Cyber Career Pathways and Opportunities

featuring Randy Trzeciak as Interviewed by Palma Buttles-Valdez

Welcome to the SEI Podcast Series, a production of the Carnegie Mellon University Software Engineering Institute. The SEI is a federally funded research and development center sponsored by the U.S. Department of Defense. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.

Palma Buttles-Valdez: Welcome to the SEI's podcast series. My name is Palma Buttles-Valdez, and I am the director of the SEI's Office of Diversity, Equity, and Inclusion. Today I'm joined by Randy Trzeciak, deputy director of cyber risk and resilience in the SEI's CERT Division. Randy has been a guest on our podcast series before, and we will provide links to his previous episodes in our transcripts. Today, we are here to talk about the various paths that people can take into the field of cybersecurity. Welcome Randy.

Randy Trzeciak: Thank you, Palma.

Palma: Let's start by telling our audience a little bit about yourself. What is it that you do at the SEI, and what is the best part about your job?

Randy: Thank you. I appreciate the opportunity to share some of my experiences and look forward to our conversation today. I am currently the deputy director for cyber risk and resilience, which is a directorate in the CERT Division of the Software Engineering Institute. As the deputy director, I

am involved in the day-to-day operations of cyber risk and resilience, looking for ways by which we, as a federally funded research and development center, can provide assistance to the United States Department of Defense, the United States federal government, law enforcement, industry, as well as academia. In addition to that role as the deputy director, I have been involved for a number of years in the work that the SEI has been doing in insider risk and insider threat. Very privileged to have worked over a course of a number of years on doing insider risk, insider threat research as well. One of the things I like about my job is that I also have a dual appointment to the Heinz College, the Graduate School of Information Systems and Management [at Carnegie Mellon University]. And that provides an opportunity for me to be the program director of a Master of Science in Information Security degree, as well as advising 80 plus students, as well as being an instructor teaching information security/data security courses for graduate students at the Heinz College. What do I like about my job? It is the uniqueness's of opportunities that are available at Carnegie Mellon University. The uniqueness of opportunity at a federally funded research and development center, and really being at the birthplace of cybersecurity, being the CERT Division. It is just a great way to be exposed to some great thought leaders in cybersecurity, provides the ability to work with the Department of Defense organizations, government organizations, and law enforcement as well. Just the opportunity to provide direct support to the national security of the United States. I really appreciate the opportunity. I have been here for a number of years, and it has just been great to work with some fascinating people, some very intelligent people. And I think we are doing a lot of great work here at the SEI.

Palma: Yes. You are. I can say for sure. Before we start talking about paths into cybersecurity, let's talk about your own journey into this area of work. Can you tell our audience about your early professional influences and what actions that they took that may have had the greatest impact on you?

Randy: I am happy to do that. Starting back with my undergraduate degree, I was fortunate to have gone to the university to get a degree in management information systems, as well as a dual degree in business administration. That right there really was not an entry into cybersecurity but was an entry into technology that provided a great opportunity to learn the foundations of the usage of information systems, the usage of information technology. And from there I was able to build upon cybersecurity experience and exposure. I went on to get a Master of Science degree at the University of Maryland, which was in business management. Again, not directly related to cybersecurity, but really, the early influences came with opportunities to

