# NICE Framework in Focus – Lonnie Harris

Rodney Petersen, director of the National Initiative for Cybersecurity Education: The NICE Cybersecurity Workforce Framework, published as NIST Special Publication 800-181, establishes a taxonomy and common lexicon that is used to describe cybersecurity work. The NICE Framework is intended to be applied in the public, private, and academic sectors.

In this edition of the NICE eNewsletter, we are profiling Lonnie Harris, Director for Security Enterprise Engineering with Equifax. Lonnie, thank you for letting us learn more about your career pathway and how to better understand or apply the NICE Framework from the lens of someone, like yourself, who is performing cybersecurity work.

**Lonnie Harris**: Thank you. I’m glad to be part of the conversation.

**Mr. Petersen**: Lonnie, explain your role and responsibilities as Director of Security Enterprise Engineering at Equifax.

**Mr. Harris**: My role is basically to protect and defend Equifax core networks. We work very closely with the business units as well as IT to understand the business drivers for Equifax core business and understand exactly what are those implementation requirements, from an IT perspective, that need to be implemented to meet the business objectives.

From a security perspective, my team is then responsible for ensuring that security controls are in place. My team consists of architects, security engineers, and security operations engineers. The security architects’ main role is – we leverage NIST very heavily – to look to NIST SP 800-53 requirements and overlay those across different policies, whether they be protection polices, asset policies, vulnerability policies. Our architects work with mapping those controls into a solution that needs to be designed to provide security stack, if you will.

My security engineers are responsible for implementing – they are the ones who are actually building, whether it be racking and stacking physical equipment, security capability, or security-related equipment or deployment into a cloud environment. Then we have our operations team, whose sole responsibility is availability. They ensure that our systems stay up and operational for our downstream customers, who are the security operations teams that consist of your threat hunters, your incident management, your forensics team.

You have to look at our team as working across the spectrum, from design to implementation to security controls all the way to maintaining and keeping it operational. That’s pretty much what my team is responsible for.

**Mr. Petersen**: Describe your career path to becoming a Director of Security Enterprise Engineering.

**Mr. Harris**: I first started probably about 20-something years ago. I came up as an electrical engineer with a bachelor’s degree and a master’s degree in electrical engineering. I started my first position as a quality assurance test engineer at Cisco, where I was working with testing software that Cisco was releasing for different types of defects and bugs. During that time, I started testing some VPN technologies, so I took the initiative to say I wanted to become a specialist in VPN. That required me to really understand the cryptology piece of it, of course the protocol itself, the difference between IPSec or your SSL tunneling. It opened up doorways because, at the time, cryptology was on the upside of things. We were still using some of the basic crypto.

Shortly thereafter, the opportunity opened up after 911 because there were so many disparate systems that could not communicate with each other. When I say disparate systems, it’s things like the police couldn’t talk to the fire department, and the fire department couldn’t talk to the ambulances, and so forth. What that required was specialized communication and you needed a virtual private network to protect that data. Having a VPN, IPSec, and cryptology background afforded me the opportunity to work in Cisco’s global government security organization to protect some of the critical infrastructure and some of our classified data.

From there I stayed in security, and then I started working on teams [focused] on the whole security development lifecycle process (SDLC). I stood up a couple teams that focused on putting together different types of security controls based upon NIST. We would build our SDLC process based upon SP 800-53 Framework or even some of the ISO frameworks – basically just putting together a security framework that was repeatable and allowed us to have a more efficient process to ensure we could put secure code out there.

That afforded me an opportunity to lead a team as a manager at Cisco that focused on VPNs, IPSec, and SDLC. From there, I moved on up and became a security trainer, if you will, for some of our global accounts that we were trying to enter into from emerging markets. What that entailed was having to work with different international customers, where we would go in and assess the posture of their network and look for security vulnerabilities. From there, we noticed that there was a lack of workforce in terms of being able to support some of these new operations or processes that need to be implemented to ensure you sustain your security posture. That afforded me the opportunity to work on developing processes and also on education and training of the security skills that are needed. We also looked at what are some of the policies that need to be in place, because if we don’t have good governance in place we can’t ensure we have the right equipment that has gone through proper testing, as well as IoT, AI, and all this integrated technology with disparate systems that have different types of security.

