A Method for Assessing Cloud Adoption Risks

featuring Chris Alberts 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: Welcome to the SEI Podcast Series. My name is Suzanne Miller, and I am a principal investigator in the SEI Software Solutions Division. Today, I am joined by my colleague and friend, Chris Alberts, a principal cybersecurity analyst in the SEI CERT Division. Today we are going to talk about a method for assessing cloud adoption risk that Chris has developed.

Welcome, Chris.

Chris Alberts: Thanks. Good to be here.

Suzanne: You have been a guest on our show, but it's been a while. You are a pre-COVID guest. So welcome back. Let's start by having you tell us, what is it about the SEI that brought you here, and what kind of work do you do here?

Chris: Before the SEI, I was working in the area of robotics. I was developing robotic systems, mobile robots for hazardous environments. Part of doing that, you have to be very good at managing risk. I had started building up this interest in risk management, especially with respect to technology. The SEI had an active risk management program, and I joined that program back in 1995. I focused initially on software risk management, and then I transitioned over to cybersecurity risk management shortly after that, focusing initially on operational security. Today I have kind of moved left in the lifecycle. I am looking at how to build security in the system. So I am looking at risk early during acquisition and development of software-reliant systems.

Suzanne: Excellent. Many of the methods that you have built yourself and with colleagues have been very useful for different aspects of that, the OCTAVE [Operationally Critical Threat, Asset, and Vulnerability Evaluation], and then Mission Risk Diagnostic [MRD] is one that I am also familiar with that is really the foundation for this recent set of adoption risks that we are talking about. Tell us a little bit about Mission Risk Diagnostic and what it has been able to do for the people that have important missions that they need to protect.

Chris: We started this work probably about 15 years ago with the initial work with the Mission Risk Diagnostic. It is kind of a quick-hit diagnostic or a health check, is the way I often refer to it. It gives you a quick snapshot of what your major risk factors are. We can use it on mission threads, business processes, organizational initiatives, and things of that nature. We started focusing on software risk in terms of acquisition and development projects. Then we have also done versions; we did an early version on technology transition for one of our customers and then did other versions on software security, supply chain, incident management. We did several pilots with that one as well. We have done a range of different assessments based on the Mission Risk Diagnostic. I focus on, there is a platform for the Mission Risk Diagnostic, and there are different sets of risk factors that we have developed consistent with that platform.

Suzanne: This is the latest, and this is related to cloud adoption. Why don't you give us the variety of organizational and technical factors that you have found can affect an organization's cloud initiative, especially affect it adversely? Let's talk about the factors themselves a little bit.

Chris: OK. When we look at an organization initiative like adopting cloud technologies, what we often start with is some of the basics, planning and preparation activities. *Do you have the right budget for what you're doing? Have you set a reasonable schedule? Do you have the right organizational capability to do this work? If you are reaching out for third-party assistance, do you have that lined up?*

Then there is also governance and management issues. Looking at things like change management, managing your suppliers. One of the things to think about with cloud technologies is they are provided by third parties. So supplier management is a key part of that. Then you are getting around to the actual execution of the activities. As you are making this transition or adopting these technologies, there are engineering activities we are looking at from requirements, architecture, all the way through testing and evaluation, and then the initial deployment. Then there is quality-of-service issues you need to be aware of as well. The things you measure in terms of cloud, you are looking at performance, agility, security, scalability, things of that nature.

Suzanne: Gotcha. A lot of these are a mix of technical and what we would call socio-technical factors. In our experience…You and I both have experience in researching technology transition. It is those socio-technical factors that often are the ones that are the make or break. The technical

is probably where you are going to find other methods that would address risk factors, because everybody has got a way to rank themselves on their technical and quality-of-service capabilities. But not so much in the, *Did you plan right for this?* and *Do you have governance structures to make sure that people are using this correctly?* And things like that. So, when I read the blog post, I was really happy to see that we are continuing on with that theme [that] socio-technical is important.

The method is one that you said is based on the Mission Risk Diagnostic platform. For people that are not familiar with that, could you just give us a little bit of an overview of the method and what makes it more of a health-check diagnostic as opposed to an in-depth kind of risk approach?

