The Silver Thread of Cyber in the Global Supply Chain

Featuring Matt Butkovic 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'm a principal researcher here in the SEI Software Solutions Division [SSD]. Today, I'm very pleased to welcome to our podcast, Matt Butkovic, technical director of Cyber Risk and Resilience within the SEI CERT Division. Today, he is joining us to talk about his team's very exciting work in assisting the World Economic Forum [WEF] with mapping high-level cybersecurity challenges. Welcome, Matt.

Matt Butkovic: Hello, Suzanne. It is great to be here.

Suzanne: Excellent. Before we delve into our topic, let us start by having you tell us a little bit about yourself, your background, and the work you do here at the SEI. People like to know about the people that we are talking to. What is the best part of your job?

Matt: Sure, thanks. I have been with the SEI for about 11 years. Prior to that, I worked in industry, specifically manufacturing and then banking before that. My focus here at the SEI is really on helping organizations understand their cybersecurity posture, both from a process perspective and from a technical perspective. I [am also on the Carnegie Mellon] adjunct faculty and teach graduate courses, and I participate in executive-education programs for Heinz College, so the CISO [Chief Information Security Officer] Program, the CIO [Chief Information Officer] Program, [and] the CRO [Chief Risk Officer] Program.

Suzanne: Excellent.

Matt: There was a question about what I like best about my job. I think if I had to describe the single best thing about my job, it is the intellectual freedom I have to explore things that I find interesting and relevant and useful for the profession.

Suzanne: I agree with that. There are amazing things that I have learned here I never would have been able to learn anywhere else and certainly not in industry. So, I second that. All right, but today we are here to talk about your work with the World Economic Forum. And tell us a little bit about the catalyst for this engagement, because the SEI is not the Software Economic Institute, right? We are the Software Engineering Institute. So how did this come about?

Matt: No, certainly. It is an interesting story, and one that is somewhat unique. This is truly a whole-of-CMU story. The World Economic Forum has engaged CMU in a number of topics—cybersecurity is just one of them. The initial request for our participation came from Dr. Jahanian's office, through our business-development function here at CERT. Joe [Joseph] McLeod brought the opportunity to me, and we then assembled a team to address how best we could help the World Economic Forum in curating an artifact they call a *transformation map*.

Suzanne: What is a transformation map? Give our audience a little bit of background on that if they haven't read about this yet.

Matt: Yes, certainly. The World Economic Forum uses the term transformation map to mean a set of connected concepts that define a specific domain of interest, for instance cybersecurity, or artificial intelligence, or vaccines. It spans the entire spectrum of topics. It's a way to affinity-match concepts and then moreover, and maybe most importantly, create linkage between those topics. For instance, the cybersecurity map then links to other topics. I'll give you an example. The cybercrime topic links to the broader topic of crime. The automation and machine-learning pieces of our discussion of cyber link to those topics in the top-level categories as well.

Suzanne: OK. So it is a sophisticated concept map, and it allows the World Economic Forum to look at relationships between different areas of interest and perhaps find connections that they can leverage. Or that, in your case, that might actually be ones that they need to be aware of in terms of risk.

Matt: Yes, that is exactly right. The primary purpose of the map is to lead the reader into specific channels of information that may be of interest for them. It is meant to convey a path in a very concise manner to those that are interested.

Suzanne: When you think about things like cybersecurity, cyber resilience, that path is needed; a guided path is needed because otherwise there are just too many things to think about. Our brains, even though we don't use all of our brains, we still can't put all that stuff together in a picture that allows us to act. That is one of the things I know in my own work, the little work that

I have done with cybersecurity, it can be very numbing to look at all the possible scenarios and all the possible risks and go, *What am I going to do about this?* What does CERT bring to the table in this work? I am leading the witness here because I know one of the things you're going to say. But how is it that you make this manageable and get the information that you need to create this kind of a transformation map?

Matt: Yes. I think your description is really a good one, which is if you look at this as an inexhaustible catalog of problems, it is so daunting that you don't know where to start. It's the paradox-of-choice problem. If I said, *Here are 10,000 topics to have a look at, you may pick nine.* But people think in stories. They think in narratives. In a sense the transformation maps are a set of narratives that lead you to specific topics germane to that subject. What does CERT bring to this? Well, I would like to think that CERT is the premier cybersecurity equity. As you know, we are one of the nation's oldest cybersecurity equities.

Suzanne: Yes.

Matt: I think that the honor of us being asked to curate this specific map cements our position or maybe reconfirms our position globally as thought leaders in this space.

Suzanne: Yes. Personally, as somebody who has economic interests, even though they may not be like the big financial ones, I'm glad you are there. Because making our connections into the security realm related to economics I think is one of the big things. In 2008, I worked with some of the CERT folks in doing some scenario planning on cyber and cyber resilience. At the time, that was like the first time that I had really hit the topic of cybercrime and how cybercrime could be such an impacting area of criminal activity that I just never really thought of before. That is one of the areas you mentioned. This is really, 12, 13 years later, we have seen a lot, ransomware, etc., cybercrime, but now I think we're getting more of a handle on it. And these kinds of maps are one of the ways that people can understand, *What is the connection between my economic issues, my cyber-resilience issues, criminal activity, things like that*. Who did you collaborate with to get some of that additional knowledge? Because it isn't just the knowledge inside the SEI that makes this work?

Matt: Sure. The team had a broad base of experiences. I tried to draw on those, of course, to have the most expert opinion that we could find within the organization. Within CERT, I was working with, in no particular order, Kris Rush, Chris May, with Alan Levine, and Brett Tucker. That was the team.

Suzanne: What about collaborators within the Economic Forum and the Carnegie Mellon community?

