey, Lisa, we met at a FutureCon event a few months ago.

Lisa Plaggemier:

That's right.

Brian Contos:

And I saw you give a talk, and I was really excited about it. I'm like, "Wow, you would just be a great individual to have on my show." I really want to ask you about some of the things that you've been working on, as it relates to security awareness and training, et cetera, et cetera, but before we get there, I'd love it if you could give our audience a bit of background about you, and the path you took to where you are today, and what it is that you exactly do right now.

Lisa Plaggemier:

Sure. I'm Chief Evangelist for InfoSec, which is an education provider, a personalized education provider, and a Chief Evangelist is just a fancy way of saying that I help people with their training awareness programs, serve the larger community of practitioners, really advocate for the role that they're in and the job that they do, and advocate for best practices. I speak at conferences, teacher training and awareness, certification class, things like that.

Brian Contos:

Lisa, you made the jump a while ago from industry to vendor. The scarlet V for vendor. We always talk about it. What's that been like making that transition?

Lisa Plaggemier:

Yeah. I like to joke that I went to the dark side. It's been good. I'm a super social person and working with so many different people is really rewarding for me. The larger community of people that do training and awareness is really collegial. I think we find that across the security industry, but in particular in training and awareness, all the vendors in the space are collegial and friendly so that's really good. I mean, we compete really hard against each other, but we all share the same mission and that's been great.

Brian Contos:

Yeah, that's awesome to hear. Well, I know you travel a ton and you speak at events all over the country. What are people saying about training and awareness? Where does it seem to be today?

Lisa Plaggemier:

Well, let me preface that with a little bit about my background. I started in marketing and sales for Ford Motor Company, so I was marketing and merchandising cars and trucks in the U.S., and Europe, and AMEA, and those first jobs that you have out of college, I think it can really mold you and automotive is an incredibly competitive business. Anybody who works in automotive will tell you quality is paramount and the competition is fierce, margins are razor

thin, things like that. So, doing sales and marketing in that environment, you really had to be on your toes and you had to understand how to sell the value of your product and all those things.

Lisa Plaggemier:

I was actually working for an automotive technology company when I got recruited into security. I got recruited specifically because I had a marketing and sales background. I was at a company that was being spun off from a large corporate parent, and so we had about four months to grow a security program from scratch, which was pretty aggressive. So, I was approached by the CISO to run a training and awareness program and I immediately got hooked as soon as I got to know the team and what they did. I think that very first incident call that I was on, just a few days after we'd been spun off, there's an adrenaline rush and a focus that goes with that incident response and that type of clarity of purpose and teamwork, that was really appealing to me.

Lisa Plaggemier:

But anyway, when it comes to where people are on training awareness today... So, I was recruited by somebody who wanted the right talent for that role, right? Wanted a creative thinker, wanted somebody with good soft skills, background in marketing and sales, really good at... Because I'd worked for a technology company in marketing, I was really good at translating from technical jargon to layman's terms, explaining a value proposition, all those things. And I think a lot of CISOs are realizing just what my first CISO realized was, that it's much easier to take a creative soft skill person and give them enough security education to do the job of security training and awareness, than to take someone who's highly technical and to try to teach them to be creative, and communicate well, and understand all those techniques you use to get and hold people's attention and influence their behavior, things like that. Those CISOs understand.

Lisa Plaggemier:

Also, I think that, just like I was involved in incident response, those soft skilled people can be really versatile, just beyond training and awareness. I did executive comms and internal and external communications during incident response. Whether it was to FAQ for sales or support or customers or whatever, working with the crisis comms team, the PR team. I also worked on marketing some of the security features of our services and our products. So all those things go beyond running a training and awareness program so you can really get a lot of value out of that role.

Lisa Plaggemier:

Unfortunately, I still see CISOs that haven't really seen that value yet. I talked to some folks that... I'll give you an example. I got in a carrot versus the stick debate lately. I was having a few beers with a CISO at a major conference that one evening. And there's still folks out there that want to run a really punitive program and really advocate for that, and they swear by it, because if you train to a very specific behavior and you have stiff consequences for noncompliance, it's going to work, you're going to get that specific behavior. I don't argue with that, but I think a lot of CISOs will tell you that what they want to see is engagement, and if you run a really punitive program, and your materials aren't engaging, and you're not inviting people in, you're also not teaching them how to think. You're teaching them to have a specific response to a specific issue, or you're teaching a specific behavior.

