The Future of Cyber: Educating the Cybersecurity Workforce

Featuring Diana Burley as Interviewed by Bobbie Stempfley

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.

Bobbie Stempfley: Good afternoon. This is Bobbie Stempfley at the Software Engineering Institute CERT Division. You will notice for today's podcast we are not in our normal studio. We are all doing what we can to flatten the curve. During this really unprecedented time, we are recording from our homes. We haven't stopped, though, so I am really pleased today to have a guest, Dr. Diana Burley. She is the executive director and chair of the Institute for Information Infrastructure Protection, or I3P. I3P is a consortium of leading universities, national laboratories, and nonprofit institutions dedicated to the strengthening of the cyber infrastructure of the United States. If that weren't enough, she is also a full professor of human and organizational learning at the George Washington University [In July 2020, Dr. Burley was appointed vice provost for research at American University].

Dr. Burley is a global cybersecurity expert who advises organizations on strengthening their cybersecurity posture, managing cybersecurity risk, assessing human factors in the threat environment, and developing their cybersecurity workforces. That last part, the human element in the workforce, is a common passion for Dr. Burley and me. Thanks for joining me today, Dr. Burley.

Diana Burley: Thank you for having me today. It is a pleasure.

Bobbie: I really have enjoyed talking to guests about the future. One of the things that has really intrigued me is what we have tried in the past and what has worked and what hasn't, and what of that we can bring forward.

At this moment where we are thinking about a new normal post-global pandemic or coming out of the global pandemic, the time just seemed really right to do this and particularly to think about your area of expertise, which is humans and organizations within it. I was really wondering if you could start us off by telling us something about the research you are currently doing and the projects you are currently involved in.

Diana: Thank you, and you are right. This is an inflection point. It is a time for us to think about what have we been doing in the past, and how can we really adjust. For me, what has really taken hold is this idea that we can no longer sit in our stovepipes and look at problems from isolated disciplinary lenses. We really have to think across and to think about the whole of the problem and how different aspects of that can be addressed. The work that I am doing is really a continuation of what I have been doing for many years, and that is thinking holistically about how to develop global cybersecurity-workforce capacity, thinking about not just developing the technical capabilities, but *How do we do that within the context of actual work requirements and thinking very critically about how to get people ready to hit the ground running*? That includes human factors and how they interact with other individuals, how they deal with the environment. But it also includes a forward leaning to think about, as we move into these virtual spaces because of the pandemic, *How do we leverage technology? How do we integrate human behavior with automation, and things like that?* And so really, it is an opportunity for me to bring all of these different conversations to bear about the future of work, about the global cybersecurity workforce, and to really leverage that work to give us a good starting point to move forward.

Bobbie: What sparked you into this, right? I love the interdisciplinary and multidisciplinary nature because it is both, as you point out. What got you started?

Diana: Well, I am going to have to give all credit—and people will think that we have set this up—but this was really encouraged in my graduate study at Carnegie Mellon. My interest, my passion has always been on looking at a problem. Really, what encouraged me were the faculty members at Carnegie Mellon who said, *This is how we as an institution move science forward. It is by thinking about the whole of the problem but developing disciplinary expertise, so that we can effectively address these problems.* That has really been the impetus behind my work. It was my natural tendency, but it was certainly encouraged by my education.

Bobbie: Thanks for the plug. We actually did not set that one up, but Carnegie Mellon is a little bit of a special place there, right? I love the work that we do at the Software Engineering Institute at Carnegie Mellon because we can bridge the applied-research element of it, the whole of the problem within these particular domains. So, thanks for that. President Jahanian I am sure is equally grateful in that. I am intrigued by your comment about focusing on global cybersecurity-workforce capacity. Can you talk a little bit about how you see the problem being the same or different around the globe?

Diana: Yes. In terms of not having enough qualified people, it is the same all around the globe. What is different are the different contexts in which people work and perhaps the different policies and the underlying foundation of what the specific needs are. But in general, it is a problem that is faced around the world. As I travel as I did and I assume will again one day, and talk to people around the globe, we are finding that the problems are very similar. We are finding that there is a disconnect between what students are taught in school and what they need to do in the workplace. That there is not enough guidance from policy makers in terms of how to prepare people. There is a lack of consistency, and so much of my work has focused on developing guidelines and standards that will allow the global set of institutions to work together to be able to meet the needs of the global workforce.

