How the US Secret Service Safeguards Data

Agency Deputy CISO Ryan Moore has his sights trained on cybercrime and digital security

Michelle Dennedy: The US Secret Service is best known for protecting the President, the Vice President and their families. But they also protect our financial system and all Americans with their investigative services, covering cybercrimes such as bank fraud and identity theft. Dealing with a lot of sensitive data requires significant privacy rigor, which naturally doesn't get a lot of press. How much rigor? Well, today, we're going to hear about the digital life of the Secret Service.

Cybersecurity, data protection, privacy. If you like to stay ahead of the curve and listen to experts who are leading the way in deriving greater value from data with a more organized approach to data privacy, you're like us, just a few deviations past the norm. You are a privacy sigma rider.

Hi everyone, Michelle Dennedy, Chief Privacy Officer at Cisco here. The investigative arm of the U.S. Secret Service is not as widely known or understood as its physical security services perhaps. I mean, who didn't fall in love with Kevin Costner back in the day? So I'm thrilled to help shed some light, not only on the heroic work that these people are doing to combat crime, such as bank fraud, identity theft, and other cyber security threats, but on the great strides they're making in privacy by design and privacy engineering and leadership. You might be surprised to learn the extent in which they zealously protect data privacy, and what the public sector can teach the private sector as you balance the needs of your business with the rights and wishes of your customers.

Let me introduce the Deputy CISO, that's chief information security officer, for the United States Secret Service, Mr. Ryan Moore. Welcome, Ryan!

Ryan Moore: Thank you, Michelle.

Michelle Dennedy: I'm super, super excited and a little overwhelmed and intimidated to have you on our show.

Ryan Moore: Oh, that's very kind of you. Too kind.

Michelle Dennedy: Well we'll get unkind later, so we'll mix it up a bit.

Ryan Moore: Okay.

Michelle Dennedy: But I really want to know your background, Ryan. I think a lot of people don't understand the intersection of security and privacy, and the Secret Service's role beyond the physical security. Can you talk a little bit about the background about the Secret Service?

Ryan Moore: Absolutely. So, Michelle, the Secret Service was formed in 1865 with the original objective of suppressing counterfeit currency. Fast forward to 1901 as a result of the assassination of

President McKinley, Congress requested our agency to protect U.S. Presidents. Since then our agency's mission has continued to evolve. Today, our investigative mission includes the safeguarding of payment and financial systems from a range of financial and computer crimes, and the protective mission now includes the protection of the nation's highest elected leaders, visiting foreign dignitaries and major events.

Michelle Dennedy: Wow. So, it really covers a lot of ground and it's interesting that the beginnings of this were counterfeit currency. And I imagine as we grow into it and it grows up, Bitcoin and some of these other proxy currencies will be the next great frontier for you guys.

Ryan Moore: Absolutely. The investigation of cryptocurrencies is already something of interest to the Secret Service.

Michelle Dennedy: That's really interesting. So, in addition to being big, strong people that have crafty skills, you have to have a crafty and nimble mind. So what is your role in all of this? Let's talk about what you do for the service, and I want to get into your background, too: about how did you prepare yourself to be a part of the Service and what role you play.

So, where you are today? And then let's talk more about your background and how you came to the Secret Service and your current role.

Ryan Moore: Okay. Well, today, Michelle, I'm the, as you mentioned, Deputy Chief Information Security Officer. That means I'm responsible for ensuring the Secret Service's information security plan and risk management strategy is implemented. To that end, I supervise the risk management process for all information systems that operate within the agency.

Michelle Dennedy: So, I imagine you've got quite a bit of information that's pretty sensitive.

Ryan Moore: Yes we do. Both unclassified and classified information.

Michelle Dennedy: So, Ryan, I also want to ask you, how do you guys measure yourself? You've got classified and unclassified information. You've got agents, you've got people in the field, you've got open investigations, etc. How do you actually meet or exceed these Department of Homeland Security metrics? Is that a centralized thing for the U.S. Government and the agencies or is this something homegrown? How do you do the craft of figuring out your priorities and how you're measuring and metricing ... metricing, I think that's a word? We'll use it today. How are you succeeding in your role?

Ryan Moore: This is actually one of the major projects that I supervise on a daily basis. The Department of Homeland Security publishes annual CIO performance metrics and the metrics cover areas such as asset management, configuration management, vulnerability management, which are fundamental to any organization's resiliency, whether they're in the federal space or the private sector. So we provide the Department raw data that demonstrates our performance across these metrics and then they, on a literally daily basis, provide us scoring feedback on how we're doing in terms of the benchmarks we are required to hit.

