"I think many of us are really concerned about the information security professional deficit that we're coming upon. And I just don't think that we can tackle it by training and getting more people involved. And, I think we have to change how we're doing things."

MARCH 16, 2020

Layers of Architecture

Presenter: Kathleen Moriarty

Summary

The Internet Engineering Task Force (IETF) is a large community of network designers, operators, vendors, and researchers passionate about the ever-evolving internet architecture. Security strategist, CISO, and board advisor Kathleen Moriarty chats with Brian about the fascinating research she's done, her upcoming book, and recommendations for scaling threat intel.

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 Kathleen Moriarty. Welcome to the podcast, Kathleen.

Kathleen Moriarty:

Thank you, Brian, and thanks for the opportunity to be here with you today.

Brian Contos:

Yeah, I've got a lot of things I want to dig into with you today, some really interesting things, I think for our listeners, but before we begin, I'd love it if you could give us some background about you and the path you took that led you into cyber, and what it is that you do today.

Kathleen Moriarty:

Sure, thank you for that. I started out undergrad as a math major, who didn't even enjoy computers in the least. But yeah, kind of funny, but by the time I got to my sophomore year with some required courses, it started to creep in and I started to enjoy it a bit more, and it was actually assembly language and translating it into machine language that was my trigger. Right? So, and it makes sense firstly—

Brian Contos:

I love that, because that's most people's trigger for not liking computer science, when they get into assembly, but you went the other way so.

Kathleen Moriarty:

Yes, yes, and a particular professor kind of helped me along the path, and I gradually took more and more computer science classes, to the point where I had the equivalent of a Bachelor's in Computer Science, but not declared that way. So, my undergrad is a Bachelor's in Math. And then, that same professor egged me on a bit. I had full intentions of just going on to grad school full-time and he said, "You should interview with all of these companies coming on campus, and take advantage of that experience." And so I thought, "Okay, that only makes sense," and wound up getting a job with PSINet, one of the first internet service providers.

Kathleen Moriarty:

And at the time, networking was just coming out as the next big thing. And a few people advised me very well that I should go to the university I was accepted into locally, and also work and take this position. Because it would be invaluable experience, and they were right. Getting in at that time was amazing, because you weren't siloed. I was able to learn everything from BGP, to Sendmail, to DNS BIND, and work with some really great people who I'm still in touch with today. It's a huge opportunity, and then started focusing in on information security. So, I had this really nice background from that first position while I got my master's.

Brian Contos:

Now I've got to ask you, when it came to Sendmail, did you have the big Sendmail? A book with the bat on the cover?

Kathleen Moriarty:

Oh, of course. Of course. And—

Brian Contos:

That thing was like a phone book. I remember that too. I was like, "This is the biggest book ever. Sendmail is such a pain."

Kathleen Moriarty:

Yeah, and we would have to walk customers through fixing Sendmail CF files. You know, I remember having nothing in front of me and just walking them through and being able to fix them.

Brian Contos:

Yeah.

Kathleen Moriarty:

A long time ago. They don't do it that old anymore.

Brian Contos:

Trial by fire. Yeah, yeah. That was a rough time for mail.

Kathleen Moriarty:

So, then I went on to FactSet Research Systems and within a year or so, became a director of information security, and my passion for the field just grew. I had a one-year stint following that at a performance company. And I realized with one year, I need to get back to information security. So then, I was fortunate to get a position of head of information security at MIT Lincoln Laboratory, which was a fantastic place to work. I was there for seven years, and it was a really nice and challenging environment. It's 65... At least at the time, it was 65% PhDs. So, you can't just make a policy up. Right? You have to be able to argue it out. You have to have a really rationalized view of it. And you can't go to lunch without having a discussion on the new topic. And I loved that. Right?

Kathleen Moriarty:

So, I kind of thrived within that environment, because it always had me thinking and kept me on my toes. So, it was a really wonderful experience, but stressful. Because of the work and information that you have to protect at MIT Lincoln Laboratory. And I'll be clear, I was on the unclassified side. There is a CISO, that is overall on the classified side. So, I wouldn't want someone to get the wrong impression there. But, I did decide to move on because of the stress of it, and I enjoy sleep at night, so···

Brian Contos:

Not a lot of sleep at Lincoln Laboratory.

Kathleen Moriarty:

No. No. No. Not so much. Just there's too much at risk. And then I went on to do consulting. Figuring I could do the same type of work, get into different companies, provide the risk levels for their decisions. But ultimately, it was their decision and that worked, in terms of stress levels. But the other interesting... I guess there is two interesting aspects of it that were career shaping, one was that I got to get into every single industry, right? And get a nice view of what works and what doesn't work, as we helped with information security program development or audits.

