Bobbie Stempfley: A Technical Strategy for Cybersecurity

featuring Bobbie Stempfley as Interviewed by Eileen Wrubel

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

My name is Eileen Wrubel, and I am the initiative lead for the Agile-in-Government Practice here at the Software Engineering Institute. Joining me today is Bobbie Stempfley who, in June of 2017, was appointed the director of the SEI's CERT Division.

Welcome Bobbie, thanks for joining me.

Bobbie Stempfley: Thanks for having me.

Eileen: Let's start off by having you tell us just a little bit about yourself and your experiences before joining the SEI and being appointed director of the CERT division.

Bobbie: I came here to the CERT Division after having spent 23 years as a federal employee working in a variety of jobs for the Defense Department and the Department of Homeland Security, largely in the application of information technology to national security missions, improving efficiency in warfighting and understanding government risk-transformation kinds of activities. Over that entire time period, 17 years in the Defense Department and five years at the Department of Homeland Security, I kept coming in and out of security, of computer security, as a part of that set of responsibilities.

It has been a great set of experiences in how to solve problems at scale and understand the application of technology to really changing the way we do things in the world. And then I left and came to federally funded research and development centers because what I wanted to do is really get back involved into the *how things happen* and really focus on, not just adoption-oriented actions, but on actually solving the problems before they appear.

Eileen: And transitioning them into application.

Bobbie: Absolutely.

Eileen: So you had a really broad and deep set of experiences at both the DoD and Department of Homeland Security. How does that shape or enrich your perspective now, as the Director of CERT?

Bobbie: That is a really good question. I have been thinking a lot about it because, at the Department of Homeland Security, I was the senior civilian over the office responsible for critical infrastructure cybersecurity and for federal executive branch cybersecurity. In the Defense Department I had a range of roles, everything from standing up the first-ever Department of Defense-wide CERT to being the chief information officer and chief risk official for DoD-wide applications.

The things I learned there, that are really informative here, are that the most technically elegant answer is not always the easiest one to actually implement. We neither are going to engineer our way out of these problems, nor are we going to buy our way out of these problems. We have to really have a holistic approach to solving so many of the challenges that we face today. When you add the scale to the complexity to the speed, we really have to think more deeply and strategically about where and how to engage.

So, bringing that here is really interesting because the Software Engineering Institute is this gem for the nation that sits here at the number one computer science school. Software is a truly strategic asset for not just the Defense Department and national security but for our economic viability and economic security. But we are not hundreds of thousands of people, and so we really have to think a lot about where we strategically engage, what challenges are the ones that are best for us to take on, and which are the challenges that are one step ahead of everybody else in the world that we operate in.

Eileen: When you were appointed in June of 2017, Paul Nielsen, our director and CEO, said *There has never been a greater need to address the persistent and growing cybersecurity risks that threaten the nation's defense, homeland security, and intelligence communities*. Let's talk a little bit about how the research that is happening in the CERT division is addressing them.

Bobbie: So that statement is really unbound, isn't it, right? *Cybersecurity is hugely important, and it is important to everything, and it is all moving faster and getting worse*. While I agree that the challenges we are facing today are different in a lot of ways from the challenges we faced over the last couple of decades, one of the things that I see today, that I didn't decades ago, was a real appreciation of the importance of focusing on assurance as a part of the development, implementation, architectural kinds of activities. So, I try to simplify what adversaries are going after. We "complexify" everything, and so I try to simplify.

Our adversaries are going after a small set of things. They are going after design trades we make [in software]. So, we build systems and architect them and there is never enough time, money, power, resources—whatever it is—and we make design trades. Adversaries are looking at what opportunities that creates. They are looking at failures in implementation. So, we understand these as vulnerabilities in today's world. Something didn't get built quite the way you though it would.

Eileen: Right, and you can exploit that vulnerability.

Bobbie: And you can exploit that vulnerability.

They are looking at our tunnel vision in use cases. We think technology is going to do one thing. We build it for something. We might test edge cases, but the thing I learned about working with 18-year-old sailors, in particular, is they use this stuff in ways you never imagined. Adversaries are looking for that.

Then, the last thing they are really looking at is the seams between efforts and activities. We know these things as race conditions or side-channel related activities. So, two pieces of software operate. They exchange data between each other. That's a seam. Or, one chip might run at a particular speed, another chip runs at a different speed. That creates an environment that you didn't expect in that.