So the pathway was almost natural from software security testing to understanding some of our top security protocols, then working on developing lifecycle processes for the organization, and then having the opportunity to engage with some of our top customers and educating them in terms of security posture, which is really based upon your policies, your processes, and your people.

From there, it was another natural matriculation. I was approached by one of the VPs at Equifax after the breach. They needed someone who had a pretty strong cyber technical background as well as someone who understands processes and some of the regulatory requirements, so it was almost a natural fit. Again, it took 22-plus years to get there, but it started simply by just saying, hey, you’ve got to master something. That was the piece that really stuck with me, to be able to master something at the time.

**Mr. Petersen**: That is a fascinating path that you took. How would you envision using the NICE Cybersecurity Workforce Framework to either guide your own career or maybe guide your role as a hiring manager or supervisor in your organization?

**Mr. Harris**: I’ve used it in a couple ways. I definitely take from it when I look at certifications that the Framework references. I also look at the knowledge and skills, of course, because a resume only tells half a story. For me, I like to understand your knowledge, and I can see that in your resume. From there, I want to understand what are some of the skills that you’ve learned along the way? In today’s market, the degrees are definitely a need – I would never not get a four-year degree or a two-year degree. But we also need to have people who have certain skills, and that means [asking] what are some of the tools you know? What are some the languages you know? I need people who really know how to use SIEM. If you know Splunk, I need to understand how well you know Splunk. If you know how to use firewalls, have you ever configured a firewall? Do you understand how firewalls work? I really want to see some of the skills and hands-on [experience] so I can really assess your knowledge level.

So I look at the Framework from the standpoint of understanding the certifications that are recommended and some of the KSAs that are a part of the Framework that are called out. Then I’m able to put together a very formal interview process or hands-on demonstration that I require of most of my interviewees or even my team. That not only helps me keep my team’s skill set relevant, but it also gives me a matrix that I can use when I’m doing my interviewing or if I’m looking to build a new team, if you will. So that’s how I leverage the Framework.

**Mr. Petersen**: Can you talk about what type of cybersecurity jobs are the most difficult for you to fill in your organization?

**Mr. Harris**: Oh, wow. [Chuckles.] Right now, the security analysts and . . . we have a lot of specialized skills needs. Oddly enough, with security on the operational side, it really is around the tool sets. So understanding some of the tools that apply, I probably have some 53 different security capabilities. When I say security capabilities, it would be a firewall, IPS, a WaSP, or any of the security tools I have in the stack. People who understand these tools not just at a surface level but how they integrate or interact with the other security tools within the network.

The analysts as well as security architects and engineers kind of go hand-in-hand, so I need people who understand, from an architectural standpoint, what does the enterprise look like? What does your on-premise network look like? Do you understand how traffic moves from on-premise to the cloud or from on-premise to the cloud and back to our data center? And then what are the security tools that are in place to protect that traffic as it leave the enterprise, goes to the cloud, and comes back? Of course, we still have people who have to work VPN into the network. So the engineer, architect, and, I would say, analyst are probably some of the top three toughest areas to fill right now.

**Mr. Petersen**: Earlier you talked about your value for higher education, but how do you decide if an academic degree or certification is required for a job announcement or position, or maybe somebody doesn’t need it and they can either acquire it or develop those credentials along the way? How do you decide?

**Mr. Harris**: You know, the approach I take I know is a non-traditional approach. Probably 50 percent of my workforce – maybe about 40 percent – are contractors. I look at folks who have targeted security skill sets, with or without a college degree. I’m really looking at, what have you done? The resume is nice to have and see or the degree, but I really want to see how much time you have spent as an analyst, and what did you do in that role? I’m able to talk through those scenarios with them and kind of pull out what they really understand from a day-to-day perspective. So I don’t weight heavily on degrees. I weight heavily on degrees when looking for a long-term engineer, for example, full-time. But today we do have a lot of contractors in the workforce who are looking to do short-term projects and may just want the flexibility to work wherever they want to work from. I kind of balance that between: Do I have an immediate need for contractors or do I have a long-term vision I need to fill? That could be somebody with a degree program. That’s the method I’ve had to use to keep these positions filled.

