Assessing Cybersecurity Training

featuring April Galyardt as Interviewed by Suzanne Miller

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.

Suzanne Miller: Hello, my name is Suzanne Miller. I am a principal researcher here at the Software Engineering Institute. Today, I am very pleased to have April Galyardt with us. She is going to talk to us about assessing cybersecurity training. So welcome, April.

April Galyardt: Thank you.

Suzanne: I am very glad to have you here today. Before we get into the subject, I want to start with why are you here? What you brought you to the SEI? What is it that excites you about working here?

April: I get to work on a lot of different problems. I am a statistician, and the SEI has been working in software engineering and best practices there for a long time. As data and machine learning and AI [artificial intelligence] are becoming more and more popular, the need for statisticians and people to use this data and know how to keep it secure and know how to keep it safe...

Suzanne: ...and how to use it properly.

April: …and how to use it properly is a growing need. We are trying to set some of the best practices at the intersection of machine learning and cybersecurity.

Suzanne: How does that relate to cybersecurity training then?

April: The cybersecurity training, just training and educational assessment that was my specialty before I got here to the SEI. I was brought on to work with the Cyber Workforce Development team. They do a ton of training across the military, all the branches of the DoD, teaching people how to protect networks and all kinds of cybersecurity.

It's a very complex area to do assessment well. We've got a wonderful simulation environment where people can get in and really practice on a virtual machine and practice securing networks and the skills they need to be good cyber operators.

Suzanne: They actually have to respond to threats and do something...

April: They have to respond to threats, they have to secure networks, and they have to trace down the IP address of who's attacking them and really practice building some of these skills. It's a very complex training environment that we could get a lot of data out of, but a lot of the assessment research isn't quite there yet.

Suzanne: Okay, in terms of which of the data is actually going to be meaningful?

April: In terms of knowing which data to collect, how to analyze it. A lot of the assessment practices that have existed over the past 50 years were meant to deal with things like the SAT. So you've got multiple-choice questions and all this...

Suzanne: ...and then they're much more recognition and knowledge questions rather than application. We're really doing application here.

April: Exactly. So the statistical models that were on the standardized assessments, those are really just modeling, *Did they get it right? Did they get it wrong?* Whereas in cybersecurity and a lot of these application tasks, what makes it really hard is that there might be many right ways to do a thing. How do you model the good pathways versus the not-so-good pathways and actually capture that?

Suzanne: Some of the difference might just be timing. The good pathway is one that only takes you three minutes. The less good pathway, may not be a bad pathway, may be an hour.

April: That's exactly…a lot of the research coming out of cognitive science on expert-novice differences that I try and pull a lot from in building these statistical models, is exactly that. An expert has a lot of different tools at their disposal. They have got many more methods, and they are very good at choosing the fastest one for this problem. The novice tends to have like, they've got a hammer and they are going to hammer it...everything's a nail and I'm going to hammer it until it goes. So it takes them a lot longer.

Suzanne: Sure. So, what are some of the key things that you are dealing with in terms of the messaging? So there is the practical aspect of what is the data? But, what is the kind of information that people are looking for out of these assessments, and how do you ensure that that information is appropriate for the use?

April: That is something I have been thinking a lot about. The short answer is that being able to say anything out of this data is a big step forward. Again, if we are going from quizzes and looking at how people did on the quizzes to looking at what did they actually do, what do they try, are they making progress, are they trying good things…that is a big step forward, so being able to say some of those conclusions and give that detailed feedback. A lot of that, the first place that it is going to be useful is for the students themselves. As we get better at it, we will be able to give more feedback higher up the chain. The first place is you can tell the student, *It looks like you're doing this. Maybe try that*.

Suzanne: I have done some competency modeling, and so we talk about skills, knowledge, and process abilities. This is a very basic kind of thing. Knowledge is the piece that we have the easiest time assessing. *There is a right answer. There is a wrong answer. This is the body of knowledge. This is not the body of knowledge.* Skills is what you have been really talking about a little bit is in terms of having access to the right tool set and knowing, *This is the tool that belongs with this problem.*

Then there is process abilities, which is actually a lot more contextual. Because, the process abilities that I need for defending a network in DHS [Department of Homeland Security] might actually be very different from defending a network out in the field in the last mile. Are you getting into any of that piece at all, or is it really just still skills and knowledge at this point?