Our systems are so complex today that there are lots of these seams. If you break it down that way, it really helps you focus on the things that you need to fix. You are not chasing every vulnerability. You are chasing, *How do I build things better*? *How do we work with the agile concepts you have with bringing security into secure-development-related activities. How do we build secure concepts for coding itself*? *How do we reduce the implementation risks that exist in that space? How do we help operators understand what their roles are in the environment so that they can play the hardest games in the scrimmage than they play in real space? How do we understand that risk, that overall enterprise risk-related efforts so we have continuity of practice, completeness of practice, and efficacy of practice in so many of these areas? And then, how do we really focus on simplification as often as possible? How are we available to catch when things go wrong?* So, we still have that practice of analyzing malware and looking at vulnerabilities so that we can speed up the distribution of the things that we know are wrong so others can put protections in place.

Eileen: I am going to take us back a little bit to what you said about software being an asset, being a strategic asset. One of the things that I talk about a lot in our work is that software is a strategic asset, and so the workforce that develops it needs to also be treated as a strategic asset.

Bobbie: Absolutely.

Eileen: So, what role asserts workforce development activity? What role are you playing in mitigating the growing cybersecurity threat?

Bobbie: I am actually going to take this in two ways, because the question and the setup are two different things here. I agree with you. Software is a strategic asset, and the workforce that develops it has to be a strategic asset. That workforce has to have tools and understanding about the role that they play. It is not just building Candy Crush and putting it out on the app store. They are actually building fly-by code kinds of pieces of software for airplanes, cars, and other pieces. One of the things that we do in the CERT Division is produce secure coding practice guides. We try to help that strategic workforce of the world understand not just their role but have tools to do their jobs more effectively and to offset those adversarial use cases I talked about earlier.

That is an important transition opportunity for a lot of the work we do. We do research. We find an answer that will scale, and then we promote that answer through training or through document standards or other mechanisms for the broader community. That helps reduce the implementation risks that come along. We are reducing the problem from the beginning as much as possible.

Then, the other part that we do is we really focus on workforce development for the cyber workforce, for those defenders and administrators that are in the national security space that need to understand how to do their job. We spend a lot of time building content for that community, specifically, because you have to tackle both, right? You have to both have folks who can build the software better and, recognizing that the adversary is always going to find a way, we have to understand how to be successful with that workforce as well.

Eileen: Going forward, what do you see as some of the most significant challenges that the nation faces in software and cybersecurity? What should we be doing now to address those? Dig into your crystal ball a little bit.

Bobbie: Really great question. The first one ties back to your comment about the workforce being a strategic asset. We do not have enough people, specifically in the cybersecurity workforce but writ large. We have talked about the national challenge of STEM-related activities. If you agree with the premise that software is a strategic asset (and it is, not just has it eaten the world, it is driving the world forward), we have to have people who understand that. It is not everybody, but it is certainly more than what we have today. I think that is a really important challenge area that we have got to take on and one that, certainly, Carnegie Mellon is focused on solving.

We have what I think about as high-velocity software production, so large volumes of software produced much more quickly, put in the hands of users more quickly to get feedback. All of this is really powerful, incredibly powerful, but it changes the dynamic for the adversarial environment, and so, *What does that mean as you are thinking about risk and as you are thinking about adoption?* There is this idea that security is the "Department of No."

Eileen: I've heard that.

Bobbie: Or, I call it the big security 180, which is where programs work with their security teams right up until the end, and they think they are in a good place, and then all of a sudden the security team says, *Oops, sorry. You are not good enough. You have got to go back to the beginning*. So we really have to think about what that looks like, today and going forward. I think that is one of the challenges that we are taking on here.

The final one is, we are in this very interesting world of machine learning and artificial intelligence where we have so much data and not enough data at the same time. It is this crazy paradox that is there, but we have to build those machine-learning algorithms correctly and with as few flaws as possible.

We have to understand how they are going to operate in a way that ensures that they are not taking on an adversarial mindset as a part of it. We have to understand that they are operating in a contested space, and so how do they stay secure? Then, how do we really think about understanding and assuring where they are going to go over time because they are going to evolve. I think those are really the challenges we are really excited to be taking on here.

Eileen: So it is an exciting time to be at CERT, and it looks like there's lots of great problems to be exploring over the next several years.

Bobbie: Wicked problems, I think we'd call them.

Eileen: Thank you so much for joining me to talk about this today.

Bobbie: Thank you so much for having me. It's been great.

Eileen: Great. This podcast is available on the SEI website at sei.cmu.edu/podcasts and on Carnegie Mellon University's iTunes site and the SEI's YouTube channel. As always please feel free to reach out to us with any questions you have at info@sei.cmu.edu. Thank you.