**NICE Framework in Focus – Chris Knox**

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 Chris Knox, Security Awareness Program Manager for CPS Energy. Chris, thanks 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. Thanks, Chris.

**Chris Knox**: Thanks for having me.

**Mr. Petersen**: Chris, explain your role and responsibilities as Manager of the Security Awareness Program at CPS Energy.

**Chris Knox**: CPS Energy is the municipally owned electric and gas company for San Antonio, Texas. My role in particular is responsible for developing and delivering security awareness education and training for our workforce. We also provide threat intelligence support, which includes vulnerability awareness, vulnerability assessments, and executive travel assessments.

**Mr. Petersen**: What is the size of your Security Awareness Program team, and what type of roles do they typically fill?

**Chris Knox**: There are two direct reports under me. One member is primarily focused on conducting the threat intelligence aspect of our work, and with that we utilize the partnerships that we have with outside entities like the Department of Homeland Security, the FBI, and the various information sharing agencies. I have another team member who pretty much oversees all of the specific training development and training delivery programs that we offer, which include our monthly phishing campaigns.

**Mr. Petersen**: Who is the typical audience for the outreach and awareness training you provide? Is it just your employees or is it people external to the organization as well?

**Chris Knox**: It’s just the internal employees.

**Mr. Petersen**: Very good. Describe your career path to becoming a manager for security awareness.

**Chris Knox**: It was an interesting transition. I actually spent 15 years as a military communications intelligence analyst, and I was a supervisor before leaving the military. In the latter part of my career, I became a leadership training instructor. All of that that training provided the foundation for the current role. I learned about vulnerability assessments, hostile threat tactics, techniques, procedures, etc. After leaving the military, I continued to work in training and development, and I was offered an opportunity about 3 years ago to stand up a Security Awareness Program here at CPS Energy. The director of security, and cybersecurity in particular, said hey, you know what, we could really use someone with your background and expertise. You understand the military; you understand security; you understand training – and we really need a robust security awareness and training program. The position was created, the department was stood up, and a few months later I was able to hire another individual. Interestingly enough, we had another individual working in a totally different area of the company who we wanted to offer a job rotation assignment. This individual transferred over and did an excellent job, and we have since hired him into the role. But my role, in particular, was all built around my experience with training, development, and communications security.

**Mr. Petersen**: That all sounds very exciting and a great opportunity to stand up your own organization. How could you envision using the NICE Cybersecurity Workforce Framework, maybe in establishing that program but also, more specifically, to guide your career and the other staff careers that you supervise in your organization?

**Chris Knox**: Great question. Since our department stood up (our department is now called Threat Intelligence and Security Awareness), my director and my team have used the NICE Framework to try to align and map our current workforce structure so that we can look across the organization and see where there might be some potential manning gaps. How can we use the NICE Framework to maybe even support some of our future hiring decisions based on these gaps? Also, how do we define more specific role-based training opportunities? Because of what we’re doing in the training and development space, we are also trying to create role-based training, and the NICE Framework provides a great foundation for how we develop training opportunities.

**Mr. Petersen**: That’s a great observation about role-based training. Another NIST Special Publication, 800-16, we revised last year but are trying to more closely align to the NICE Framework work roles, tasks, and KSAs. I know that your team is fairly limited in size, but both with your team and maybe across the cybersecurity organization, do you have a sense of what type of cybersecurity jobs are the most difficult for you or other managers to fill?

**Chris Knox**: When I thought about that question, I had a conversation with my boss and we were in agreement: Cybersecurity as a concept is something that affects all of the aspects of pretty much any organization, and it’s no different in our organization. As such, the challenges that we run into in trying to fill jobs related to cybersecurity all center around having a pool of candidates who, first of all, have adequate functional knowledge, technical knowledge, technical competencies to support their respective business areas and, more importantly, have a sufficient understanding of how cybersecurity impacts those functional and technical aspects of the job.

Additionally, we want to be sure we have candidates who have the right depth and breadth of technical competency and business acumen that will often times put them in places to command a higher-than-market-based compensation. If we have candidates who really have a strong depth and breadth of technical and functional knowledge and really understand cybersecurity, they’re simply going to command salaries higher than what our current market will bear.