Bobbie: So, Resilience Week 2019, you keynoted. It strikes me it was all about this topic, wasn't it? It was cybersecurity education, what works, and what was broken. So if we take this moment of reflection, what do you think we are going to bring forward from this pandemic to do differently? Or what should we bring forward to do differently?

Diana: I think that it is an opportunity for us to really think about what we should do differently. Hopefully, as we begin to emerge from this environment, we will begin thinking very critically about helping our individuals—whether they are citizens in general, whether they are students or people within the workplace—helping them to be more aware of their technology and of the technical environment. So, specifically, when we think about security awareness and we think about privacy issues. For many of us, we were lulled into a false sense of security because we worked inside an environment and perhaps our corporate environment had the types of protocols and safety measures that we did not really need to think about our behavior as much as we do when we are at home. My hope is that as we continue to work remotely, live remotely, in terms of schooling, shopping, all of these things that we are doing as individuals within the society, we will begin to understand the really critical importance of the individual and the role that the individual plays in overall security, cybersecurity in my specific case, but really security in general.

Bobbie: It is interesting because I am reflecting on a conversation I had earlier today about how, 30 years ago, we started thinking about this as an information-security thing, right? We trained and taught it as a really technical dimension. As our dependence on technology has evolved, our needs for security have evolved as well, and our need to think about all of the dimensions of security: the humans, the technology, the organizational culture, the processes. All that comes together around an emergent property of organizational and individual resilience.

Diana: Yes. Absolutely.

Bobbie: I can see that. I can see that parallel there. I remember a few years back, you and I talking about work that you were doing with the ACM Task Force on Cybersecurity Education. Can you tell me a little bit about what niche that filled? What was the gap that this needed to step into, and how is that changing the future?

Diana: Yes, absolutely. Really in order to think about the importance of that work, I am going to take you back about 50 years. Because in 1968, the ACM and the IEEE collaboratively published the first set of curricular guidelines in computer science. That set of guidelines really set the foundation for what computer-science degree programs are today all around the world. So when you see computer science at Carnegie Mellon versus computer science at an institution in Europe, you can be fairly certain that the foundational curriculum, that the students who have earned those degrees have had, is consistent. It is standard; it is the same. We did not have that in cybersecurity, so the work that I did, the task force that I co-led with my colleague, Matt Bishop out of UC Davis, was the ACM and IEEE's version of this new development for this new field. So we developed, along with a task force of other academics around the world, of global researchers, of industry people, and government contributors, we developed the first set of curricular guidelines for cybersecurity in global post-secondary institutions.

That curricular guidance document was published in 2018. Since then, ABET [Accreditation Board for Engineering and Technology], that accredits engineering programs around the world, has developed a new accreditation for programs in cybersecurity based on our curricular guidance. So we are seeing the emergence of—and I hesitate to use the word *standards* because we especially stayed away from that word because we recognize that there are many different flavors of cybersecurity. But, we wanted to at least have some foundational commonality so that when employers work with institutions to get students to come into their workplace, they have some sense that if they are getting a student who has now earned a degree in cybersecurity, they have some sense of what that means. There is something that they can rely upon. We hope that 50 years hence, that the same way that we look at computer-science programs around the world, we hope that that will be the case with cybersecurity programs all based on this foundational curricular guidance that we developed.

Bobbie: One of the things that we do in the CERT Division is partner with a part of Carnegie Mellon that you are familiar with, with the Heinz College, in production of certificates, master's level certificates essentially for CISOs (chief information security officers) and for chief risk officers. We have been able to take advantage of some of those curricular guidelines, even if it is not a degree in cybersecurity. But we have really been able to take advantage of some of that foundational work to help guide the kinds of things that…

Diana: That is great. In fact, we developed the document to enable just that kind of use. We did not develop it so that it was only used by individuals who wanted to create full degree programs. But we created modular blocks within the guidelines so that individual institutions could use it the way that it made sense for them.

