“I always say to people that I can teach the technical skills, but I can't always connect the why. And that's what I think a lot of companies are really looking for now. I've often had pen testers come in to tell me, "Hey, I found this vulnerability." But then can't tell me why that's important relative to other risks to the business or tell me even how to fix it. They'd tell me, "Oh, I don't know how you would fix it in that environment, but here's the risk." And that is not as useful to me as somebody who can come in and clearly express to me, "This is why this is a risk to the business, and this is why this is really important." I think in security sometimes we're very focused on the cool and shiny new things and forget to check and make sure they really do matter.”

MARCH 9, 2020

The Evolving Educator

Presenter: Dr. Meg Layton

Summary

No one’s path to finding a career in cybersecurity is the same, but most can agree that it all starts with education, whether formal or informal. Podcast guest Dr. Meg Layton, Director of Engineering & Cyber Security Services at Symantec, finds her passion in helping others discover their own cyber path and effectively translate their technical skills to aspects of the business.

Transcript

Brian Contos:

Welcome to the Cybersecurity 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 Dr. Meg Layton. Welcome to the podcast, Meg.

Meg Layton:

Thank you so much. Happy to be here.

Brian Contos:

So, Meg, I have a lot of things I want to ask you today, but before we get going, could you give our listeners a little bit of background about you and your path to cyber and what it is that you do today?

Meg Layton:

Sure. I always have a hard time answering this kind of question because we always talk about our careers in terms of your career path and your career journey. And somehow that gives the impression to people that there is a clear path forward. And those of us who are actually living through it, it's more like a jumbled ball of yarn or somehow clear cutting through the jungle to get from one point to the next. So, I'm always very conscious to talk about my journey in a way that I understand that no one person ever has the same experience and resources and background as another.

Brian Contos:

Sure.

Meg Layton:

I think that's pretty traditional actually in cybersecurity. So, here's my quick introduction to the jungle. I graduated college before cyber was a thing, with a degree in political science. Like with most people in political science who do that, I came out and wanted to change the world and really make a difference. And I went to work for a nonprofit which was in the process of installing their very first network ever. And they offered to send me to classes to learn about networking. I agreed. That put me on the technological path. I learned networking, I learned databases, and eventually went to school for my Master's in telecommunications and computing.

Brian Contos:

Oh wow.

Meg Layton:

It was the nineties – dot coms were big. So, I eventually started working for cellular telecommunications company doing business in Africa. And that's really where I found security and fueled my passion for security side of things because the security issues in developing countries are not the same issues as in North America. Or in some cases they're the same issues, but the solutions are different.

Meg Layton:

And so, I really... My first real attempt at tracing network traffic was done through dial-up connections on cellular modems, trying to validate the country of origin and the connections that were being terminated to, and it was at the request of a government that was in the middle of a civil war. It was just this crazy time in my life, but one that I really did learn things through. And really that's... I spent lots of time at the time gathering logs from different countries. They were sent to me via DHL on CDs and I would run scripts, detecting patterns in the traffic and try to come up with what was happening and that sort of thing. And eventually I decided that there was too much that I didn't know and I needed to move from the operational side to the creator side of things and I went to work for a startup.

Meg Layton:

We were acquired by Symantec and I've been at Symantec for a long time. And I work in a variety of roles and security specializations and now I work with a talented team of software engineers and security folks. We build the tools used by our frontline defenders in cyberspace. I often say my job is connecting technology to people to help each side understand the other, to better secure the world. Sometimes it's the developers [that] are the people. Sometimes it's the customer that's the person and sometimes it's a front-line defender somewhere that's the person, but that's really what I spend my time doing now.

Brian Contos:

Wow. Wow. You know, when you were talking about receiving these CDs of log files via DHL and writing scripts to do analysis, it reminds me of my early days at ArcSight when we were talking about near real time versus real time analysis. And if your timestamps are right and your parsing is correct, we can do it in just a few seconds. And sometimes we forget, there was a time where not everybody had these high-speed connections and these massive… And that's how you did it, right?

Meg Layton:

That's how we did it.

Brian Contos:

Real time was measured in weeks.

Meg Layton:

That's exactly right. And you're trying to connect things and if you were able to connect to a system, it was on this dial-up connection that was just a crazy amount of space trying to get things done. I often tell people that it's actually lucky for me because if networks were as ubiquitous then as they are now, I probably would not have been able to learn it at the level I was able to learn it.

Brian Contos:

Yeah, sure. Sure. Well, I want to dive into some of the questions. And you teased it out a little bit there with your work internationally, especially in some of these developing countries. I know one of your passions is really about this next generation of people coming up in cyber. So, tell me a little bit about it. Why is that such a passion of yours today?