apply technology to try to solve organizations' challenge problems to make them more efficient, and at the same time to do that securely. In my early stages of career, I was building executive information systems at the Naval Research Laboratory in Washington, D.C. That really gave me exposure into databases and data security in formal systems, like database administration. I was also a software developer, and that gave me some pretty good exposure into developing interfaces into backend databases. But really, it was the usage of the technology to try to make organizations more efficient. And then looking at the challenges from an efficiency standpoint, but also from a security standpoint. And again, working with some great people. I had a great exposure in my first job to a very influential mentor who walked me through the usage of technology and critically thinking about challenge problems and then to be able to apply that in looking for ways by which you can test and add security in, rather than add security on. And looking at ways by which you build security into the development of systems, into the data management systems rather than just trying to add it on later. Again, was very fortunate in opportunity and certainly very fortunate with some great people that were able to provide mentorship and mentoring-type support that provided a career trajectory, not a straight line, but certainly gave advice and guidance. And that is certainly the recommendation I would encourage all the people looking, you know, and watching this video here today, is look for those opportunities to bounce ideas off of. Looking for people that you can trust to give, you know, advice and guidance. Not always agreeing with you, but giving you their opinion and taking the opinions of others and forming your own career path and trajectory, knowing that it is not going to be a straight path to the ultimate career goal for any individual.

Palma: You are a good example of the traditional is not always the way to get into cybersecurity, so that is great. You are also a mentor to future generations of cybersecurity professionals because you are bringing it around. Let's shift directions a little bit now and talk about some other items that we were going to talk about today. In our work, we are continually hearing and seeing reports about cyber shortages and demands for workers in the field. According to the latest ISC2 Cyber Workforce study, the cyber workforce grew by 10 percent last year. Despite that, there is a shortage of cyber professionals that remains and has nearly reached the four million mark, which is pretty high. These shortages can have a devastating effect nationally, I would say. ISC2 also found that two-thirds of organizations lack the staff necessary to prevent or troubleshoot security issues. What barriers to entry in cyber are you seeing that could contribute to this shortfall?

Randy: That is a great question, and certainly the challenge is that

domestically we are facing and internationally, it is pretty significant. And we certainly need to do more to encourage individuals to consider cybersecurity information technology careers. If we think about this in two perspectives, first, from an organization standpoint, I see the challenge being that organizations are in need for cybersecurity professionals. At the same time, they are in need for *experienced* cybersecurity professionals. Someone coming from an undergraduate degree or a graduate degree with little or minimal work experience, they are really being challenged to be able to be hired by organizations with knowledge, but maybe not with those skills and ability. What I would say from an organization standpoint is, aspire to hire experienced cybersecurity professionals, but really aspire to hire folks that can critically think about the challenges that you are facing. Challenges that can be overcome by quick learning and quick learners. That as we look for people that are coming with minimal experience, look for someone that has the ability to learn something quickly, efficiently; critically think about the problem they're trying to address and looking for ways by which individuals can solve a problem, not only someone with specific experience to solve a particular problem. That is one thing that I would see from an organization standpoint. Really encourage you to consider those entry-level people for some of your positions and put them on that fast-track to be really critical in your organizations that have to be effective as quick as possible. Now, when you focus on the individual perspective of, *I want to apply for a cybersecurity job*, people in some opinions, and the folks that I advise as part of the graduate students here, they are wondering, *am I technical enough*? *Am I enough from a skill perspective, am I an experienced programmer? Do I need to be an experienced programmer?* Many times, in this social media world that we live in today, people are always comparing themselves to what they perceive everyone else knows but they do not know. They think that everyone knows everything, and I know very little because you are only comparing yourself to the aggregate of the entire environment that exists today. Going into cybersecurity, recognize that the field is about a mile wide in terms of opportunities to where you could be an expert in network security or security architecture. And that may be specifically cloud or industrial control systems or operating technology security, or maybe you are an expert in asset security, maybe risk management, maybe software security. There are a lot of opportunities, but really, when you try to compare your knowledge, your skills and abilities, no one is an expert in all of those areas. What I would recommend is focus on the critical few first. Become an expert in a couple of areas, or more than one area if you have the opportunity and expand your horizons from that point. But do not compare yourself to the aggregate of what everyone else in cybersecurity is perceived to know, just really focus on what you, as an expert, can be. And also, from

the standpoint of not all jobs in cybersecurity require an in-depth technical skill in a particular technology. There are opportunities in policy or legal or privacy where you do need to have that technical foundation, but you do not need to necessarily need to be an expert in all of those areas. Just generally think of this from the individual perspective. Apply yourself and critically think about the opportunities and really just, you know, expand your horizons as you do go to work for that first organization or second or third, and look for opportunities to expand your career trajectory to include many areas that cybersecurity has comprised.

