

Framework in Focus: Santi Kiran Summer 2021 (publish date: June 2021)

Interview Transcript:

Hello. My name is Karen Wetzel. I am manager of the NICE Framework at the National Initiative for Cybersecurity Education at the National Institute of Standards and Technology (NIST). The NICE Cybersecurity Workforce Framework, published as NIST Special Publication 800-181, establishes a taxonomy and common lexicon used to describe cybersecurity work. The NICE Framework is intended to be applied in the private, public, and academic sectors. In this edition of the NICE eNewsletter series, Framework in Focus, it is my pleasure to speak with Santi Kiran, security control assessor at NIST, under the U.S. Department of Commerce. Santi, thank you for letting us learn about your career pathway and understand more about the NICE Framework and what we do from the lens of someone like yourself who is performing cybersecurity work.

Santi: Thank you for having me, Karen.

Karen: So let's begin. My first question for you is pretty straightforward. Could you explain your role and responsibilities as a security control assessor here at NIST?

Santi: Sure. I'm in a unique role. Previously I was supporting NIST as a contractor. Within the last year I've joined in on as a federal employee. I'm kind of supporting two different areas within our team: 1) security control assessments to ensure we're meeting compliance requirements set forth by the government; and 2) working to integrate our security assessment and privacy processes into a governance, risk, and compliance tool. I'm kind of helping with development and new efforts related to the GRC tool but also supporting assessments.

Karen: That's really helpful, thank you. How did you get to become a security control assessor? Could you describe your career path?

Santi: Sure. It's an interesting one. Initially when I was graduating from college, I was envisioning being a lawyer and going to law school. But then I started off my career in consulting, just doing general management consulting, and I started to notice a trend in cybersecurity and how that's increasingly becoming important and relevant in terms of day-to-day business operations. I thought there's many people in the management consulting field, how can I differentiate myself and really stand out and develop my skill set? I thought maybe first doing a masters degree in cybersecurity would help give me some of that foundational knowledge that I didn't necessarily get during my undergraduate program. That kind of helped me pivot into more cybersecurity consulting. From there I received a few security certifications, and that helped me get more into cybersecurity but also understand the vast domains within that field.

Karen: That was forward-looking of you. It is an area where we've really tried to emphasize that, at least for the NICE Framework, it's not just for those whose primary role is in cybersecurity but across the enterprise – exactly what you just described, that people in the business portions of the organization also need to have this knowledge. I'm sure it was extremely helpful for you in developing your career. My next question is more about how you got into this as a career. What were maybe some of the

difficulties you might have experienced in going into cybersecurity as a career? That's a common theme that we hear when talking to people about cybersecurity as a career.

Santi: I would say there were two – I don't want to call them issues – areas I had to really think through in making this career move. First, I come from a very business functional background, and I thought I don't want to sit there and code all day and look at incident response reports. But after doing some research, I realized cybersecurity is a very large field. There are so many different things you can support. I found leveraging the existing skills that I have from that business functional background and serving as that translator with the technical side of an organization is something that, at the time when I was starting off in my career, was lacking, and I thought I could fill that role. I've found that it's been very beneficial for me. In terms of actually pivoting into cybersecurity, I kind of had to take a step back in terms of the roles I was first starting off with. Having been graduated from college for a few years and having a role already established and moving to a different field – I don't want to say it's like starting over, because some of the skills are transferrable, but I did have to take that into consideration.

Karen: Just recently, with our 2020 revision of the NICE Framework, we introduced competencies, and among those are some of those professional skills, like communications skills that you've highlighted. Something we keep hearing over and over again is that it's an important trait to have those kinds of capabilities and those professional skills in cybersecurity careers as well as in non-cybersecurity careers. It looks like you're ahead of the game. Another question I have is around academic degrees in cybersecurity and certifications. How important do you think those traditional certifications are for cybersecurity positions?

Santi: In terms of the degrees, I think it was important for me because I was pivoting into a field in which I didn't have on-the-job skills or any formal education. That was important for me personally. In terms of certifications, the guidance I received from my leadership and supervisors in the past, especially being part of the federal government, is to have certain security certifications. I had gotten a few to help strengthen my knowledge and my skill set in the field. It also helped me to understand the vast domains so I know one certification I was studying for was eight or nine different domains, understanding cybersecurity as a broad field but having an opportunity to specialize in one or two of those areas where I thought I could best use my skills.