Bobbie: I think that freedom is really important. A recollection of a debate six or seven years ago, right after the academy study about the professionalization, was, *Is the cybersecurity workforce ready for professionalization?* There was quite a fervor, perhaps, when your report came out and said, *No, it isn't ready*.

Diana: I remember that fervor quite well.

Bobbie: I am sure you do. So we have all been working and understanding what the gaps are and how much of it is professional. How much of it is trade oriented? Who and how can we fill this entire activity? I can see all these things connecting together. You have been pushing on all the different elements there. Perhaps for a moment, can we talk about the I3P?

Diana: Sure.

Bobbie: It has a great mission, right, a bridge-building mission. What do you think has been the most impactful part about that bridge building? What has happened because you have been able to build bridges that maybe would not have happened had you not?

Diana: I think it goes back to early in our conversation when I talked about looking at the whole of a problem. The real value of the I3P is not just that it is multiple institutions. And we have 26 different institutions, 17 academic, five national labs from the DoE, Department of Energy, and then some research institutions. But the beauty of the I3P is not just that we have this multi-institutional focus, but we also have a multidisciplinary focus. We are really able to push conversations—whether those conversations are through policy-type workshops, which we do a lot of workshops and convenings where we get different kinds of people in the room, or through research studies that we conduct. It is really being able to look at a problem and bring in experts across different disciplines who can come together and sit in a room and drive forward in a way that allows us to think very holistically. For me, that has been just the real value and benefit of the work that the I3P does. That is what I see as I talk to different sponsors and such around the country.

Bobbie: I think it is only fair to say that CMU is a member, is a participant in I3P. One of the things that I think we share through that is the work in developing security teams and incident-response teams globally. If you are going to have a security issue, it helps to know that there is someone there who can help. Who can help products, inside companies, and help nations, and other pieces. So what do you think, from your perspective, what has made the most difference there?

Diana: The most difference in terms of the I3P?

Bobbie: Yes. In terms of the I3P and this establishment or development of international…

Diana: Excuse me, ok. I think that it is bringing in the human-factors perspective and bringing that in along with the technical perspective, right? I think that even as we are seeing emerging changes in the technology now, we are really, I think, as a collective just starting to realize the importance of bringing the human-factors folks and the technical folks together. The human-factors people were there, but there was not an integration of the efforts and a conversation across those spaces. Really the work that the I3P has done was on the forefront of saying, *No, it is not sufficient to have two separate groups having this conversation, but we really need to have an integrated discussion so that we can begin to understand the impact and the interplay of those two areas of focus.*

So I think that that has really been a very strong contribution that particularly now, as we look at the way that automation is happening. We often talk about automation as if one day there was no automation and the next day there was, right? The reality is that it is a continuum. As you think about that continuum, think about the individuals who are working in that continuum and trying to secure systems in that continuum, understanding how humans, either as individuals who are trying to help to secure or humans who are using those systems, along that continuum and having to switch back and forth between what is automated and what is not. [This] really, I think, highlights the critical importance of having conversations across technologists and human-factors experts along the development pathway as well as the implementation-and-use pathway.

Bobbie: Most recently, probably two years ago, we participated in a national study, the Cybersecurity Moonshot Initiative, that really focused on this, this idea of how we make the default position for humans the more secure one. That elixir of usability and engineering and human factors in the product itself as well as the security considerations, all mixed together. I think as we bring all of the work you have done into how to think about how to teach people, how to educate them to do things, and then how to give them the experiences through simulations or other mechanisms to reinforce and validate, I can see the way the I3P can participate in that. I think that is particularly useful.

Last week, just last week, it seems like it was so long ago, you had an interview with ABC News where you talked about how criminals were taking advantage of the vulnerabilities, really specific in this moment. What do you think people need to look out for? How do we help advise them to see the clear and consistent guidance in what they are seeing and hearing?