Chris: Sure. As I said, we started developing the Mission Risk Diagnostic about 15 years ago, and the idea was to provide a broad-based initial diagnostic of an organization's capability in a given area. I often draw a parallel to a medical paradigm when I discuss this, so that you can think of the Mission Risk Diagnostic as equivalent to going to your primary care physician. I will talk in a minute specifically about how we structured it, but you are doing some basic things. Like, if you go to your PCP, they will check your temperature, blood pressure, and a few things like that. If there is some type of an issue, then they will have you do an ultrasound or an MRI or something of that nature. So we have positioned this as the health check, and we have deep-dive techniques that are associated with it and can provide specific information to us that relate to what we find in the Mission Risk Diagnostic. For example, we have a technique called the Security Engineering Risk Analysis Method, or SERA, that looks at architectural risk. So, if we find an issue with the architecture, we can do a deep dive into the architecture. We have another one that looks at leading practices for building security in. If we notice that there is a problem with the way that the organization is executing its practices, we can do a deep dive and do a practice-based assessment as well.

So we had designed this to be a way to do a quick check of where the major risk areas on an organizational initiative or mission thread are. Basically, each of these is somewhere between 15 and 25 questions. For cloud adoption, it turned out to be 24 questions. They are *yes/no* questions. We also allow for variants or responses related to probability, which is typically hard. They are *yes, likely yes, equal likely yes and no, likely no*, and *no*. That gives you an idea of the probability nature against each these risk factors.

Suzanne: OK. I am not going to get details of what all the problems are. I am really going to get that indicator of, *This is an area that we are probably okay. We are probably good on planning, but we are not so good on how we establish quality of service, so we need to go deeper into quality of service.* For this set of factors, do you have the detailed kinds of activities yet? Or is that still some of the research that you have yet to do?

Chris: Well, very similar to what we have done here with the Mission Risk Diagnostic, most of our analysis methods can be adapted to various types of technologies. I mentioned the Security Engineering Risk Analysis, or SERA method. We've done that on all kinds of technologies. We did a pilot of that with cloud in a cloud environment several years ago. Much like the Mission Risk Diagnostic, we can do these follow-on assessments in a variety of environments.

Suzanne: Some of the magic is that these techniques can be applied to multiple kinds of technologies, and this is the latest in the set that you are applying it to. You don't necessarily have, instead of SERA, you don't have SERA, cloud.

Chris: No.

Suzanne: You don't have CERA yet, but you might if it turns out that the cloud is such a big deal that it has its own special flavor of that you could go there. MRD has been piloted in the field extensively, but how new is the set of cloud-assessment risk factors? Have you had a chance to pilot this in the field yet?

Chris: Well, they are very new. About a year ago—and this was kind of done as a side project—we had the opportunity to look at adapting the Mission Risk Diagnostic to a cloud environment. We brought together three types of information as we did this. We had done various technology adoption of risk assessments in the past. We had that as a basis to start with. Within the documentation within the community, Google and Microsoft and Amazon all have cloud-adoption frameworks that they have published. They are publicly available, so we mined those as well. Then, as you know, the SEI has a lot of people with cloud experience, and we consulted with them as well. We took these three diverse sets of data and put them together and came up with this initial set of cloud-adoption risk factors.

Now, we have not piloted them yet. This is basically…When we put together a new set of risk factors, the first step is to do what we just did, mine the available information and use this as a starting point.

Suzanne: By publishing it into the field, you will get interest from various places. I assume that you have interest in collaborating with organizations in the DoD, and commercial, DHS, across a wide breadth. We have that info@sei.cmu.edu email that is very useful to all of us. That is a great place for people that are interested in collaborating on this to contact you. But I also know that the way that, historically, you have built your methods, they are quite self-service as well. Am I correct in saying that you are welcoming people to send you, *Hey, here is what happened. Here are the results that we got from when we applied this on our own?* And then that is another way you can get feedback on, *Why did you ask us this question? That turned out to be, like,*

totally weird and, took us down a rat hole. And why do we do that? That kind of dialogue I know has happened in the past as well.

Chris: Yes. So people who self-apply, we would love to get their feedback. A lot of people, especially with this method, just take it and run with it. Often, we don't even hear back from them. Or sometimes we'll be at a conference or some other place where you run into somebody that said, *Oh, yeah, I used this method and I found it very useful*. But we would like to get feedback that way from people who have applied it, and we also like to pilot these when the opportunity arises as well.