Karen: That's really interesting. I love the idea you brought up that you didn't have the actual on-the-job experience. It's interesting to see how all of these can come together and provide different things and the role that certifications have – that's great to know. How do you keep those skills sharp and current?

Santi: The fun part with having certifications is maintaining those with learning credits. Basically, attending conferences, webinars, and things like that to keep yourself well-informed of what's happening – not just security trends but also new ways of approaching common security problems and challenges.

Karen: Thank you for that. My next question is on a slightly different tack. Talking about how diversity, equity, and inclusion are really obviously important for the success of the cybersecurity workforce, it's well-recognized the importance of those traits for all workforces. Cybersecurity is no exception. How are you seeing diversity, equity, and inclusion play a role in cybersecurity, and what kind of role do you think they are going to play in helping us to develop our future workforce?

Santi: I think cybersecurity, again, is a very broad term and encompasses many different aspects, even things that touch our everyday lives. Any field you see having a more diverse background, different insights, different perspectives is really key to help ensuring that field and fostering growth. Personally I have attended a couple NICE webinars as well, and it is interesting to hear how there aren't many women in these cybersecurity fields or the STEM workforce. I'm interested to see how we can leverage the NICE Framework to encourage more women to join the workforce in that field.

Karen: You mentioned the variety of different kinds of roles there are in cybersecurity. I do think that is one of the things we've been trying to focus on – how to communicate to people who might be interested in this as a career that it isn't a one-size-fits all. There is a variety of different kinds of roles out there that anyone can fill. For anyone who is interested in this career, there is likely a role that would be a nice match for that person. That is one thing that with the NICE Framework work roles that we try to bring forward and certainly with some of our groups around transforming learning process, around developing our workforce and some of our working groups and efforts in that space. That is one of the areas we're looking to focus on. Going back to you and your specific job, what is it you enjoy most about the work you do?

Santi: I actually really like how the things I do and the larger scale of things is very relevant to everyday life. You hear about things like the SolarWinds hack or the ransomware attack of the Colonial Pipeline – how relevant what we're doing is. I see that becoming even more relevant and pertinent to how we live as a society. It's always fascinating to me how the little things I do, at the end of the day, kind of bubble into this larger topic that's very relevant to how we live our daily lives, especially with things being more interconnected – how important it is to make sure that folks know [not to] click on suspicious email links and how it can result in so many different things. The relevance of it is what makes it interesting for me.

Karen: I had a conversation not long ago with someone who was pointing that very thing out – how especially with so many devices that exist out there, even appliances and all of that, that cybersecurity knowledge and awareness should be something that is taught from very early stages and be part of everybody's common knowledge, regardless of whether you work in this field or not. It's nice to be able to create those paths and to start to help with [GARBLED] as well as to protect our systems and services. I get that. One last question. If you could give advice to a young person considering a career in cybersecurity, what would you tell them?

Santi: I would say it's important to understand that – again, I keep going back to how cybersecurity is such a broad field – there is a place for everyone. Personally, I don't consider myself to be very technical, but I feel like there are things I can still do in this field and still understand it. I know there are certain stereotypes about cybersecurity technical work. There's more to that than just some of the things that might come to your mind initially when you hear cybersecurity. Be open and do a little research in terms of what you can actually do and what your interests are. I think that, at the end of the day, everything is interconnected.

Karen: That's a great note to end on. I saw a Twitter post - somebody had recently gotten a job of their dreams in cybersecurity and posted an announcement about that. I guess somebody had followed up and said, what is the thing you were doing? He too had suggested connecting with other people in this field. When it comes to that, there are so many different kinds of things out there and being able to reach out to people who might be in those different job roles or to learn more about them. I think this is a really welcoming community, and we're always willing to share our knowledge with people coming

up. I'd certainly encourage folks who are listening to this interview to think about that. If you're interested in a job, as Santi shared, reach out to someone and we'd be happy to chat. Santi, I really appreciate you taking the time to speak with me today. What an interesting career path you've had. I'm looking forward to actually meeting you in person one day around the NIST corridors. I really appreciate your time.

Santi: Thank you, Karen.