Palma: That is excellent advice, Randy. I will tell you that at many of the conferences that I go to, the students will say, *I am not sure if I have enough to get that first job, or my skillset matches the need*. Thank you very much. That is, I think, very good advice. Thinking back again, talking a little bit more about jobs, is there really any difference in how one should pursue a job in the government versus the private sector, or even in our area, which is in the federally funded research and development center, or national labs, or UARC?

Randy: Well, certainly the opportunities are similar from a technology standpoint. The same challenges that are facing organizations whether they are DoD organizations, federal government organizations, law enforcement, or private or even academia, the same type of technology is being deployed. The same thought process should be applied for looking for threats, looking for vulnerabilities, identifying from a risk management perspective what the potential impact to our organization would be if we're being compromised by a threat exploiting a vulnerability. The foundations are the same, but organizations may be challenged differently from different threat actors if you are in a government space, if you are in industry space, or if you are in the academic space, or the law enforcement space as well. That is common knowledge, the skills that we talked about before will be common across the organizations. When you tend to go to work for a government organization, particularly here in the United States, different threats might try to exploit vulnerabilities. Different threats may try to cause harm to a government organization. But really what you are looking to do is to apply a solid risk management perspective to an organization, whether it is government or non-government, and try to address the vulnerabilities to reduce the likelihood that threats can impact organizations. What we have seen in the government space, the DoD space, is really just opportunities that exist, similar to the private sector as well, but you are really focusing on protecting the national security of the United States. Which again, in itself, is a rewarding opportunity to go to work for a government organization, or at an

FFRDC like we are, or a UARC that we talked about as well. And again, the same mission across the government may not be the same mission across the for-profit organizations. But really, the technical challenges are pretty similar. The ways by which you do a risk assessment when you do things like penetration testing and vulnerability assessments, incident management, that seems to be pretty similar. Truly up to you as an individual to decide what type of organization would you like to go to work for and does it really meet what you want out of your career that includes more than just financial compensation for whatever career that you are being paid for to do this. A lot that also that goes into a rewarding job as well.

Palma: Thank you. If I was a younger worker, for example, the traditional trajectory of high school to college, and I am trying to join the next generation of cyber professionals, or if you were someone like myself, who had a career and maybe wants to transition into a field of cybersecurity and needed to be upskilling, what is the educational baseline and what path or paths should I consider to build off of that? Certificates, go to conferences? All of the above? None of the above [laughs]?

Randy: That is a great question. And certainly, the more of the above the better. But keeping in mind again, if you are coming directly out of high school or you are coming directly out of undergraduate or graduate school, you may not have the experiences in terms of formally applying that knowledge, that skill and ability to an organization's challenge of protecting their cyber asset. As you look to build upon formal education, and the more formal education traditionally the better, whether it is an undergraduate degree in a technology field, an undergraduate degree in cybersecurity, a master's degree or PhD program, look for ways by which you can get that experience. The ways by which you can actually take the initiative to learn a tool, learn a technology. Because really what you want to do is present yourself as a life-long learner to an organization. You have demonstrated through high school, through college, through a master's program, through a PhD, you have learned something in the theoretical sense and hopefully, most of those programs will include some type of an experiential learning component where you are applying that knowledge and using a tool or technology. But in addition, what you do on your own is very, very important as well. Sell yourself as, *this is something that I have learned. This is something I have picked up on my own. This is what I intend to learn next,* as organizations should be looking for you as a way to keep up with technology. What we are using today and three to five years in the future will be different, if not completely different. You want to be able to be adaptable, to be flexible. But also, you have the curiosity to want to learn about the tools and the