And I'm going to brag a little bit about my team. My team has actually achieved the DHS benchmarks across all categories of the metrics for the first time. And it's a very, very difficult

task to do and we actually achieved it last month and we're looking like this month we're going to be able to achieve it once again. So, I'm incredibly proud of my team to be able to do that.

Michelle Dennedy: You should be. So, let's dig into this. This is a pretty epic task and you're in a very complex environment and wide-ranging one. So what are the categories of metrics? What are the — without revealing anything you shouldn't—what are those kinds of categories and what does the team look like to hit those metrics? Are these all homegrown? Are these agents? Are these people you're training? Or is this more of a blended leadership team?

Ryan Moore: Sure, we'll start with the type of metrics first. The type of metrics are collecting information such as can we scan all the systems that we report as an inventory? Can we remediate vulnerabilities within a specific amount of time, based on the severity or criticality of the vulnerability? Can we manage the configuration of our assets to ensure that the software is within its life cycle of support and it's being updated as patches are available?

In terms of the team that actually goes about this process— the leadership is from the agency, the federal side of the agency. But the team that actually performs the work is predominantly composed of contractors from multiple companies that provide services to the organization.

Michelle Dennedy: So, you're a humble guy, Ryan, so I'm going to toot your horn a bit. So this is not a simple, straightforward leadership task. And when we were chatting before, you were telling me something that I think is really important for people to understand, and that's really these concepts of referential leadership versus formal leadership. And we haven't dug into your background yet, but most people would guess you probably come from a fairly formal background with a hierarchal leadership.

So, let's talk first about referential versus formal leadership. How does that come into play when you are dealing with contractors and folks who may not be permanent team members, to achieve that level of success where all across the board you're hitting these really critical metrics?

Ryan Moore: So, in terms of leadership, whenever we bring on a new employee or a new member of the team, whether they're a member of our contract team or a federal employee, the baseline we're looking for is someone to be a referential leader. And our definition of that is they are an expert in their field and they can internalize the organizational values and then demonstrate their technical expertise as well as their internalization of the organizational values. So, it's leadership by example. That's the expectation of every member of our team, that they will come in the door and either they're in a position to be a referential leader or they are willing to develop into a referential leader. And that allows us to take a team that is not necessarily very hierarchal in nature, that comes from multiple contracting sources and is composed of both contractors and federal employees, and get that team all working in the same direction to accomplish the goal.

So in terms of my background, I think you hit the nail on the head as far as coming from a very structured background ... I actually started my career as an infantry officer in the army. In fact, I'm a graduate of West Point with a degree in Arabic, which is -

Michelle Dennedy: Wow.

Ryan Moore: A little unusual for information security. I chose foreign language for my undergraduate degree, because I felt communicating with someone in their own language was the most effective way to connect with them. And I think that's actually served me fairly well, translating some of the arcane or obtuse technical requirements that we get involved with in terms of security to some of our stakeholders who may not have that same technical background.

Continuing on from the army, I really firmly believe in West Point's ethos of its graduates, providing a lifetime of service to the nation. So, I was fortunate enough to join the Secret Service and here I am today.

Michelle Dennedy: That's pretty amazing. There's a lot to unpack there. Again, I think popular entertainment paints a very one-sided view often of career military. It really is a life of service and a life of sacrifice in many ways. But I like what you were talking about studying Arabic and really communicating to people and the way you've pivoted into that. And I totally embrace this ethos and I think it does speak volumes to both the traditional type of leader as well as a referential leader. Being a leader to me is as much about listening to the needs of your team members to be successful and really empathizing with what it's going to take to get them there, as much as it is coming up with some super-duper plan and then directing them to go and execute on your behalf.

Ryan Moore: Absolutely. Never letting pride stand in the way of a good decision is one of the mantras that I started out with as a junior officer in the Army. It's carried me over today where all initiatives tend to work better when the stakeholders have ownership of initiative and what starts as a compliance issue just becomes the way that business is done because we intrinsically know that's the right way to do it.

Michelle Dennedy: Yeah, and I think compliance can often be a dirty word for people. They're like, "Oh, it's in the way of getting things done". It's like, sometimes it really is the ethic of why and how and the job well done. And I think that leads into privacy and security and the relationship. Because what you were talking about before, in hitting these metrics categories on the security side of vulnerabilities or remediations, those are pretty standard security type things. But there's also all of this data itself, the corpus of the data. It sounds like from your description, there's no real opting out if you want to use a system that processes data. You have to by default assess the privacy of that system. How does that work in your operation?

Ryan Moore: Well, so it's funny you mention compliance. I agree, it's not necessarily a bad word. It's rather a starting point where the culture of risk management begins.

Michelle Dennedy: Yeah.

