**Project Completed by:**

**Selections from the**

**EDUCAUSE Security Professionals Conference 2018**

**August 21, 2018|12:00 - 4:30 PM EASTERN**

**Selections from the**

**EDUCAUSE Security Professionals Conference 2018**

**August 21, 2018|12:00 - 4:30 PM EASTERN**

>> And we're back. Our next session will be it's nice to have a cyber-security system. Welcome Todd. We are so glad you could join us. Please feel free to begin.

>> Thank you very much and thank you everyone for being here today. As it, we're looking at the nice framework today so if you are not familiar with nice framework here's our agenda today. We'll look at what nice is. One, it might be a nice idea for you and how it can benefit you and how it can be operationalzied. First of all. Let's look at what nice is. It's the national initiative for cyber-security information and SP eight hundred dash 180 one. Nice categories and describes security work and the types of work that will be used within cyber-security. Jobs within cyber-security and although it was designed with the federal government and federal government employees in mind, it is certainly useful for academic, military and industry in addition to government. I think we have some use cases that we can look at within higher education as well. Let's look at a quick graphic of the structure of nice if we can. You can see, first of all, this has to be decoded a little bit but I think if you look at it for a moment you can see that nice is designed specifically for a few particular activities within staffing. Identification of the needs of cyber-security professionals within your organization, how to qualify them for specific roles and responsibilities, the types of training, the development of those individuals as they progress in their area of expertise but perhaps also as they develop throughout their career. And human capital planning. The whole idea of course as identified by the framework is to develop a capable and ready workforce. So, there's one way to do this. We can certainly start out with the structure and determine what types of positions you may have within your organization. However, what I've noted is that there are a number of jobs and responsibilities that are used within cyber-security. In fact it's very inconsistent. I did a quick search on the web recently and found seventy-seven hundred nearly cyber-security related job titles but they were all over the map so after doing some due duplication of those I came down to eight hundred and twenty-two variations on those themes and that's still a large number of job titles and responsibilities for us to deal with within higher education. Certainly, the nice framework helps us out a lot. Some would agree, I think, and others would disagree that nice is still too complicated, but it does reduce that number from eight hundred twenty-two to something more manageable. Here are some of those sample positions. On the left-hand side of your display are those that are often the least poplar and the ones on the right are often the ones most poplar. So, as you look at job descriptions you'll find various incantations on that theme of what a job description will look like or we could play bingo. You can pick a column or pick a title out of each column and come up with your own job descriptions, but I don't recommend that. We need to use some type of a standard that we can communicate between industry, between government and between education. If we would all adapt some standard terminology and job responsibilities and descriptions it would be much easier for us to staff, it would be much easier to understand the roles and responsibilities someone has who is already a cyber-security professional and we're considering hiring them. So having those positions consistent within our organizations helps us tremendously in our ability to communicate what someone is doing versus what someone's responsibilities were, as opposed to some made up job description or title. Of course, career path is important to us within cyber-security and the factors that we use to progress someone are often education, experience, expertise, certification and their interest in aptitude. The missed framework takes into account all of these factors as we begin to exam it more closely. There's seven high level functions within the nice framework and thirty-one specialty areas of cyber-security work within which fifty-two different work roles in four dimensions are created and those are knowledge, skills, tasks and abilities. I'm sure most of us have seen some of these already. Had a quick poll for you today and I was just curious from the ones who are attending today, if you were mapping your job titles, would you consider that to be easy or difficult as they are today? I'm going to let that poll run as we continue to look at some of the information on the slides. We've got a few people participating. Thank you. I'm seeing the same responses that I would have expected. Sometimes the job mapping is difficult and it's because the responsibilities are hard to define or haven't been clearly defined in the past. We could look at another view of the job pyramid and I don't know if anyone has seen this before but it's a good example of how to characterize jobs within cyber-security and at entry level we'll begin incorporating specialists and security administrators and those have a progression through the organization toward the Apex to that pyramid toward the roll of chief information security officer or something similar. This is one way to look at the roles and responsibilities and another way to look at it is to look at the functions that each individual group does. Operate, respond and assist and this diagram attempts to structure those in such a way so that you can by looking at it determine where a specific job type might lie within the