technologies to keep up with the challenges that organizations will face. Let's say that you do get that first job as well. You might come in somewhat overwhelmed by, again, what you do not know. Certainly, look for the opportunities for that continual learning. Many organizations will try to incentivize you by professional development opportunities. That might be part of yearly goals and objectives. Keep up with that. Keep up with those skills as well that have been formally applied by the organization. But also, look for those opportunities for mentorship. You know, great organizations provide the ability for younger workers to be mentored by more senior, more professional individuals in the organization. And I will tell you that many times, that as one of the more senior members at the SEI, I am almost flattered when someone, a junior person comes up to me and says, *would you be willing to talk with me or maybe go out for coffee?* And that type of thing, that really kind of makes me feel fulfilled in my organization, and that is one of the things that your previous question talked about what I liked about as well. Look for those formal mentorship opportunities, maybe the informal as well, and that's not always your direct supervisor. That could be someone in a different line of business, someone in a different department. Just someone that you can actually get advice and guidance [from] that could be very, very helpful in your career. And look for opportunities, whether that is informal education for internships, you know, go out on a limb and apply for an internship and go out and look for some of the fellowships that might be available as well. One of the ones that I like to very quickly promote is the Heinz College, the Graduate School of Information Systems. We have a fellowship specifically for cybersecurity. We are looking to bring students to the campus of Carnegie Mellon to pay you in a fellowship to take cybersecurity classes and give you project work as a way to give you some experience and exposure as well. The Heinz College has a great relationship with the Software Engineering Institute, and we build that into our fellowship as well. Again, lots of opportunities to be a continual learner. Think critically to really offer yourself as available to organizations once you are hired by them to look for increased leadership as well as experience in other opportunities as well.

Palma: Thank you, Randy. You remind me that your comment about being asked to be a mentor to get some guidance may be letting folks know that sometimes it is uncomfortable to ask somebody, *hey, can I get some advice from you*? But take that risk and suggest that people go ahead and do that…

Randy: Yes.

Palma: … because you never know, you may get a really good mentor.

Randy: I agree. That is very helpful. And I will tell you that it is much easier to ask questions on your way in the door, and the longer you are there, the more you're perceived of *should be knowing things*. As you go forward as well, you ask questions continually. Again, if you have that mentorship relationship, it is a great opportunity to build, you know, professional and maybe even personal relationships as well.

Palma: Or, if you live in a smaller community, maybe you go to a conference and you might meet somebody that could be a potential mentor. It is not only at work, there are other places that you could find mentors in this area.

Randy: That is great. And Palma, you did ask the question—

Palma: I do know—go ahead.

Randy: Yes, I am sorry, you did ask the question about certifications. I did not intentionally exclude that. There are a number of certifications, again, we said the more the better. But certainly, think about certifications specifically of what is the job that you are looking to get. What is the career direction you want to pursue, because again, there are generalist certifications, and a couple examples of those would be maybe a CISSP or a CISA or a CISM. Those are more for the generalists. And there are more specific technical certifications in database or penetration testing or things like that. Again, is it good to have a certification? The answer is absolutely, yes. But again, it should be preparing you for the job you are going to get and as well as the job that you are getting now. And in some organizations, they will incentivize you while you are employed with the organization, that they will pay you for those certifications as well. Just something to consider. I think it is a great opportunity to consider getting a certification.

Palma: Randy, when you apply for a job in cybersecurity, do most of those say if they require certification? If you find a position that you are interested in, do they typically say, *a certification in this area is suggested or would be good*?

Randy: Yes.

Palma: Is that the case?