Meg Layton:

Well, probably education and being the advocate of lifelong learning was ingrained in me when I was young. Both of my parents were educators. But education and cybersecurity really connected for me a few years ago. I was presenting to a group of middle schoolers, kind of this is what you do. I think it was a career day fair. And they told me they had never heard of careers in cyber. It just wasn't even on their radar. And then, one of the children asked me what was my biggest regret in my career. It hit me that while it wasn't so much a regret as a lesson learned, I didn't realize that people who do cybersecurity are really the unseen people in the world. Children, by the time they get in school, interact with doctors and police and grocers and sanitation workers and teachers and all sorts of different positions, but they don't always think about the creators and the protectors of the technology they use.

Meg Layton:

Technology is really just kind of this thing and they don't think about the people who create it. The media sometimes helps with this. It tends to provide, though, a somewhat skewed version of the roles or the people in them, when you think about television shows. And so, wherever we can provide a kind of this is reality view of the ever-changing cyber world. I think people should take advantage and really help provide that because if we don't work to be more visible, who really will?

Meg Layton:

Nobody's going to paint a better picture of what you do than you, and there is so much potential in this field. The idea of the hooded hacker sitting alone at a screen, while we definitely have some of those, I'm not saying those don't exist. But I'm going to say that's not the only path. And so, there's a lot of people in security who are building policy or creating cool things. Or they're makers, or they're breakers, or they're testifying in Congress, or they're writing books and teaching classes or traveling the world. And there's just all this opportunity. And how do you make those possibilities more visible? So, I started working with the teams in CyberPatriot and teaching some of the scout

badges and transitioning. But we build these kinds of things. So, I'd been teaching some college courses and I really look to expand and help everyone, whether they are young, starting a career or transitioning to a new career, and really broaden the spectrum of understanding of what security really is.

Brian Contos:

Yeah, I love that. And I love how your path wasn't through... You know, I got a degree in computer science and then I did this and that. So many people I meet in our industry, and I don't think this is changing and I actually think this is a very good thing. They don't necessarily come up through what you would assume is the traditional path of computer science, computer engineering or some schools now offer degrees in security. But they come from political science, psychology, biology, some type of liberal arts school or humanities background. So it's such an eclectic mix of people because there's so many different things you can do in security, right? I mean there isn't just one thing. So I really like that about our space. It is very eclectic. It is very unique.

Meg Layton:

Right. And security when you think about it is really that... It is a technical field, but it is driven by traits that only humans have. Things like confidentiality and integrity and trust. Those are all very human things, right? So the more that you understand about psychology of the human or the politics that might lead humans to making one decision over the other, the actual stronger you are in security.

Brian Contos:

Very well stated. Very well stated. So, how do we tap into someone's learning potential then? You're working with people of all ages at all phases of their careers. How do we tap that?

Meg Layton:

So, I think the first thing is you really want to understand that not everyone learns the same way. So when I'm thinking about curriculum, I really think about lessons that are accessible to different types of learners that they can tap into for their ongoing success.

Meg Layton:

And that means balancing out hands-on technical, some guided learning with some deeper abilities for research. It includes things like the history and background of why things are the way they are. While some people learn best in a classroom with other students challenging them and personal interactions with teachers, some prefer self-paced labs and really getting into the zone and kind of thinking through it themselves and explore multiple paths at their leisure. And you have to think through all of those scenarios to create your content and really think through things. And in addition, there's so much from that past that informs the future. Much of technology and cyber is really fundamentally creative from lessons of the past. The more you understand and connect why things exist or why they are the way they are, sometimes it is easier to learn and more importantly remember for the future.

Meg Layton:

So, I'm often reminded of two things when I go in to really teach a class and I'm working with learners. The first is, something... One of my first jobs I was working for a Congressman and he told me, "When you're answering letters, remember that when someone asks a question they probably represent 10 other people who have the same question but don't have the resources or don't know the path or don't have the skills to ask. So, you always want to make sure that you're considerate of that and consider how questions are answered to make it an accessible answer for as many people as you can." And the second thing is something we come across, I think, in security a lot is there is always a reason for a rule. If something has made it into the policy and guidebooks, there's a reason. Somebody did something wrong to make that happen.

Meg Layton:

And so, if you can find that event or reason that triggers it, you have a very interesting background and really can tap into what I think is always great about the security culture, which is the storytelling part of it. Because that's what resonates with a lot of people. That personal experience, the story of why things are the way they are.