Diana: Yes, the challenge is that notion of clear and consistent, right? Because there is no "clear and consistent" in an environment that is as volatile as a pandemic. What I like to really focus on is something that we talk about all the time and that is, trust but verify, right? So, even if we could just get that message across, but regardless of what the specific activity is, *trust but verify*, *trust but verify*, and just get that as a mantra, I think that we can begin to make some headway. As I mentioned earlier, there is a false sense of security that many of the folks who are professionals and have moved into a teleworking environment, because they are used to working under much tighter security protocols that perhaps they are just not aware of even, right? Now they are leveraging their own personal technology that is often not as secure. We have privacy concerns where we are sitting. We are sitting in our living rooms and studies. There are often other people around. So how do we make sure that we think about that? Being ever vigilant about protecting information, about knowing who you are speaking to, and a lot of the cyber-hygiene tips and tools that we tell people all the time. But they matter even more now, because we are having to leverage technology in very different ways, and we are doing it under duress.

Even when you know what the right thing to do is, when you are stressed because you do not know if your job is going to continue, because you have your kids in the other room that you are trying to home school, because your partner is sick or your parent is not with you, it can make you take shortcuts and make mistakes. I like to tell people, be vigilant, pay attention, and then if you do make a mistake, if you make an error, if it was related to work, tell your IT folks so that they can begin to remediate and address the issue. We have to just continue to help our society and help citizens around society to just stay calm and focus on the security aspects of the pandemic as well because there are people out there…Unfortunately, there are people out there who are trying to take advantage of any vulnerability that they see. So we really have to be careful.

Bobbie: Back to that, *How do we make the more secure option the default option*? Because everything is just taking a little bit longer right now. There is just a little more friction in the gears for things. So, if we can take the friction that might be associated with making a more secure decision away and make that easier that becomes more helpful. So, we have talked about a number of things that you have been involved in. Over the course of your studies in your career, what was easier to solve than you thought it would be?

Diana: It is not going to be an answer about a specific type of problem. I think that it was more just recognizing that I could be productive in all situations, regardless of how much that there was to do. It was a tip, actually, that my dissertation chair taught me, and that was about breaking problems apart into very, very small actions. Because when you do that, you are not trying to solve this very, very large task or accomplish this very, very large task. You are just trying to do these very tiny little things. For me, that helps regardless of the type of tasks that we are talking about. That was something that I was able to solve much easier than I thought I would.

Bobbie: I like that idea, and I think it is incredibly applicable to the world we are in today where we are complexifying everything. We need to break it down into these pieces. We are not going to engineer our way to security. We are not going to compliance our way to security. We need to bring all of these things together.

Diana: We need to bring them all together and just chip away. Chip away, and eventually we get somewhere, and do it with friends.

Bobbie: Exactly. Build the relationships that are needed and push things in all of these dimensions. I think that is really wonderful. I really appreciate your joining me today. Thank you so much.

Diana: Thank you.

Bobbie: This has been such a fun conversation and the human element of it, both the usability and the workforce, is so important. It needs every ounce of focus we can give it. I love the fact that this is a place we have been able to work together and push things forward.

Diana: Looking forward to many, many more years of collaboration. So thank you very much.

Bobbie: Absolutely, absolutely, and just to think that Carnegie Mellon started it all for you. I…

Diana: Yes. I always have. This is my Scottie mug.

Bobbie: Nice. I am super embarrassed. I…

Diana: And just so that George Washington does not get mad, I have on my blue for GW.

Bobbie: Okay. There you go.

Diana: I always have my Scottie coffee mug with me.

Bobbie: My Scottie coffee mug is sitting in my office on campus. So, I did not think to bring it, to bring it home. But I have the Carnegie red. So…

Diana: There you go.

Bobbie: What has been true of this discussion is, I think you have always, for as long as I have known you, you have personified that your heart is in the work. So I think the university would be, it remains proud.

Diana: Thank you.

Bobbie: If you would like to learn more about GWU's Human and Organizational Learning Program, please visit GWU.edu and search for "doctorate in human and organizational learning." If you would like to learn more about the I3P and what it is doing in cybersecurity research and cyberinfrastructure, visit www.theI3P.org. To learn more about what we are doing in the CERT Division and how we partner with government, industry, law enforcement, and academia to improve the security and resilience of computer systems and networks, please visit www.sei.cmu.edu. We will include the links in our transcript of the podcast today. Thank you so much for joining us.

Thanks for joining us. This episode is available where you download podcasts, including SoundCloud, Stitcher, TuneIn Radio, Google Podcasts, 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 email us at info@sei.cmu.edu. Thank you.