Kathleen Moriarty:

And the other aspect was I was eventually moved up to be the team lead. And was leading a team of peers and all former CSOs, some more senior than me. But I really learned one of my strengths as a good peer manager, and so I tend to have a collaborative leadership style that worked really well, especially for that team. Where everybody's voice was heard and we were able to advance our programs collaboratively. We had really good people to work with.

Kathleen Moriarty:

Then, I had a jump from there, internal within EMC, where I moved into the office of the CTO, based on some research work that I had been doing. That opened up the door for more research opportunities, and changing my career a little bit, and more involvement in the IETF.

Brian Contos:

Yes. And I'd l... I want to really dig into the IETF here. Because I remember thinking back, and it tells you how geeky I was. I think it was about 1999 I started reading a lot of internet drafts, which eventually, RFCs as well, and I think it was RFC 2549. Yeah. RFC 2549 which was IP over AB and carriers.

Kathleen Moriarty:

Oh. Sure.

Brian Contos:

Yeah, right. It's the comical draft. We all... We all ran out like, "Wow, this is really cool." And then I found out the other drafts and RFCs aren't this interesting. I remember getting into that. But maybe you could give us just a very short synopsis of what exactly it is that's the mission for the IETF. For those that aren't quite aware, and then, of course what you're doing there as well.

Kathleen Moriarty:

Sure. The IETF makes these standards that essentially make the internet work. And so, in the tier standards bodies, they have handoff points where different standards bodies typically work on different layers of the stack. So, Itripoli is a layer below and the IETF sits on top of that. Right? So, they do routing protocols, transport protocols, transport encryption, endpoint security to some degree now and DNS. All sorts of internet-based protocols. And then, there is like W3C that's a layer above that, who is... So, the IETF does Divine's HTTP, but W3C is webspace operating on a layer above that. So, the core internet protocols, IP, IPSec. Whole list of them. And in terms of what I've done at the IETF, after involvement for more than a... I guess it was probably at least 15 years, I was appointed to the role of IETF security area director and the... All of the positions are on a volunteer basis and they're nominated and then selected based on worldwide community input.

Kathleen Moriarty:

So, it's an honor to be able to serve in that role. And then as IETF area director, you have a co-area director and between the two of you for the security area, you manage all of the working groups that are active. And so at any given time, you're managing about 10 to 12 working groups. And, at the same time, you're also reading every single document that comes through for final publication. And when you're doing this for security, you're looking specifically; was there a glaring security hole that was missed? Or do I need to question something to ensure that a particular decision was made because of working group consensus, whether it's right or wrong? Because sometimes you can ask a question and the answer is, "Well... Nope, the documents going to stay that way for these other reasons." And maybe they are very good reasons.

Kathleen Moriarty:

So, it was really great to serve in that role. And then also to get the view across all of these different protocols of what's changing and emerging in the internet space. Right? So, not all these protocols will become active or used within a few years. The timeline is usually a little further out. So, it was nice to get that broad view into these trends.

Brian Contos:

Yeah. Yeah. And what's nice about it, it's that broad view, but you're sort of there at... Essentially ground zero of it. Right? So, you're... It's that deep thing which I love and always very impressed with how that all came together.

Kathleen Moriarty:

And so many great people to learn from.

Brian Contos:

Oh yeah. To me, it sounds like that was a nice sidestep from Lincoln labs. Right? Because it's a...

Kathleen Moriarty:

Yes. Yes. Very different. And it was a fun role and lively. There's a lot to manage.

Brian Contos:

Yeah. So, now you've recently put a book together and I'll let you talk about it. But, congratulations by the way. And let's hear a little bit about that.

Kathleen Moriarty:

Thank you. I'm not quite done with it. But, it is feeding off of that IETF work and observations. Pulling together five different trends and they're not all in the security area. But, taking a look at these five emerging trends. How they intersect and how that might lead us to more secure information. Security postures with the need for a lower number of professionals to manage them. I'm... And I think many of us are really concerned about the information security professional deficit that we're coming upon. And I just don't think that we can tackle it by training and getting more people involved. And, I think we have to change how we're doing things. And so, that was the premise of the book and the suggestions and recommendations within it that feed from these five trends.

Brian Contos:

Now that's I think... What a timely book. Right? I mean that's top of mind for virtually everybody in our space. And let's—

Kathleen Moriarty:

Just have to get it done.

Brian Contos:

Yeah. You have to finish it. That's all. That's the easy part.

Kathleen Moriarty:

Small details.

Brian Contos:

And words on a page. So, one of the things that I hear a lot about in terms of scale and as it comes to that... That deficit of skilled cybersecurity folks is threat intelligence. Is there a way, in your opinion, to get threat Intel to scale?