Brian Contos:

Exactly. I'm a big proponent of the story-fication of things. People will forget stats and figures and charts pretty quickly, but they'll remember those stories and they can relate to them.

Meg Layton:

Exactly.

Brian Contos:

So, let's play it forward a little bit. You know, someone's, they've shown an interest. They've said, "Hey, this is something I'd like to pursue." What are some of the most challenging things when people start getting into this space that is difficult for folks to grasp when it comes to cybersecurity?

Meg Layton:

So, I think... I always say to people that I can teach the technical skills, but I can't always connect the why. And that's what I think a lot of companies are really looking for now. I've often had pen testers come in to tell me, "Hey, I found this vulnerability." But then can't tell me why that's important relative to other risks to the business, or tell me even how to fix it. They'd tell me, "Oh, I don't know how you would fix it in that environment, but here's the risk." And that is not as useful to me as somebody who can come in and clearly express to me, "This is why this is a risk to the business, and this is why this is really important." I think in security sometimes we're very focused on the cool and shiny new things and forget to check and make sure they really do matter.

Meg Layton:

And so, I do think that the ability to communicate in that risk-based language and the business and risk perspective, doing the thorough and informed evaluation is a challenge. I don't think it's a challenge only for cybersecurity people. I think it's a challenge for a lot of people to learn, but I think it's one of the most important skills that people need to have so that they can communicate at all levels.

Brian Contos:

Yeah. You know, it's funny. It reminds me, when I was in my early twenties I was working for Bell Labs and I was living in Brazil at the time. And I remember my manager gave me my annual review, and in it she said... She said some nice things, but then she said, "One of the things you need to work on is you're technically arrogant." And that was a nice way of her saying, "Look man, you've got to understand the bigger, broader business aspect and stop talking bits and bytes to everybody."

Brian Contos:

And half the time like most people, I'm like, "Ah, she doesn't know what she's talking about." But over a little bit of time, I really processed that. You know, she was absolutely right. It's not about my little fiefdom, it's about... Nobody opens up a bank with the goal of being the most secure bank in the world. That's not a great business model. That's not going to get you funding from the Sand Hill VCs. You're in business to do business and what you're doing has to assist that and align with that. So...

Meg Layton:

Right. And I think for a long time, security gets that reputation of being the people who say no, and I think that's what it comes from. Because they can't say because it impacts the business this way if we allow... If you can change that conversation, that reputation can definitely go away and be transitioned to a partner or a helper who can say, "Okay, here's how we can get business done in the most secure way possible."

Brian Contos:

Yeah. Well, let's focus on people, go a little bit deeper. You're, in a role where you mentioned you have people doing pen testing and red teaming and audits and things like that coming to you with these ideas and reporting up to you. When you're evaluating what people know versus what they still need to learn really, what's that like? When you're trying to take somebody that... They might be one of the best pen testers in the world and they're... With that sometimes comes a little bit of swagger, maybe a little bit of arrogance. I'm being very nice in the way I'm putting this. How do you work with those types of individuals and say, "Hey look, there's, there's still some things that you know, we can improve on here."

Meg Layton:

So, I'm always of the opinion that everybody has something to learn. In security, I think it's very true that that which you know today, somebody else will know more about tomorrow because it's constantly changing and it sometimes does change that fast.

Meg Layton:

And as kind of the educator, I don't want to be teaching the same thing over and over and I don't want to... It's a challenge to assess where different people are in their learning cycle so that I can add to the knowledge base in a constructive way. So I always work trying to get people to explain things to me, either through their own life experiences or through something which is kind of current. For instance, it's not uncommon for me to ask someone just to tell me about a security incident they were involved in, and then I kind of end up with the people who are like, "Oh, well I don't work in the field. I've never been involved in a security incident." And I say to them, "Really? Never? You've never gotten a phishing scam in your personal email? You've never gotten one of these phone calls?"

Meg Layton:

And they really back it up and think, "Oh. No, I did that." And so I say to them, "Okay, well what did you do? How did you recognize it? What were your next steps? Who did you alert?" And that helps me understand where they are learning and working through the incident response life cycle and where I may need to fill in. Or I'll ask about something that might be trending on the news cycle such as the latest threat and say, "Okay, why is that important?" And if people can explain to me in real world terms why it matters to them, I can tell quite a lot about what they knew. I think it goes back to what we were saying earlier. If I can get them to tell me their story, I can assess what they're conscious of that they know and what is underneath the surface that they may still need to kind of structure around.