Those are some of the challenges that really make it difficult for us to find the right candidates. More times than not, they’re short maybe in one area or another. We don’t have a cybersecurity job per se; it’s just how well do they understand cybersecurity in the bigger picture of what we do as an organization or what they’re supporting in their particular area of the organization.

**Mr. Petersen**: That’s a great point as you describe the capabilities or qualifications you’re looking for. Traditionally or historically, academic degrees and certifications have been a big part of position descriptions or job requirements. I’m curious, in your organization, are degrees or certifications required, and how do you assess or determine whether or not they’re necessary to be an applicant for a position?

**Chris Knox**: Academic degrees or certification [requirements] will really depend on the level of the position that we are recruiting for. We may have an entry-level position or, a lot of times, it may be an analyst-level position but it’s a level-1 analyst versus, say, a more senior analyst or level-4 analyst. Depending on the level of the particular position, we may place more weight on the actual technical experience the individual has versus their formal education or professional certification. Where professional certifications and academic degree come into play is as they start to move into higher-level positions. A level-4 analyst will be expected to have more technical knowledge and broader experience and competencies – being able to integrate all of those things into the work that’s being done as well as having an appropriate level of soft skills or people skills. With that, we don’t put quite as much emphasis initially on academic degrees or certifications, but we will definitely place more of an emphasis as they move into the higher-level positions and particularly if they move into the management-level positions.

**Mr. Petersen**: Those are great points in terms of proficiency and how that changes from entry level to advanced and also the capabilities or qualifications. We know cybersecurity is a field that’s constantly moving and changing and even if you come in at an entry- or mid-level with experience or credentials, you need to continuously learn. I’m curious how you keep your skills and those of your team members sharp and current.

**Chris Knox**: Our company has a very robust professional development program, and we use a number of different channels. One in particular allowed me to step into my role and also allowed me to bring another individual into the fold here, if you will. We also have professional development as a key component of our individual annual performance reviews. Every employee has some aspect of professional development, and management across the board is very supportive of anything that an individual does in the area of professional development.

In our particular areas of security, integrative security, IT, IT skills, and any of the more technically oriented professions, you will find that we encourage employees to look to industry-specific certifications. For my team, it would be IT-related or security-related, and we will support anything an individual does, be it web-based seminars, conferences, or formal courses. More specifically, I have two individuals attending SANS courses here in the coming months. We are supporting them by putting funds behind courses like SANS to allow these individuals to grow.

**Mr. Petersen**: Cybersecurity is also a field that has complex challenges, where either you work in teams or you need different approaches to solving problems. Among the challenges in the cybersecurity workforce are 1) the under-representation of minorities, women, people with disabilities, veterans like yourself, and others potentially who are generally under-represented in the field, and 2) this notion of diversity of thought or experience. I’m curious how you or your company may approach this or may be attempting to make your workforce more diverse or more inclusive of these different backgrounds or experiences.

**Chris Knox**: Within our company, workforce diversity is primarily managed and monitored by our HR department – we call it our “people and culture department.” We also have across the organization several of what we call employee resource groups. We have a NextGen Group, which is what I like to call our young adults group – our 20-somethings and upwards into the mid-30s or just under 40. We have groups like our Veterans Connection with all prior veterans. We have a lot of employees who are members of professional organizations – IT-related organizations, minority-based organization, women-only organizations, or women-specific organizations.

All of our employees who are part of these groups – and some of them actually are part of both a resource group and a professional organization – go into the community and speak to like-minded individuals who want to learn more about what we do with the company. More importantly, what we do in the space of security and professional development, how we support like-minded individuals if they were to come, and how they learn from these individuals who have moved up in their career. We go into the community quite a bit, we discuss opportunities, and we look at pipelines as a means to attract new talent.

**Mr. Petersen**: I love the reference to people and culture because obviously people, as you know, doing security awareness training are such a big part of the solution, both in terms of awareness and also the human resource aspect. Culture speaks to both the ability to recruit the diverse talent that we were just talking about as well as potentially retain them. Given that issue of culture, I wonder if you could talk a little bit about what you enjoy most about your work at CPS Energy, particularly as the Security Awareness Program Manager.