Brian Contos:

Yeah.

Lisa Plaggemier:

And most CISOs I think will tell you that because technology is so pervasive, and in every type of role in the company, and Shadow IT is an awful, terrible problem that keeps... So even the first CISO used to say what keeps him up at night is the stuff he doesn't know about, and that was really a Shadow IT problem.

Lisa Plaggemier:

I think we want that engagement because we want people thinking for themselves, not just having a response to certain stimuli. We also want them to think for themselves, and to involve us upstream, and wonder for themselves, "Is this tool, or this process, or whatever I'm working on, is this secure? Should I be involving the security folks? Do I need a process review? Do I need an architectural review?" We want [that] demand for services, and the business coming to us, and wanting to work with us, and that's all culture change, that's all engagement. If you're punitive and you're rigid and that's the way the security team runs training and awareness, and that's the way they communicate out to the business, then you're not going to get that engagement and you're going to be left out of those conversations and that's when you have bigger problems down the road.

Brian Contos:

Yeah. No, that makes really good sense. You know, you hit on something there a minute ago about soft skills, and everybody's talking about technical people needing soft skills today, and a lot of people were saying, "Ah, this is not really that much of a requirement." But you've been preaching this for a long time. Now that it's gotten the spotlight a little bit, what should they actually be doing for people to develop... Just go, go develop some soft skills.

Lisa Plaggemier:

Yeah, it can be really hard. Like I said, I think it's easier to take a creative person and train them on some of the issues, as opposed to taking somebody who's a great and a fantastic engineer and then try and train them on soft skills. I would say just don't be afraid to hire from a variety of backgrounds, and hire for aptitude as opposed to somebody's current understanding of security. I talked to a lot of frustrated security engineers or people that work in a SOC that have been tasked with running a training and awareness program 'in their spare time'. And they know that they don't have the right skills, and they know they're not doing the function justice, but there isn't any other dedicated resource, and so it frustrates them because they know it's a critical piece of layer defense. They also know they don't have those skills.

Lisa Plaggemier:

There are more and more types of training popping up to try and teach communication skills and creative skills to engineers and things like that, but I think the other thing you remember is that there is economics at work here. Are you going to want somebody, a highly paid person in your SOC working on training and awareness? The reality is that marketing people are not as expensive as security people.

Brian Contos:

Yeah.

Lisa Plaggemier:

Recruiting for some of those soft skills, it just looks very different. And, I think we've all gotten... You know, whenever we have turnover in our departments, it can be grueling. It's hard to find people with the right skills. It can be really expensive, it can take a long time to fill the open rack.

Lisa Plaggemier:

But I think if you have... You know, I was kind of a jack-of-all-trades because I was doing a lot of communications, and board presentations, and a lot of things that were coming out, you know, spun out from that training and awareness program. So, I kind of took the load off of some of the other folks when I would help them put together their slides or their message from whatever part of the security team it was. If there was information and we were trying to report up and out, I would help them craft those messages. And so that took that burden off of them so they could go back to doing the work that they're really paid to do.

Brian Contos:

Yeah. Well, let's play that forward a little bit. You know, you're hiring these creative people into the security field, so this is exactly what you did. You know, you were in marketing, you did all these things. What was that like for you personally, being a creative sort of thrust into the security field?

Lisa Plaggemier:

It was a little bit lonely, to be honest, at the outset. I was definitely the oddball on the team. There are few, kind of more concrete thinkers that would roll their eyes. Like, what is she doing here? But I had a few people that I sought out in the department that I like to say... they spoke Lisa, right? I mean, I remember the first engineer that explained a flat network to me and he said, "It's like when you break into the mall, one store in the mall and you can get into every store in the mall." And I'm like boom, I got it, right?

Brian Contos:

Yeah, yeah.

Lisa Plaggemier:

I'm off running. So, I knew who to talk to about things, who would sort of translate for me so that I could translate for the business. Sometimes I do have to check myself and make sure I'm not missing something. I had a question, I was doing a webinar, I don't know, six or eight months ago and during the Q and A at the end it was all about training awareness. Somebody asked at the end, “My company doesn't have policies developed yet, so how can I start a training and awareness program, cause we don't have policies?” And that just struck me as such rigid thinking, you know? Yes, in a perfect world, if it was textbook, you'd have policies, and guidelines, and standards, and all this great stuff, and have a framework for your training awareness program. But what came out of my mouth at the moment was, "Do the bad guys care that you don't have policies?"