Brian Contos:

Sure. Sure. No, that's great. I think that makes a lot of sense. Let's play it one more step forward, because I want to take people to the last phase of this, really. You're a hiring manager. You have people on your team. You're seeing some of these folks come up with perhaps nontraditional learning paths and maybe they're learning things through Khan Academy or maybe they go to the O-OSS site or maybe they build a lab in their environment or some combination thereof. As a hiring manager, what are some of the challenges that you're seeing when these job seekers are coming into your applicant pool, if you will?

Meg Layton:

So, I think this was one of those kind of, hey, how valuable are certifications or degrees versus hands-on experience? The challenge is, at least if it is a certification I know and a certification that I have some experience with and somebody comes to me with that certification, I will have a shared experience or a known experience that they have gone through. And the same thing sort of holds true for a degree. If you have gone to the... I got my Master's at Polytechnic university, which is now part of NYU. But if you've gone through a degree program at NYU, I sort of have an understanding of what that may have been like. Right? Whereas if people just come in and say, "I know this, trust me," I don't really have a way to validate that. I don't have a shared experience to work through.

Meg Layton:

So I think that's the biggest challenge job seekers have. They really need to be thinking about building themselves a portfolio of work or something that shows their knowledge, their ability to apply the knowledge, and their ability to learn new things. Software engineers have been doing this for years with GitHub and other locations where they've been putting code snippets for their careers. And security folks need to do the same. It doesn't matter to me whether it is a blog post or they've participated in a capture the flag or as I work through with some of my CyberPatriot students, I tell them, "You need to be able to answer what did I learn from this and what will I do differently next time?" And, "Why would this have been important in a business setting?" If they can answer these sorts of questions about their experience, then you can trust and validate a little bit of that experience and that learning from them.

Meg Layton:

So, I always encourage them to speak at a local meetup, connect to people who can help validate. Yes, I know that person. Oh, I saw them at the local B-sides or I went and I worked with them at the CyberPatriot team. And that really helps them connect, because as a hiring manager, I'm never looking to hire folks who know everything. But I do want to hire people who know how to find the answer.

Brian Contos:

Yeah.

Meg Layton:

Which either comes... So, I will always ask, "Where do you like to look for your security information? What are your websites that you go to? How do you stay up to date? Who can you call?" I always ask, "Who's your phone-a-friend if

you really get stuck on something, trying to solve something? And why do you think that they would take that call? And how do you think they'd be able to help you?"

Meg Layton:

If somebody says to me that they only ever get any of their security information from, I don't know, Yahoo news, maybe that's not the best place you would get it. You have to have more than one source, you always want to be looking to validate things, and you want to be building out your portfolio of, "These are things I have done. And it's not a resume as much anymore as kind of that visible, here are a couple things I can browse through that maybe I can relate to. Say this is my shared experience and get you storytelling about why that's important to the position I have available.

Brian Contos:

Yeah. Yeah. I would imagine, and I don't know, but I would imagine if I was a photographer applying for a job, I wouldn't just have a text-based resume talking about all the great things I've done. I'd probably have, "Here's a bunch of pictures I've taken."

Meg Layton:

Exactly, exactly. And I think that there's a certain artistry to cybersecurity. I certainly have said that to people, but I think people really need to be looking at that because as it changes so fast... Nobody sets out and says, "I'm going to be the first person in the world to do this today." You don't actually know that that's the first time you've done something until eons passed. And so being able to share those experiences and say, "I know it's commonplace now, but when I was working in Africa, we dropped our first video conferencing lines in there and ran the first video conferencing feeds out." And talk about what kind of things that we had to consider, what did the business look like and why that was important. That really changes the conversation, I think, when you go in to talk to people.

Brian Contos:

Absolutely. Well, Meg, as we wrap up here, I have a very important question I like to everybody on our show, and that's, who's your favorite superhero or super villain and why?

Meg Layton:

So, if I have anybody who's heard me talk before, it's going to be no giant surprise to them cause they'll all know what I answer. But it's going to be Buffy the Vampire Slayer.

Brian Contos:

Oh, I love it.

Meg Layton:

I have often thought of doing a blog or a talk about everything I know about cyber I learned from Buffy. I haven't quite gotten that out off my chest yet, but at some point I'll do that. And she, like most of us, just wants to be a normal girl and drink mochaccino and hang out at The Bronze. But she knows that she has to save the world again. And so, she does that and she does it with style. And I think that's a lot of us in cyber, kind of like Buffy just out there saving the world every day because that's what we do.

Brian Contos:

I love it. I love it. Well thank you so much, Meg. Thanks to our listeners for joining and be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.