Ryan Moore: For my organization, how that works is, as an advantage the government is required to comply with any number of federal statutes and regulations and policies. In parcel with that is that we have a risk management framework that's mandated that we use and that includes the privacy controls. So, when we look at a system that we would like to grant it the authority to operate, part of its assessment is, we apply that risk management framework to it and then just by default, all the privacy controls are then included.

It starts with executive sponsorship, so all the way at the top from our Director, CIO on down, about the importance of achieving these privacy controls. And it translates both into the

technology and the way we do business here. I think a great example is our software development team that we have internal to the organization, where all the privacy security controls are actually captured as user stories, because we're an Agile development shop. And then those user stories are built into sprints and then our teams are actually addressing those privacy controls as they build the application. So, when the application is done and ready to go live, those privacy issues have been already addressed and baked into the process. So, it's not a one-off, it's not something we bolt on afterwards. It's part of the process from the very beginning, right on through to the end.

Michelle Dennedy: So this is straight-up privacy engineering practice. That we recommend. I think it's fantastic and I think Agile is not a new thing anymore, but even if you're still in more formalized waterfall types of development scenarios, having a user story ... it has a beginning, a middle and the end. It's time-bound. And then adding those into those recurrent sprints in the Agile or if you want to put that as a gate in your waterfall system, that's cool. I'm down with that. But what you're talking about is so much more then telling someone they need to comply from leadership and training. It sounds like you're talking about going all the way the down into the architecture of hardware and software here to get privacy controls and safeguards.

Ryan Moore: Absolutely. We look at it that both privacy and security should be organic to the hardware and the software that we field. So, it's not something that's an afterthought. It should just be part of the expectation of our stakeholders that, when we authorize the system to operate, that those controls are addressed within the system.

Michelle Dennedy: You bring up a good word, and I think it will lead me to my next question which is, who do you think your stakeholders are?

Ryan Moore: Well, we have a variety of stakeholders. We have our internal customers, who are the ones who… whatever is being developed has to be aligned with their strategic business objectives. We also have some of our most important stakeholders, who are the actually owners of the privacy information themselves. So, the government is entrusted with a variety of types of privacy information just to do its day-to-day business. And at the Secret Service, we value the trust that individuals place in us, by allowing us to hold their privacy information. And each and every day, we're working to live up to that trust by designing systems and software that are secure by default when they get deployed. And then continuously monitor them to make sure that the level of security and safeguards for the privacy information does not slip over the lifetime of the system.

Michelle Dennedy: What you're talking about is an incredibly high standard and I completely embrace it. So I'm coming from a private sector background, you're coming from public. What are your business wins, do you think, within the federal standards? And how do you think the private sector stacks up?

Ryan Moore: Well, so the government has a unique advantage and disadvantage insofar as the amount of regulation and statutes that apply to us and that direct which risk management framework we leverage. That's a terrific advantage because that gives you the baseline for building your risk management culture. It's almost the catalyst to get you to go from mere compliance to actively managing the risk with the organization, because the framework is selected and gives you a lot of the direction.

It's also a disadvantage because that, at times, can influence innovation and may slow some business processes, where a different framework may accelerate them. So, the private sector, I think, conversely has exactly the same advantage/disadvantage. It's a challenge to select which is the right risk management framework for your organization—which one aligns most closely to your strategic objectives. It that can be a challenge to discern that, but likewise there's a lot of flexibility where someone can select an existing risk management framework, they could create a hybrid of several, or they could just create their own and still accomplish the same objective. So, in terms of comparing and contrasting the government, I think we share the same issue, just on opposite sides of it.

Michelle Dennedy: Yeah. It's so true, because I spend a whole lot of time doing business cases to demonstrate efficacy and why do we really need this? And it's like, "because you do" if you want to do risk management and you want to have these organic, robust systems. But it's nice to have a mandate sometimes. But I also have a great deal of flexibility that allows me to do stuff that's different.

So, speaking of flexibility, one of the biggest challenges that we face, and I think collectively "We" who are fighting for the integrity of systems, is the insider threat. So, let me ask you the question on a couple different fronts, which is ... One is, how do you—especially with contractors and this heterogeneous team of hierarchal leaders as well as these referential type leaders—how do you detect and spot and notice if someone is about to go rogue on you, if they are? And then how do you build up a resilience to folks who may want to do damage from the inside out?

Ryan Moore: Well, Michelle, I don't know that there's any one specific characteristic or pattern that you could point to that would be the best way to detect an insider. I think insiders manifest themselves in any number of different ways. I do think in terms of framing risk, it's important to keep in mind that it's not just risk associated with technology or risk associated with the process. It's risk associated with the people behind the processes and the technology. So using due diligence for background investigations, taking reasonable steps towards identity management, credential management, are all things that are really part of day-to-day operation maintenance of information technology, but also contribute to insider threat programs.