Brian Contos:

Mm-hmm.

Lisa Plaggemier:

Isn't there something you could... You know, you can be training on phishing, and using a VPN, and there's a million different things you can be training on that you can still do even though you don't have policies carved in stone.

Lisa Plaggemier:

And I think that's the one thing that creative people were willing to do, is take a little bit more risk and not let perfection be the enemy of the good. Just get started, just do something right. The worst thing you can do is nothing.

Brian Contos:

Yeah, yeah. You know, it is interesting though, security people do think A then B, then C, then D. Juxtaposed to, well maybe we go B, then B, then A, then B. It's not quite as linear, and I love the way you put that, you know that the bad guys, they don't care you're going in a linear state.

Lisa Plaggemier:

Nope. They sure don't.

Brian Contos:

So, let's get into some stories then. I know you've had some really interesting stories as it comes to security and awareness. Maybe some horror stories even but share couple of those with us.

Lisa Plaggemier:

So, the presentation that you saw in Detroit was about a program that I ran, an awareness and training program that was a game show and the game show host was a made up sort of Eastern European, maybe reformed gangster type character named Pavel from Bokrania. And we did a series of videos--

Brian Contos:

Who was absolutely amazing by the way,

Lisa Plaggemier:

Thank you.

Brian Contos:

It was so funny and so well done. I mean it...

Lisa Plaggemier:

He was an improv actor and a comedian, and who better to hire to do your awareness program than improv comedians. Right. Anyway, so when I was... It was a wacky idea, right? It was an ad agency that came up with this idea and it was absolutely wacky, and we loved it, and it was great, and it got a lot of attention. I mean, it's something like, I don't know, 50% of the people in the company watched the videos without making any of it mandatory.

Lisa Plaggemier:

And anyway, so before I started the whole program, I was presenting it to the security organization. Just tell everybody, "Hey guys, this is what we're going to do. We're going to do this game show and shoot these videos." And on, and on, and on. And one of the engineers said – kind of pounded the desk – and said, "I don't know why we're using humor to communicate about security. This stuff isn't funny." And I did, I said just to myself, "We know you live in a very dark place all day, every day, and you've... We all see a lot of awful things and wish the world weren't this way." But that's, that's not going to get engagement from our employees. Right? That's not going to... People. Fear is not a great motivator. It's not a sustainable motivator. It causes a fight or flight response. That's the exact opposite of what we want.

Lisa Plaggemier:

We don't want people to just run away and stick their heads in the sand and pretend this isn't happening in our world or pretend that they're not targets. We want people to engage. So, it actually really has made me chuckle, the more I think about that story, cause it's really kind of sad. What other stories have I come across?

Brian Contos:

I just love that impression though, because you know, what do we to do then just sit there and—

Lisa Plaggemier:

Scare everybody

Brian Contos:

—read line for line our security policies and guidelines. I mean, people will last maybe 15 seconds through that, so...

Lisa Plaggemier:

Yeah, exactly.

Brian Contos:

Everybody loves humor, and especially if it's a little bit edgy, which—

Lisa Plaggemier:

Right.

Brian Contos:

—certainly can be challenging these days to be edgy, you got to be kind of careful.

Lisa Plaggemier:

Yeah, we definitely pushed the envelope of political correctness, that's for sure. But that was one of the reasons, I think… The CISO and I had the time kind of thought there's no bad thing, there's no such thing as bad PR. And he was willing to have those discussions with legal, and corporate comms, and HR, and all that stuff and so that's why we forged ahead. The other thing I see that's kind of a little bit of a horror story is companies that have their phishing program run by their SOC because they view it as pen testing of humans instead of having it be run by whoever's doing the rest of their training and their awareness.

Brian Contos:

Oh yeah, sure.

Lisa Plaggemier:

It just becomes a more punitive thing. It's a lot of them blame the user. It's not really seen as training anymore. And I think it creates a disconnect between your true risks due to phishing and what you're actually training people on. And then the other thing I see that I don't really feel is best practice. I mean everybody has different policies and ways they can handle this, but if you're not reading your training and awareness person in on incidents, if they're not part of your incident response team, and you're not reading them in, then they kind of don't know what to train on, right. Those incidents are a really important source of information in crafting the strategy and the plan for the training program.