organization, whether it be operate, respond or assist. The nice approach takes those seven high level functions, provision, oversee government, analyze, operate maintain, protect and defend, collect and operate and investigate and uses those as a way to categorize the functions of cyber security. It's pretty well organized in my opinion. I think this does a better job than some of the other frameworks that may be available in higher education such as cue paw HR. I don't think they do a great deal in respect to cyber-security profession in terms of setting up positions in which we can clearly understand the purpose within the organization. Another way of looking at classifications is to categorize the individual job descriptions into classes such as engineering, business integration and technology operation and you can see where those provision analyze investigate etcetera, different categories can end up wherever you segment them into those three areas. This is also helpful when organizing your cyber-security organization. So knowledge, skills and abilities in tasks are certainly what we're after within the function of determining where our people and our organization are going to lye and where they are going to be most affective for us. The nice framework is set up so that each one of these areas is described and you can use those areas to determine what the job functions are, what types of skills or capabilities an individual should have in order to perform those functions, what the individuals abilities are and what types of work they will be doing within those particular job areas. So here's another way of looking at the same seven categories. We understand the names but this is what the functions are within those names so if we're doing securely provision, conceptualizing and building cyber-security systems is the primary responsibilities with those in the provision area. Just like overseeing govern would have direct and strategize security efforts and each one of those is important as we build out a cyber-security program and staffing it appropriately. I know we don't all have the capability to have a staff that would have fifty-three different roles and I certainly understand that because most of us are operating on shoestring budgets or operating with a small number of people because the scope and size of organizations are just that. However, it does help to use associated roles and responsibilities, so you can combine the functions of a particular individual into certain responsibilities. That's always helpful when we have or when we're short on resources so that's another capability that's available within the nice framework is to combine those but yet keep them into categories so that their expertise can be used across the organization more effectively. Now, within the nice framework you'll hear several specialty areas and I'm certainly not going to read them all but I would suggest that they are areas that can be helpful within higher education for developing areas of expertise and areas of excellence. For example, you may have someone who is very good at training, education and awareness and that's their specialty. Well, they probably are focused within that discipline much more directly than they would at providing legal advice, or language. Nevertheless, your organization may not have all of these things. Language analysis is unlikely, I would say, to be a heavy component within higher education in the cyber-security department. You may, however, have strategic planning. You may have collection operations, threat analysis and vulnerability management. There's no right or wrong way to do this and implement it in your organization. What's important is the framework helps to guide how we can staff our organization to more adequately deliver a maturing cyber-security organization with the idea that those who are within those work roles have specific knowledge skill abilities, talents, tasks to do. Now, because nice is a complex framework, you can read it. You can re-read it and read it again and it will eventually be something that one can begin to operationalize after having read it several times. When it started out it was a conceptual idea and there were very little tools for implementing the nice framework. Over time nice has developed tools that have made it easier to use the nice framework but ultimately, I think, the folks still continue to focus on what types of tools they can provide for the federal government. That leaves a bit of a deficit for us within higher education because we don't necessarily have the need for some of the folks that would be existing within say a DO D or even other government agency within the federal government. So, what I have done is to develop a tool that I'm going to show you in just a moment that combines the framework and it combines other tools together into a single wrapper so that you can go through the tool and find out, first of all, starting with the question, I have a need within my cyber organization. And answering the prompts that you have there, you can drill down into the job descriptions that will be useful for staffing within your own organization. I'm going to try to share my screen now and show you this tool. And let's see if that doesn't show up. So this is the tool. It's in Excel. I think we have it available for everyone and if you'd like to download it, feel free to do so. The tool begins with those seven functional categories, securely provision, operate and maintain, oversee and govern and so if you want to and you are trying to staff within your organization, this is the place you begin. Let's say I want to operate in maintain. You can click on operate in maintain. The roles will be to support, administer and maintain effective cyber-security systems so we're talking about someone in an operation al role.