Michelle Dennedy: Yeah, and I think some of the things that you were saying earlier too about just being someone who speaks to people in their own language, whether it's technically Arabic or if it's technically technical or in leadership, hierarchy-speak. Oftentimes I think, if people are heard and they feel like they're brought along as part of the mission, you sort of lower that risk. It's never a perfect risk, but it feels like you lower your risk at least of the insider really doing a great deal of at least long-term damage.

Ryan Moore: Absolutely.

Michelle Dennedy: So, I want to pivot a tiny bit to do a final question for you and it's not a short question. But if you weren't doing this and just killing it with your metrics—because it's easy to ride on top and go "Hey, I'm pretty darn good at this"—what would you be doing? What is the ideal ... and I won't tell your boss ... when you were a Private Moore, what would you be doing with yourself?

Ryan Moore: Oh wow, Michelle, that's a hard question.

Michelle Dennedy: It's a big question.

Ryan Moore: It is a big question. I'll give you the most sincere answer I can give you. If I wasn't currently serving as a Secret Service agent, I would probably be trying to become one.

Michelle Dennedy: Cool.

Ryan Moore: It is a wonderful agency and I have had the opportunity to serve with some of the very best people in the nation and enjoy some professional experiences that just aren't available elsewhere. And I'm not exactly sure what the future holds for me. I still believe I have more to contribute to the agency and I think I can do more and add more value to the organization. But perhaps someday I'd like to contribute to the next generation of security and privacy professionals by sharing my experience in some way.

Michelle Dennedy: I love that answer. And how many people can honestly look at themselves in this Steve Jobsian way? Look at yourself in the mirror and say, "If I wasn't doing what I was gonna be doing today, how long should I be doing it?" So, if I wasn't doing what I was doing today, I would want to be trying to do what I'm doing today. I think that's a wonderful, amazing answer.

Ryan Moore: Well, thank you.

Michelle Dennedy: That's cool. So, what have we not talked about that we should talk about? That was my final big ta-da question, but I feel like I could talk to you for about ... people, process, technologies ... how about, give me a good hobby? What are you doing for fun?

Ryan Moore: Well, I know this sounds a bit odd, but I really enjoy working with natural language processing. So I'm searching for some ideas and one of the things I came up with is, can you program a chatbot to rhyme—to learn how to rhyme, just by interacting with it? So, I spend a whole lot of time trying to figure that out, until I discovered that [inaudible] has already figured it out and has a lovely chatbot rhyming library. But it was really interesting. Things that are linguistic in nature are something I've always had a big interest in. So, it was an interesting challenge to figure it out.

Michelle Dennedy: I like that, electronics and love of language and an interest in the arts. Who would know we have a special agent who's interested in ... and nerdy enough, may I say with respect in my heart for nerds like myself out there ... to actually have a hobby in natural language. Do you have any favorite rhymes off the top of your tongue, from your bot?

Ryan Moore: Oh gosh. You know …

Michelle Dennedy: If it rhymes with Nantucket, we're gonna have to just beep you out.

Ryan Moore: Yeah, I don't know that ... I can't remember exactly what we tried.

Michelle Dennedy: Okay. Fair enough. I won't put you on the spot for poetry this time. But thank you very much and I'm hoping I'm not going to get the title wrong. So, I know it's Deputy CISO, is it Special Agent Ryan Moore?

Ryan Moore: It's ... sure. It's -

Michelle Dennedy: Sure. No, we want the real one! I want to feel official!

Ryan Moore: Technically I'm an Assistant Special Agent in Charge.

Michelle: Okay. So a special thank-you to the Special Assistant Agent in Charge, Ryan Moore. Thank you very much for coming on the Privacy Sigma Writers and really illuminating a lot of what I think has been a secret and too long held.

Ryan Moore: Well thank you very much for having me. It was very gracious of Cisco to allow me to appear today.

Michelle Dennedy: Well have a great one and thank you for your service. We appreciate it and we will do the best out here in private sector to keep us safe online as well.

Ryan Moore: Wonderful.

Michelle Dennedy: All right. It's a wrap, kids.

Michelle Dennedy: You've been listening to Privacy Sigma Riders, brought to you by the Cisco Security and Trust Organization. Special thanks to Kory Westerhold for our original theme music. Our producers are Susan Borton and David Ball. You can find all our episodes at www.cisco.com/go/riders, or subscribe wherever you listen to podcasts. Then please take a moment to review and rate us on iTunes. To stay ahead of the curve between episodes, consider following us on Facebook, LinkedIn, and Twitter. You can find me, Michelle Dennedy on Twitter, @mdennedy. Until next time.