Randy: I would say many of them will say that a CISSP is required, or a CISSP is preferred. Or, particularly when you get into the more specialized

positions, when you get into things like penetration testing, they may ask you for a Certified Ethical Hacker pen test as a way that an external organization verified your knowledge, your skills, and abilities and your ability to use specific tools. Also, I am asked the question from my students that are graduate students, should I get a specific certification in a technology? And the answer is it depends. If you are going for a job that uses the technology and they require it, the answer is absolutely yes. But should I get a certification in a specific networking technology? Well, if the organization you want to go to work for is using that, it would certainly benefit you. But again, if it is a different networking technology, you may not want to consider a specialist certification, but more of a generalist certification.

Palma: OK. That is good advice.

Palma: We are going to move on a little bit, talk about you. I have had the privilege to work with you before, and one of the things that has always impressed me about you is your efforts to support diversity and future generations of cyber professionals. And I know that you were recently asked to represent the voice of male advocates at a women in cyber AI conference. Can you talk about the importance of diversity in your field? And maybe what diversity can bring to help solve our current issues in cyber as well as anticipating future issues?

Randy: That is a great question. I appreciate you bringing up the opportunity I recently had. That was back in March of 2024. ISACA, the greater Washington, D.C., chapter, was sponsoring a Women in Leadership and Technology conference, and I was very privileged to be part of a panel looking at ways by which that the cybersecurity field as a whole can really increase the diversity in those particular roles and responsibilities. From a diversity perspective, we generally as organizations are not necessarily keeping up with what the threat landscape is. From a diversity perspective, I think there should be more diversity in perspectives but also more diversity in experiences and ideas. And we talked before about the challenge problems and critical thinking. You know, organizations are being compromised by threat actors on almost a daily, if not an hourly basis. We just do need more thoughts, opinions, ideas, skills, and perspectives and experiences when we are trying to address the constantly evolving threat landscape. We mentioned earlier before about the millions of opportunities that exist in cybersecurity. The capacity is needed to think about ways by which we can encourage at the kindergarten through 12 level to bring those opportunities in terms of knowledge that these are careers that you can pursue all the way down at the kindergarten level. More and more young

kids are using technology at a very, very early age. Think about that as a way by which we can build security opinions and ideas and awareness at the very early ages all the way to the point where it could be part of a formal education, as a high school education, an undergraduate education, or a graduate education. We certainly need to be able to keep pace with the opportunity with just more people coming into the pipeline, and that is certainly what we try to do as part of this opportunity and many other great opportunities that exist to get more diversity into information technology as a whole, but also cybersecurity as a specific. Looking at the United States Bureau of Labor and Statistics, it is estimated about 24 or 25 percent of IT jobs are occupied now by women in the field, and that certainly needs to increase significantly over the foreseeable future. It is getting better from where it was, but it is at no point where it should be in terms of representing the population today with about a 50/50 even split between, you know, females and males that exist in the world today.

Palma: Randy, I have a question we really had not talked about, which is something you said made me think about, is you are an academic as well, and I am curious if someone is pursuing a degree, say in business, or in arts, are there any advantages to taking some basic courses in cybersecurity?

Randy: Absolutely. The advantage is that you, in those particular roles and responsibilities, business administration, arts management, healthcare management, whatever field you are pursuing, it is likely you are relying upon some form of information technology to do your job better, to do it more efficiently. And currently today where we are with the massive emergence of artificial intelligence and generative AI as well, more and more jobs will be supported by AI in the future, so certainly the knowledge of what AI can do for you to make you more efficient and do that securely would certainly be something that is beneficial. But what also I have seen over the course of the years is that historically, organizations have the technologists, and they have the business units or the functional units, and there is this huge gap or chasm between the technologists and the business units. If you have the ability to speak the language of the IT folks, speak the language of the business, to think critically about how do we apply technology to make the organization more efficient, you will be extremely valuable to any organization that you work with. The ability to communicate effectively in non-technical terms to the non-technologist [about] why we are deploying technology, why we are being faced with some of the challenges using information technology. If you have the knowledge and the skills, but also the ability to translate the IT-speak, because many organizations mystify cybersecurity with all the acronyms that exist today, but if you can wade

through that and you know enough to say *this is what we are doing, this is why we are doing it*, *this is how it is going to impact us as an organization, and this is how we are going to do it securely*, you will be very, very valuable to many organizations. That is a great point that you brought up. Yes, the more technology you know, the better to make more organizations more efficient.