>> Todd just a quick interjection. Do you mind maximizing your screen?

>> Absolutely. I'll make it a little bit larger here. Is that better?

>> That's much better. Thank you.

>> I'm going to make it a little bit smaller since it fell off the screen there on the right. How's that?

>> Perfect. Thank you.

>> As you drill into the tool, operate and maintain is one area and here are some job functions that are available in the operate and maintain category. Let's say that systems analysis or a system security analyst is something that is of interest to you today in trying to staff for. You can click on the system security analyst and again, I'll enlarge this I chart because it's small. There's a lot of words but these are taken directly out of the nice framework. The beauty of the tool is that all of those things have been consolidated into one handy tool to use as opposed to having to Polk through pages and pages of documentation to get to this. All of the tasks and knowledge, skills and abilities that are indicated here are actually within the mist documentation so you could go to any one of those numbers and find out what that particular number does or you can use this table and they are all there in front of you. When it comes to education an entry level may or may not have any need for an education depending upon your organization, of course. This is just a guide. It's not the law and you can implement this however works within your organization. If you did have an educational requirement it might have a specific discipline. For example, if you are looking for someone to provide legal advice, well, I would presume that you would want somebody who has some type of legal training doing that. At least we would. At this particular level or no particular requirements for an entry level but as one progresses through their career then we would expect them to have a bachelors' degree, perhaps in information systems. We might have a discipline of computer science or information technology and as they get into it in more advanced role in the organization then we start delivering a bit more specifics in terms of what we expect from that particular role. There's also area here for defining the types of training that they would need. We're talking about nonacademic training and the types of certificates that you may have. One thing that's noted within the mist framework is certifications aren't called out specifically but rather the skills associated with those certifications are. For example, a certified security analyst or certificate information systems auditor, if you wanted a particular role then this tool is not going to tell you you need a C /S\*EF. CIS P is not listed, same type of thing but it does give you the types of certifications that one would expect to have in this particular role. There's also an area at the bottom with regard to exponential learning and whether that's beneficial or whether that's not beneficial for a particular role and in some cases, it progresses as someone advances into a more higher level role within your organization. Also, continuous learning, this helps all of us who are budgeting for the overhead associated with keeping employees on the payroll. If training is a part of what you provide your employees, it's important to have or understand that and realize that you may need to invest in that individual each year so that they can continue to improve in their skills. Now, as I mentioned at the top of the page here, the task, knowledge, skills and abilities are listed here. However, I believe we can go right down to the bottom and we'll see those again. That's the master list of all of those within this tool. Those are also copied on to the page where we were before. There's several tabs in this workbook. Each one is associated with a different role. So we'll go back to the home and I think we were in operate and maintain. Here we went to security analyst. So at the bottom are all of those specific knowledge, skills abilities and tasks associated with this particular job function. You don't have to implement it this way but this is the way nice framework recommends that you use it and the nice part -- I hate to use that term but it seems that I have to do that every time I talk about nice. The great part about the tool is that all of these features are included in a single page and you don't have to derive all of these things from various and desperate resources. There are shortcuts at the top so you can go back and navigate through the system using navigation tools. The same is true for any of the other functions within the nice framework. If you have analyze and I wanted to bring this one up in particular because there are job functions here that are grade out. I don't believe these are necessarily going to be applicable to higher education. If you have a very large cyber-security organization, some of these that are in color would actually potentially be part of your cyber-security staff but it's rare to have some of these other ones. Target developer and target analyst you get the implication that this was developed for the Department of Defense which is was. They are there if you want to look at them. The hot links continue to work and you can go to them but they are just not typically recommended as a job function within higher ed. That's the nature of the tool. As I said, it should be available for your download if you want it, and I'll return now if I can back to the regularly scheduled PowerPoint that we had running before. Let's see if we can get it back.

>> Todd, you should be able to maximize the window now. It might be minimized. I'll still have you here broadcasting audio with us.

>> Alright. Let me try this. While I'm working through the technical details I'm at a point where if anyone has any questions, I'm happy to respond. I'll have to hear the question until I can get my screen back in order.

>> Anybody have any questions for Todd? Go ahead and type it into the chat window. There is a question that has just been chatted. Is there a place where salary expectations are listed for the different roles?

>> That's an excellent question and the answer of course is no. The reason is salary levels vary widely across any particular job function within the Universities systems, within private industry and within the government. So, that's going to be one that we'll still have to workout from other sources. I wish we could find something that would work. There's certainly a job that is compensated in Los Angeles is not going to be the same as one that's compensated in a rural area of the country.

>> I think we have one other person typing right now. Is there anything in the tool which highlights progression, steppingstones to the more senior positions?

>> Well, there is some aspects of the tool that tell you what requirements that one should have as they move from entry level to advanced level in terms of education and experience. So, that's about the only thing that it would provide is just those very general guidelines to get you from one point to the next.

>> Are you back online with your slides?

>> No, I'm not but I only had one left so it's not a big deal and you know, some of the things that we want to remind everyone of is that there are different specialty areas within higher education that don't exist within the federal government or it doesn't exist with an industry but adoption of framework language such as nice is nice for all of us attempting to staff in our cyber-security departments. I suggest if more of us begin in higher education that is begin to use the nice framework it would make it easier for those of us who are trying to hire from the federal government to understand what they did in their roles in their previous roles and it also would be a great benefit for those who are developing curriculum within the higher education progression of a cyber-security degree by using those roles and responsibilities that are outlined within the nice framework and then we can develop our classes around specific job descriptions associated with those roles and then whenever those students graduate and they are in the job market, their respective employers can understand exactly what it is they've learned within their educational experience. I think there are a tremendous benefit in higher education in not only hiring people but in our academic programs.

>> Todd thank you for discussing the nice framework. We're going to move on to the next presenter at this time so we need to reset the stage, so we will go silent for just a few moments. Thank you.

>> Very good. Thank you.