**Mr. Petersen:** Welcome to the first of the first edition of the NICE Framework Focus Series where each quarter we will focus on a practitioner from the field to help us focus our attention on the NICE Cybersecurity Workforce Framework. Of course, our primary focus will be on the real people who do cybersecurity work and make it such an exciting and rewarding profession. Today, I'm pleased to welcome and introduce Tina Thorstenson, who is the Chief Information Security Officer for Arizona State University. Welcome Tina, and thank you for being the subject of our inaugural interview.

**Ms. Thorstenson:** Thank you for having me, Rodney.

**Mr. Petersen:** Tina, Explain your role and responsibilities as the Chief Information Security Officer.

**Ms. Thorstenson:** My role as Chief Information Security Officer is one that involves overall governance, policy and compliance. We're a relatively small unit within the larger Arizona State University system, and we are responsible for helping the university architect new solutions that meet our security requirements, making sure we have awareness campaigns that are helpful to our university, faculty, staff and students and continuing this evolutionary process of making sure that we are achieving our goal of meeting the university's appetite for risk. Meaning that we want to implement solutions and enhance our solutions and services in place today to meet ASU's security requirements.

**Mr. Petersen:** What is the size of your information security team and what types of roles do they fill?

**Ms. Thorstenson:** Well, we have nearly 25 staff members that are 100 percent focused on information security. Meaning they are part of the Arizona State University Information Security Office. The roles of those individuals include some focus on identity and access for the university, meaning the governance process around how we move people in and out of the roles that they need to do their job or students in school.

We have, additionally, teams that work on the governance and awareness programs. I've got a team that focuses one hundred percent on compliance and audit functions. Meaning, being a liaison for the university for all kinds of compliance initiatives, rolling out whatever the new requirements are. This year we are focused heavily on GDPR, for example. And then, last we have a team that is focused on the Security Operations Center, or the SOC.

**Mr. Petersen**: That's great. And Tina, could you describe your career path to becoming a **Chief Information Security Officer**?

**Ms. Thorstenson**: Ah, Rodney, my path maybe was an interesting one, and may be a little atypical. I started out as an industrial engineer for a transportation company, and quickly found that I liked, I liked projects where we were bringing technology solutions to the line of business. I ended up in higher education fairly quickly after moving to Arizona, and started out in a variety of different business analyst roles and I worked my way up taking on more and more leadership challenges to the point where I had worked in a leadership role in virtually aspect of the information technology organization. And then, it was asked at one point, at a couple points in my career, but one point in particular, if I would be willing, based on my experience serving in all of those areas, as the university began to focus on security as a critical element of all of our services if I would be willing to take on the Chief Information Security Officer role. That was quite a number of years ago.

That's the short of how it happened. Just before I moved into the security focused role, I was responsible for infrastructure and security on the side. That was just before we decided to focus on it, and create an office that we would staff to support not only infrastructure, but our applications development teams, and our endpoint desk-side teams serving faculty and staff, and students at the university.

**Mr. Petersen**: How could you envision using the NICE Cybersecurity Workforce Framework to both guide your own career and in your role as a hiring manager for your organization?

**Ms. Thorstenson**: So, this answer's simple for me, having built a program from the ground up in the last few years. Having a framework like this in place would have been invaluable when I started this office a few years ago. I guess the couple of examples I might give you: the way I might use it today would be to take the Framework and map my current team to perform essentially a gap assessment. Today, prior to this sort of a framework, ASU might have hired an external team to come in and do an assessment for us and try and identify the gaps. Tools like this, in particular this one that is so well thought out and so detailed, would be amazingly valuable in helping us identify gaps in our current program. The space is evolving so quickly, and really expanding as the years go by. That's one particular way I plan to use the Framework.

The second one is, one thing we don't have at ASU right now is a deputy Chief Information Security Officer. And one of the tasks I have on my plate this year is to identify you know, what are the knowledge, skills and abilities that make up an individual in my role, and what a deputy to that individual look like as we look at enhancing the overall program. Rodney, I've just found that leadership is so critical. That's an example of a different form of gap assessment that'd I'd expect to be using this Framework for in very short order.

**Mr. Petersen**: That's terrific. Thanks for those insights. What type of cybersecurity jobs are the most difficult for you to fill in your organization?