Lisa Plaggemier:

So, I think that's something that I see. I don't know that it's exactly a horror story, but it's not exactly best practice.

Brian Contos:

Yeah, for sure.

Lisa Plaggemier:

And I think, for training awareness managers I see that are running really good programs are really integrated into the whole security department and everything that's going on.

Brian Contos:

Yeah, yeah. No, I think that's a good point. It does come down to that integration, because if you have somebody just trying to cowboy the whole thing, people feel they're left out, and their message wasn't included, and that's not the way it's going to work in real life.

Lisa Plaggemier:

Absolutely.

Brian Contos:

Then you just end up redoing it again, anyhow.

Lisa Plaggemier:

Yeah.

Brian Contos:

So, with that, let's talk a little bit about advice. What's the best, single piece of advice that you'd give to a training awareness manager?

Lisa Plaggemier:

I'd say to be agile and try new things. Like I said, if you're waiting for every single thing to fall into place, and be perfect before you kicked off your program, you'll probably never get out of the gate. Right? It's not brain surgery, it's training and awareness. I mean, what are you going to what... You know the risk that you have of sort of breaking something is not that great. You know, you can pilot things, you can test your messages with small groups, you can test your training with small groups. You can just... I'm a big advocate for trying new things, and if you need to pilot them or test them, do that, but keep moving as opposed to trying to get everything perfectly. You know, have all your soldiers lined up in a row on the battlefield.

Lisa Plaggemier:

And use some of the marketing and sales tactics. I teach a lot about them in my class. There's plenty of books out there. You know, Dr. Cialdini's principles of persuasion is really all about how to influence people and how salespeople have been doing it for centuries. So, really leaning into those kind of tactics. I mean you mentioned using humor to get people's attention or sell ideas, that can be kind of controversial at some companies, or even with some vendors who don't like to use humor in their training materials. But we see it so often in TV commercials, and I think if it wasn't working, advertisers would have stopped doing it a long, long time ago. Right? Obviously, it's successful in selling things or they wouldn't spend millions of dollars on ads that get our attention and then hold our attention because they're funny.

Brian Contos:

Yeah, I mean look at the most expensive ads, right? On TV during the super bowl. What percentage of those have humor? I'd say probably over ninety.

Lisa Plaggemier:

Yeah, it's a large percent.

Brian Contos:

And there's a reason for that.

Lisa Plaggemier:

And actually, it's funny because the guy who worked on that Pavel campaign with me, the director was the same guy who has directed Superbowl ads. Probably his most famous work was the Chrysler 'Imported from Detroit' Eminem ad from the Superbowl a couple of years ago.

Brian Contos:

Oh yeah, yeah, yeah, yeah. There you go.

Lisa Plaggemier:

Yeah, really talented people.

Brian Contos:

Very cool. Very cool. Well, Lisa, this was great, but I have one last question to ask you before we wrap up, and that's, who's your favorite superhero or supervillain and why?

Lisa Plaggemier:

I got to go with the classic Superman. Maybe cause, my family's originally from Cleveland and Superman is from Cleveland. Most people probably didn't know that. I think also—

Brian Contos:

Cleveland being a suburb of Krypton...

Lisa Plaggemier:

Exactly. I think he's kind of the unsung hero and that reminds me of the lot of the fantastic... You know, in his normal life. You know, very quiet, and unassuming, and all those things. And that reminds me a lot of a lot of people. They are great folks that I've met, doing the hard work of security. Right. They're fighting bad guys all day, and I'm the one who gets up on stage, and RSA and talks about training awareness. But there are people that... The real heroes in this business are the folks that are doing that courageous work every day. So, and they're—

Brian Contos:

Yeah, yeah.

Lisa Plaggemier:

—usually pretty quiet about it and, and kind of unsung heroes themselves. So, I pick Superman.

Brian Contos:

Yeah, the unsung heroes, the self-deprecating heroes.

Lisa Plaggemier:

Exactly. Yeah. Yeah.

Brian Contos:

Well, thanks so much, Lisa, and thanks to our listeners, of course, for joining and be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.