Palma: Great advice, you may have more students in your classes than normal [laughs]. An important aspect of our podcast is transition. What resources are available at Carnegie Mellon University to those who are early on the path to a career in cybersecurity?

Randy: Yes, we mentioned earlier in the podcast about one opportunity, a specific opportunity through Carnegie Mellon University's Heinz College. It is the IT Lab Summer Security Intensive. And as part of that we do want to provide students an opportunity through a fellowship to come and study during the summer between their junior and senior year to come and take cybersecurity-related courses. In addition, we give them an opportunity to focus on project work as well. And one of the benefits of being at Carnegie Mellon is the great relationship CMU has, the Heinz College has, with the Software Engineering Institute. The SEI faculty will be teaching as part of that program, providing direct opportunities to work with government organizations through the project work, so that would be one of the opportunities that I would say is a great resource for someone that is studying in information technology or a related degree, and a summer opportunity to spend some time here in Pittsburgh, Pennsylvania. I would also like to call out some of the resources that are available through the Software Engineering Institute. As a federally funded research and development center, we do a lot of outreach and transition that comes in the forms of formal training, but also publications. We have hundreds of reports that are available on our website focusing on cybersecurity, software security, and emerging technologies like artificial intelligence and machine learning. Those are some of the resources that we have available through the Software Engineering Institute, sei.cmu.edu. I would also like to call out some of the great resources the federal government has available as well, including the Department of Homeland Security, CISA—the Cybersecurity and Infrastructure Security Agency. They provide a significant amount of material that is available through free online courses and assessment methodologies as well. That is a great place to start. You can also focus on some of those organizations that provide certifications. ISC2 or ISACA, they provide a lot of great material that is available. Through some of their certification programs they do offer scholarships for individuals as well to take some of their training, but also to take some of their exams. I would also like to call out

some of the massively open online courses or the MOOC courses that many universities are making available, a lot of their free cybersecurity or information technology training as well. Other resources, Women in Cybersecurity. That is a great organization that provides lots of great resources focusing on women in cybersecurity. And finally, looking specifically at minority-serving institutions. They offer great quality cybersecurity education programs for minorities in those particular areas as well. Those are just some of the things that I recommend that you start with, but there is a lot of information that is publicly available just going and doing a search. And like I said, trying to tie it back to you, as an individual, taking the initiative to learn something. To basically demonstrate your ability to keep up with technology, and that is what in my opinion, that organizations should be looking for. I have been hiring or been involved in the hiring processes through the SEI and other organizations as well, and I am looking for people that have the ability to think critically, to solve problems that can work independently, but also that have the ability to keep up with the changing and the pace of technology change that we are all experiencing today.

Palma: Thank you, Randy, for sharing your story with us today. And actually, I think we just got a mentoring session by Randy this afternoon as well. To our audience, we will include links in the transcripts to resources mentioned during this podcast. Finally, a reminder to our audience that our podcasts are available on SoundCloud, Apple Podcasts, and the SEI's YouTube channel. If you like what you see and hear today, give us a thumbs up. Thanks again for joining us, and thank you, Randy.

Randy: Thank you.

Thanks for joining us, this episode is available where you download podcasts, including SoundCloud, TuneIn radio, and Apple podcasts. It is also available on the SEI website at sei.cmu.edu/podcasts and the SEI's YouTube channel. This copyrighted work is made available through the Software Engineering Institute, a federally funded research and development center sponsored by the U.S. Department of Defense. For more information about the SEI and this work, please visit www.sei.cmu.edu. As always, if you have any questions, please don't hesitate to e-mail us at info@sei.cmu.edu. Thank you.