April: What you have actually hit on there is one of the reasons that this is hard. I tend to think about it a little bit differently. What you are calling knowledge, like the discrete pieces of information, this is that. The skills and processes can be modeled actually somewhat similarly, because a lot of the, *I take this, and I do that with it*, you have to put different pieces of knowledge together. You have to know that, *This network has these properties, and this network has these properties*. Even just the choice of strategy tells you a lot about where they are.

When somebody can't carry out their strategy, it can be very difficult to pull out of the data, *Were they unable to execute it because they were missing a piece of knowledge that they needed, or their strategy fell apart because they didn't know the process?* And, so teasing that apart is actually quite difficult.

Suzanne: What are the accomplishments that you would say in approaching this work that we have seen at the SEI so far in terms of helping people to understand the problem, which is part of what we do, and are there sort of some leading indicators, some, *This looks like a promising path for helping people to do better and better*?

April: It's funny because we are just beginning to collect the richer data and beginning to model it. Some of the leading indicators are things that as soon as you think about it you are like,

Of course. If you are looking at things on the command line, *Did they use the right set of commands? Which commands did they use in which order?* That is pretty useful, but one of the things that really distinguishes the novices from the experts is, *Did they use a pipe?*

Suzanne: Do they know the shorthand?

April: Yes, can they connect two different commands in the same line. Once they start learning that shorthand, that is a real indication of leveling up. You say that, and it seems so obvious, but until you tease that out in the data, it is not necessarily something...

Suzanne: There is a lot of need for this. DHS is one of our sponsors, and we do a lot with the Department of Defense. What are some of the training needs and things that you have seen that we have been able to do for those different kinds of environments, because they are not all the same?

April: No, we have got a lot of different things going on. It ranges from some pretty basic introduction to skills, like how to use a command line kind of things, all the way up to preparing people for more advanced training that might be provided by the NSA and other organizations. We also run a couple of the largest cyber games, the Cyber Guard and Cyber Flag. That data is a lot messier because each event is one thing.

Suzanne: Right, so it is one instance.

April: It is one instance. There is a lot of exploratory analysis that could be done on what the different teams are doing, but it's not something that happens over and over again, which you can reuse the results in the same way. That is data that I am looking forward to digging into.

Suzanne: What are you thinking about in terms of what the results of this kind of work you are hoping to get?

April: One of the biggest things is that it should help us speed up and streamline training. If we can give better feedback and faster feedback. Even just, at the beginning of being able to use the results, if we can give better feedback to the trainees, they can learn a little faster. They can get up and running. One of the hardest things about training people is that contextualization, knowing when to do this and when to do that...

Suzanne: ...and when to stop.

April: ...and when to stop and what to pay attention to even. So the more that this kind of analysis can pull out, *This is what experts do, and this is what novices do,* the more we can teach novices faster what to pay attention to and help them develop some of those skills.

Suzanne: OK, So this is a long-term project. This is not something you're going to finish...

April: This is a first piece of a bigger endeavor.

Suzanne: This is really our very first part of research. Nobody expects final results at this point, but it's exciting to talk about where we're going next. This is an area that I know, as a trainer myself, just doing subjective evaluation of students is what you end up defaulting to. It is not very satisfactory for the student or the teacher. So having us move forward in this arena I think is very exciting.

April: This is exactly the kind of thing that can make some of those subjective evaluations more concrete.

Suzanne: Sure, and more useful to both the instructor and to the students. I am looking forward to seeing results from your work. If you have got any resources that are related to this we will be posting them on the website for you along with this podcast.

I want to thank you for joining us today, April. I am very excited about this work because I do have to do my own training assessments, not in cybersecurity but in other areas. I am hoping there will be something generalizable out of this as well.

Suzanne: The algorithm that I come up with, as the data maps, we should be able to use it in lots of different areas.

Suzanne: Yay! So, I want to thank you again. You also have a blog post on this topic, so that is one of the things that people can look at. We also will have this podcast available through all the places that you get podcasts [Soundcloud], [Stitcher], and [Apple Podcasts]. Best thing to do is search on April's last name, Galyardt. G-A-L-Y-A-R-D-T. That should take care of it, and they should be able to find you that way. So, thanks very much. Thank you for viewing.

Thank you for joining us. Links to resources mentioned in this podcast are available in our transcript. This podcast is available on the SEI website at sei.cmu.edu/podcasts and Carnegie Mellon University's iTunes site and the SEI's YouTube channel. As always