Suzanne: Sure. OK. I'm excited about this. I may actually end up being one of your users for this. We will talk about that offline. But I want to mention for a minute, just transition in general, and I know your history. You are very, very focused on making resources available to people for self-serve, so that they can do as much as they can on their own. What resources are available beyond the blog post, and where can they be found? Then we will make sure that all the audience gets links to all of those places as part of the transcript.

Chris: Right. We published a lot of information on the Mission Risk Diagnostic related to some of the different variants that we have done. I think the most published versions are for the software-project version and the incident-management version, and those are available on the SEI website. In addition to the blog post, we have a white paper that accompanies it for the cloud-adoption version. Basically, we have a set on developing the risk factors that we published, a technical report that we published several years ago. At that point in time, we were calling risk-factors mission drivers. It is a focus on how do you develop a set of risk factors for any unique situation that you look at. We have a number of things published throughout the years. Cloud adoption, the white paper and the blog post right now is all that's available.

Suzanne: OK. So the mission-drivers technical report, if people are really interested in how this developed, and they want to extend this for their own particular cloud-adoption context, then they could actually go to that and say, *What are some other drivers that we should be looking at?*

Chris: Right.

Suzanne: If we are a medical device firm or whatever the particular context is.

Chris: Yes, so that breaks down into five or six areas that you should think about when you are identifying drivers or risk factors related to whatever problem you are looking at. That actually comes down to the approach that we take when we develop them as a way of documenting how we approach the problem.

Suzanne: You are one of the technologists that gives away the secret sauce. I really find that wonderful because it does make it more accessible, but I also am always surprised at how few people actually use it. It is like, *We don't really want to know the secret sauce. We just want you to make us the dinner.*

Chris: Right, right.

Suzanne: It is an interesting thing to reflect on sometimes. All right, I want to know what is next for you. You are someone who does not sit still and does not rest on your laurels. What are you thinking about now, and what should I be talking to you about in a few months?

Chris: Well, one of the ongoing tasks I am working on is the SERA method. We have been working on that for about five years or so. What we are doing right now with respect to that is we have a concept called *threat archetypes*. Our long-term vision is to create a library of these archetypes that basically, based on system type, you could then identify a set of threats that you need to consider for that type of system. That is now one of our background activities but something that we are looking to, hopefully in the next fiscal year, do a little bit more aggressively.

The focus right now that I am working on is developing a set of cybersecurity engineering practices, leading practices, across the lifecycle. A couple of years ago, we started this work, and we also go to an accompanying assessment called the Cybersecurity Engineering Review, CSER, that we use to assess programs against these leading practices. Recently, I won't say recently, about a year ago, I started collaborating with several colleagues across the SEI. We are taking the engineering practices, along with some supplier-management practices—I think it was supply-chain risk-management practices—some program-management practices, and putting them together in a broader framework called the Acquisition Security Framework.

We are about two-thirds of the way done with developing that. That will give us an opportunity to look at a program across the lifecycle, look at their in-house engineering activities, their contractors' activities, as well as any third-party software that they are using and look at how well they are putting all that together and creating some of these complex systems that we see these days.

Suzanne: I know from having participated in threat-modeling workshops as one of the program participants, I am loving the idea of the threat archetypes because that is really hard to wrap your head around. I think it took me almost a whole day before I could get into the space for doing that. So I hope that work goes forward quickly.

Chris: We have an initial white paper on that on the SEI website that people can refer to as well. We at least have an initial prototype of how we are looking at documenting these archetypes, and

so people can look at that. It seems like the idea of putting them together in a library really resonates with people.

Suzanne: It certainly does with me. Well, I want to thank you again for joining us today, Chris. I am always interested in what has got you going and the kinds of things you are doing because you are wonderful at the outreach and making sure that your work is accessible to the community. I know that is going to be important to our readers, and I know there are lots of DoD and other programs that are in the middle of moving to cloud-based systems for doing their work. This is really important content for them to be thinking about. So, thank you.

Chris: Thanks.

Suzanne: I do want to say to our audience that you can get this podcast, video, audio, SoundCloud, my favorite, of course, the SEI YouTube channel, and so please, access it however is best for you. As I said earlier, we will have links to all the resources we mentioned in the transcript, and I want to thank all of you for joining us this very fine day.

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.