**Chris Knox**: Thank you. I have spent the latter part of my career as a training manager, and I like to think of myself as lifelong learner. From the time I first entered the training space or started working as a training instructor and then a training manager, I really enjoyed helping others learn and grow in their professional development. Given this opportunity now to not only take the training aspect but also the security aspect of it, I really like helping our workforce understand and value the importance that security plays in our company and in our day-to-day lives. I like the idea of helping folks understand the tools that are available, the tips that they should be aware of, and the techniques that the bad guys are using to try to deceive them. Hopefully through the work that I’m doing and my team is doing, we can change our workforce culture when it comes to security and raise their awareness of security and how it impacts their day-to-day work.

**Mr. Petersen**: That sounds interesting – in addition to the inclusive and supportive workplace culture, it’s the notion of a culture of security that people like yourself are very much trying to shape and maintain in your organization. You also talked about the pipeline work that you do, and I suspect a lot of that is with younger people. You also referenced, by the way, the different ages within your workplace and how you’ve organized accordingly. Can you talk a little bit about what type of advice you’d give to a young person considering a career in cybersecurity?

**Chris Knox**: Well, I’ve learned that a lot of young people have a pre-conceived notion or maybe even an unrealistic stereotype based on the media of what cybersecurity is all about. I try to show them that it’s not the [ ----- ] that you might think, but it really is about understanding how cybersecurity impacts everything they do and the things that they work with, whether it’s their phones, their tablets, or their games. Security in general, but even cybersecurity, plays an important part in everything we do. If we’re connected, if we’re online, cybersecurity is playing a part in that. I want to try to illustrate that through as many different vehicles and mediums as possible.

More importantly, I want young people to understand that cybersecurity is really about controlling access and protecting access to the things that we find are vulnerable – our information and our identity. That’s valuable and that’s vulnerable. Cybersecurity is all about the efforts we take to protect that, to make sure it’s not exploited or taken advantage of. How do we solve that problem? How do we make sure that the people who are supposed to have access to it have access to it and the people who don’t need access don’t get access. If young people can see that, then they’re much more security-conscious. They’re less likely to just post anything and everything that they’re doing. They can share it with their friends. They can share it with their families.

It is really about solving problems because as we continue to add more technology into our lives, we all need to be more security-conscious and particularly cybersecurity-conscious. How do we solve that problem of making sure we’re not exposing ourselves unintentionally to the bad guys and making it easier for them to hack into our lives and steal our identity and all the other things that we know can be the bad side of – or the bad result of – what happens in this space and this world of cybersecurity.

**Mr. Petersen**: Chris, there is probably no time like the present to raise awareness as students at K-12 schools and colleges and universities are learning online and employees are teleworking. Many people are collaborating and connecting across the miles. I suspect that may even be true of your community, if not your workforce. Any quick and final thoughts about lessons learned about security awareness at a distance or in the new world of online learning and teleworking.

**Chris Knox**: That’s a great question. We have a workforce now that’s working remotely like so many other organizations. Once we saw this situation unfolding, my team was one of the first ones to quickly communicate to the workforce: Be careful, there are going to be a lot of malicious emails, a lot of phishing attempts, a lot of people who want to take advantage of this situation. It’s interesting that we’ve seen it grow exponentially since it started. We’re putting out messages daily to our workforce to be careful – here are the things that we’re seeing, whether it’s information about COVID-19, stimulus checks, or testing, anything and everything related to this situation is creating an opportunity for the bad guys. It is also creating an imperative to remind our workforce that you have to be careful about what you share. You have to be careful about what types of information you’re pursuing. You have to validate anything and everything related to what’s going on. Security becomes top of mind in terms of how we go about conducting our business.

In our organization, we place a lot of emphasis on safety. One of the things my team has been very committed to is [making] security just as important as – if not more important than – safety. Security is an aspect of safety, but it needs to be top of mind with everyone just like safety: I need security to do the work that I do. How do we continue to keep that first and foremost, especially now when we have people working remotely? They’re working under conditions that they’re not typically used to working under. They don’t have the access to their typical information, their networks, their collaboration opportunities. They have to be creative, but they have to be that much more security-conscious about what they’re doing and how they’re doing it.

**Mr. Petersen**: Great points, Chris, and timely advice both for your employees and probably the rest of the nation. I want to thank you for speaking with us today, and best wishes in your role at CPS Energy as you continue to help your organization, and quite frankly the rest of the nation, to reduce the cybersecurity risk for individuals, organizations, and economic sectors like your own. Chris, thanks so much for speaking with us today.

**Chris Knox**: Thank you, sir. I appreciate the opportunity.