**Mr. Petersen**: I appreciate that. How do you keep your skills and those of your team sharp and current?

**Mr. Harris**: Thankfully, we coordinate very tightly with the security operation – the cyber ops team, we call it. That team consists of everything from investigators to forensic analysts to incident response analysts to vulnerability management. To hear some of the day-to-day threats and vulnerabilities that Equifax has to contend with, I’m learning from the cyber ops team.

I know that with business transformation nowadays, everyone wants to go through the cloud – whether it be for reducing the costs or just being able to move some of the data off network to reduce costs from a transactional standpoint. I’m able to leverage the business needs as well as understand what our cyber operation team is seeing or not seeing in their domain. That helps me then turn to my team and say, hey, I need people with technical understanding for, say, remote access. Or I need people who really understand how to protect cloud environments. That allows me to go out and look for targeted training. If I need people who understand cloud, I look for Google training. We do a lot with Google training. Or if it’s network-related, I look for programs such as Cisco’s training programs on their tools and technologies. I typically work with my cyber team to hear exactly what their gaps are, and then I’m able to translate that information back to my engineers to make sure they have the skill set in order to meet those objectives.

**Mr. Petersen**: What of the opportunities for growing the cybersecurity workforce is to develop more and hire more from under-represented populations, particularly women and people of color, or it could be veterans or people with disabilities. How are you in your organization attempting to make your workforce more diverse and inclusive?

**Mr. Harris**: That’s a great question. I think we’ve been afforded an opportunity. I’ve been working with universities. At Cisco, as well as at Equifax, what we’ve noticed is that cyber is different in terms of the skills that are needed or the intellect or the mentality. It’s really about trying to find that needle in the haystack. You’re trying to stay one or two steps ahead of the adversary, and you really don’t get that in a book. It really takes a person who looks at data, who understands what the vulnerabilities are, the threats, understands what the gaps are in the technology or protocol. From there, I’m able to communicate to under-represented communities, whether it be minorities or females: Don’t make it seem as hard as it sounds. I don’t come in and try to make it all about engineering this or security this. No, it really is, do you like solving crossword puzzles? Well, here’s the puzzle of the day. We’re trying to figure out who’s trying to hack in. I give them real-life scenarios and kind of bring it down to a level that is complex but only complex until you figure out a methodology or format to follow in terms of how you go about putting together plays and playbooks, as we call them, to be able to isolate, mitigate, and then operate in an environment that’s highly vulnerable to attacks.

I’m able to now work with the universities and the different colleges and under-represented colleges. We’re going into the engineering schools or even the computer science schools – and even some of the tangential schools, whether it be business or agriculture – and form partnerships and say, hey, I can put internships and programs in place where we can provide training in cyber, and we really want to target some of the under-represented demographics. What I really like about it is that we find a lot of people in the veteran space and lot of females who, once you kind of explain what cyber is and don’t make it sound so complex and intimidating, you’re now able to recruit more.

At both of my companies, and especially now at Equifax, we work very closely with a lot of universities in terms of putting together internships and apprenticeships as well as sending back some of our engineers into the classroom to actually teach. What we’ve found also is that augmenting that staff in the classroom is necessary because [students] need to hear those real-world experiences. Cisco, as well as Equifax, allowed me the opportunity to either send my engineers back or myself – I’ve gone back and taught for two semesters. We work with the different schools now that recognize that they need that field experience and they need to be able to correlate what they’re teaching in engineering or computer science or IT into real life and then tie it all to cyber. Again, the engineering and computer science is only one facet. We’ve still got the process piece and we’ve still got policy pieces of it. Universities are now more welcoming to certificate programs. They’re more welcoming to augmenting their traditional coursework in order to provide the students or candidates with a non-traditional pathway into the workforce that they would not have had before.

**Mr. Petersen**: Lonnie, thanks so much for speaking with us today and offering your insights. That was all terrific. I just want to offer best wishes as you continue to help your organization and the rest of the nation reduce the cybersecurity risk for individuals, organizations, and economic sectors like your own. Thanks again.

**Mr. Harris**: Thank you very much . I’m very happy to be a part of NICE.