Kathleen Moriarty:

That's a great question. The way we're doing it now will never scale in my opinion. You can't expect people to share them within local and regional sharing groups. And have an individual at every single company that can pull that data in, digest it and push it out to all of their infrastructure. That just doesn't scale and never will. So, I've written blogs on this in the past. And, I have been thinking about it even more. But I believe we have to switch things where the vendors responsible for the software and code that has the vulnerabilities, are going to have to take the ownership of those problems in order for us to move beyond this mindset where we can have add-on products. And that goes into some of the intersecting trends. And I would go on way too long if I went into it here. But I do think we'll get there in time and it's almost inevitable.

Brian Contos:

Yeah. Well, I liked the way you put it. The way that we do it now won't work. So, we have to readdress it because it's... It won't get better by itself without making some change. Which actually brings me to my follow up question. I know you've done a lot of work on TLS and some of the different versions there for strong transport encryption. And, that's making... It's driving a lot of architectural changes and some decisions that are being made there. What's your perspective on how organizations should be addressing these changes that are happening in that area?

Kathleen Moriarty:

I think that this change needs to be embraced for TLS 1.3. And for organizations that aren't ready to do that, they have time. TLS 1.2 is not going away anytime soon. So, they can continue to use their current architecture that's in place. There's no big vulnerability unless one comes out on TLS 1.2 that's not fixable. Which I don't think will be the case anytime soon. They can continue to operate but, plan for a switch to where our detection and prevention capabilities are more at the endpoint. And rely less on interception technologies that do this in a passive way. And that's really what's going away is the use of static keys where you can passively monitor encrypted traffic. And doing that type of interception actively just doesn't scale. You can't do it at the volume that you could with passive. There was also a study by USC on through the hacking for defense.

Kathleen Moriarty:

Are you familiar with that program?

Brian Contos:

No, I have not heard that one.

Kathleen Moriarty:

So, it's a program where U.S. government agencies come up with projects and then they're published on the various university's websites. But, USC did one looking at this and what is more effective and efficient to do your detection and interception work on the edge or in the middle. And through all of these hundreds of interviews, and I helped on this a little bit, just on the interview side and helping them get additional interviews, was that we should move towards this new model. Right? And so, they even talked within the government and got blessings on this eventual decision in terms of effective inefficiencies being improved.

Brian Contos:

Yeah. Well, one of the things that I know the IETF has been working on is some new work as it could potentially relate to helping with security posture assessments. And is that something that you've been involved with and can you talk a little bit about that?

Kathleen Moriarty:

Sure. So, that would be through the sacrum working groups, security automation and continuous monitoring.

Brian Contos:

Yes. Yep.

Kathleen Moriarty:

So, sacrum is... Their goal is to be able to enable assessments where you are doing the assessment on the endpoint and then pulling that data into a central repository. So, a little bit different than how we've been doing assessments today. Where each product might have their own interface to a particular system and they would use that interface, pull out the same data via different mechanisms into different repositories and perform their analytics. So, this new model, which also aligns with the S CAP 2.0 vision, is to pull the data out using one method. And then your network, your security, your operations tools could all use that data from a central repository where the analysis would be done. So, less taxing on your system, a lower number of tools to manage and such. And then, there's also attestation work that's happening. That's a little different and further out.

Brian Contos:

Very cool. I like that approach. Because to me, it almost reminds me of when SIEM first came on the scene. And this idea that you had this usually ever-growing number of products out there. Security products. And the hope was that by getting log information from endpoint and network and email and all these different other security controls, that you could make heads of tails of the... Kind of the supergroup if you will, or the platform of platforms and to give you that viewpoint. And I think that's interesting from a security posture assessment, if that can be leveraged and you can get that value as you add more products that actually makes you more intelligent. Instead of just running around in a crazy way.

Kathleen Moriarty:

That's a really great comparison. Because they both suffer from... Potentially suffer from the same problem. We need buy in and we need customers to push for these new models. Because they will all fail without a push for this type of model that benefits the customer.

Brian Contos:

Yeah. Yeah, I agree with you wholeheartedly. Well, Kathleen, as we wrap things up here, there's a question that I like to ask everybody that's on our show. And that's who is your favorite superhero or super villain and why?

Kathleen Moriarty:

I'm going to go with the Princess in Black.

Brian Contos:

Ah!

Kathleen Moriarty:

Yes! So, she's a princess by day and then stops... Stops monsters at night so.

Brian Contos:

Well, it's always nice to have a princess by day that can stop monsters by night. It reminds me of, a little bit of Buffy the Vampire Slayer. Cheerleader by day, vampire slayer by night.

Kathleen Moriarty:

Exactly.

Brian Contos:

Awesome. Awesome. Well, Kathleen, thanks... Thanks so much and thanks to our listeners for joining. And be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.