**Ms. Thorstenson:** Well, all of them are difficult to fill. But I guess the most challenging job to fill is our more technical roles as security architects. And the reason I believe these are difficult positions to hire is we are looking for someone with a deep technical understanding that can also relate well to the business. We can go to meetings with the Provost Office or the Registrar, or Admissions, or our online programs and have the right level of conversation to discuss risk sometimes, and have very technically oriented conversations that are so critical to reducing our risk, on the other hand. But those are the ones that take me the longest to fill.

**Mr. Petersen**: So, how do you decide if an academic degree or a cybersecurity certification is required for a job announcement in your organization?

**Ms. Thorstenson**: So, it depends on the level of the job we're trying to fill. For the most part, unless we're talking about management interns or student worker positions, we require a Bachelor's degree without question. In some very rare cases, we may take a tremendous amount of experience over that. But, that's pretty much a baseline for us. In terms of additional cybersecurity certifications, we have moved to a model where we like to see certifications, especially in terms of the more technical roles. We have not moved to a point where we require it. We will hire people, and then send them through the training programs to achieve certifications and then following that to help them maintain them.

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

**Ms. Thorstenson**: So, I love this question. There is so much to learn, and it always seems like there's a mountain of things coming at us. We're being a part of a large university and there are more than a hundred thousand students this fall, and there are new ideas and ways to innovate around every corner. The way we keep our skills sharp is, I guess really twofold. One is, we are huge proponents of training campaigns and making sure we give our staff the opportunity to break away from the day-to-day and spend focused attention on receiving the training they need to focus on the rollout of—you pick the thing. Maybe it's Amazon Web Services, or some other new or upcoming technology we're trying to figure out how to help the university figure out how to most effectively secure.

Then on the other side of it is that we make sure we give our staff opportunities to get out and about. It may be local events here in Arizona. It may be regional and national conferences and events. Or, maybe it's getting out to business meetings here on campus so that we can understand the growing needs of our constituents. And also go to the security events, so to understand how we might offer the services we need to deploy.

**Mr. Petersen**: So Tina, how are you attempting to make your workforce more diverse?

**Ms. Thorstenson**: Rodney, I get asked this question frequently. We've done a number of things to make our workforce more diverse. We are strong proponents, and we think it's such an essential element – especially of the growing security program. We have people that come from different backgrounds, different areas of expertise. Many of us did not go to school decades ago, thinking that we were going to be focused on security someday. It just wasn't the way things were at that point. It was all about making systems available, and far less a focus on security.

Now, we bring in, we make sure we bring as many student workers and interns as we can to give the up and coming generation the chance to inform us in some of the decisions we're making while we train them for the workforce to come work for some wonderful company to launch their career. We are focused on meeting every level of diversity, and that's from an ASU perspective across the board. We work hard to model the fact where we want to have a support staff that models our student and customer base in every way we can. We are huge proponents of women in security, for example. I have discussed in recent years and will continue along those lines. We've done a large variety of things there.

**Mr. Petersen**: So, what is it that you enjoy most about the work that you do for Arizona State University and as its chief information security officer?

**Ms. Thorstenson**: What I enjoy most about working at ASU, especially in this role as CISO, is that I learn something new every day. There is never a dull moment in this space. We have worked hard not to be the department of "no", instead to be the department of, "what are you trying to do, and let us help you do it in the most secure way, the lowest risk way possible". So, that's what I love to do, seeing us deploy solutions that we're all comfortable with, that meet the needs of our students.

**Mr. Petersen**: Well, Tina, it sounds like you've had a terrific career. So, if you could give advice to a young person considering a career in cybersecurity, what would you tell them?

**Ms. Thorstenson**: What I would tell them, is that if they have wonderful critical thinking skills and are interested in a vibrant career where it's hard to picture what five years down the road looks like, an individual that likes to be thrown into projects where you're creating new and different things, that individual will be a wonderful fit in the cybersecurity space. I would also tell them that it's a great thing to do from just a job retention standpoint. The number of individuals we need to support cybersecurity initiatives in the years to come is going to continue to grow. So, it's a great choice for a job.

**Mr. Petersen**: Well, that's great advice. Tina Thorstenson is the Chief Information Security Officer for Arizona State University. Tina, thank you so much for sharing your insights with us today.

**Ms. Thorstenson**: Thanks for having me on, Rodney.