Matt: Sure. The process that World Economic Forum provides is that you have two key contacts within the World Economic Forum, and they really want you to bring the ideas to the table. It wasn't as if they were feeding us specific content but rather suggesting topics of interest based on the views and downloads that they receive. I am still working with these folks today; we were given two cyber experts within the World Economic Forum, and they helped guide the process. One of the things that I found interesting was, we were writing for a truly global audience. So, everything from the use of idioms to assuming that the U.S. was not engaged in things that made the world nervous. There are things that are quite different from the way that we write or express ourselves domestically.

Suzanne: I have done some international work as well, and I know exactly what you are saying. We are not the center of the universe, even though we sometimes think that we are. The World Economic Forum is one of the places that you see that there is a lot going on outside of our own borders that affects us, certainly, but that we don't control. Now, we talked about the fact that there are so many topics, and thankfully it's not 10,000 topics, but there are 273 challenges, is the number that I have got, that are challenges that are transforming economies and industries. That is where you started with the conceptual interconnections. What kind of content did you add to that content that was already there, and do you think you had any effect on how those transformations are being perceived by the users of this kind of map?

Matt: Yes, certainly. So, when you think about it, those challenges are meant as a superset of concerns about the vitality and survival of the global economy. This is really top-level concerns, and that decomposes into finer…One of the areas that I thought was underrepresented, and feel proud of the fact that we were able to convince the World Economic Forum that we need to say more about, is the supply chain, specifically how cyber both underpins the broader supply chain, and then the cyber supply chain itself, if that makes sense. I describe it as the *silver thread of cyber*. Everything that we do economically at some level with very few exceptions, is going to tie back to some exchange of digital information. With that as the backdrop, we would then explore a number of related issues in the supply chain. For instance, how do you develop and maintain justified confidence in your supply-chain partners? How do you determine what a worst-case scenario looks like? How do you determine the resilience you need and then the resilience you have currently? These are things that we are able to bake into our new content.

Suzanne: We are seeing some of that right now in terms of supply-chain disruptions, some of which have to do with COVID-related kinds of disruption. But also, cyber disruptions are things that when…. You don't realize, until it happens often, that this little part way down the supply chain is an integral piece that if it is not there—we just take for granted it is there—but if it's not there, we are not going to be able to achieve the economic benefit that we are looking for, whether it is a Ford Bronco or anything else that we are looking to take advantage of. That is very cool, and I have other friends in CERT that work supply-chain issues, so I'm like, *Yes*.

Matt: It is interesting to have been asked to do this by the World Economic Forum in the middle of what we hope is a once-in-a-century pandemic, and at a time also when I would argue, that there is this convergence of cybercrime and critical infrastructure concerns.

Suzanne: Yes.

Matt: For instance the Colonial Pipeline hack and SolarWinds were occurring as we were developing this content and certainly influenced the way we thought about things.

Suzanne: And probably were helpful in getting people that aren't used to thinking about cyber and cyber resilience, you have got some real-world examples that are affecting not just the U.S. but a lot of equities across the world.

Matt: Yes.

Suzanne: I guess it is making lemonade out of lemons. You don't want to have SolarWinds or the pipeline disaster, but if you are going to have them, at least you got some benefit in terms of maybe preventing something worse in the future by making people aware of some of these issues.

Matt: Yes. Absolutely correct. One of the elements that we needed to address was the human element. If you are viewing the transformation map, you will see that there is also a component where we're looking at workforce development. I think it's important to understand how things fit together. When you're in a highly complex situation with too few people who understand it, it kind of compounds your problems, and cyber, I would argue, is experiencing that right now.

Suzanne: Ah. Say more.

Matt: Well, right, it is generally accepted—and I believe to be true—that there is a shortage of qualified cyber resources globally. There is a war on for talent. All of these things come out in what we wrote for WEF. So how do you ensure that you are focusing your energies on training people on the things that are relevant today and anticipating tomorrow? Doing it at scale? Then another section of the content that we are quite proud of is, we spoke to casting a wider net, how do we ensure that people with diverse backgrounds and from underrepresented groups are part of cyber going forward?

Suzanne: OK. I am not the World Economic Forum. I am a business owner in automotive or in healthcare or in an economic entity, but not at that World-Economic-Forum level. What can I do with a roadmap like this? Is there something that when you take it out of the broad worldwide that I can do as someone local or as a researcher or even as a cybersecurity manager? What are some of the uses of this kind of mapping for other equities in our supply chain for security?

Matt: Sure. Certainly you don't have to be a Fortune 100 company to find benefits. The list of concerns or considerations that we lay out in the transformation map apply universally. Now, the scale is going to be different. That is kind of the point of the format in which we develop this, which is these can't be niche concerns only for the few, but rather we are focusing on broad problems that are universally recognized.

Suzanne: OK.

Matt: It doesn't matter if you are a bank or a hospital or a nonprofit, you are experiencing now, and will likely experience, the things that are described by virtue of participating in this cyber-enabled global economy, which is unavoidable. That sounds a bit dramatic, but that is really the truth, which is there is really no off-the-grid for very long.

Suzanne: Right.

Matt: This is a roadmap to the things *on* the grid that you should be aware of when you're participating *in* the grid.

Suzanne: OK. That is a good advertisement for this. You have got me. I want to learn more about this. What are the kinds of resources besides the map itself that would help me with addressing some of these things?

Matt: Sure. So, the World Economic Forum is a membership organization. There is a portion of the content that requires a subscription, and there is a portion of the content that is free to everyone. The World Economic Forum website has summary reports, really interesting analysis that they have done. There is a catalog of artifacts out there in addition to the transformation maps.

Suzanne: OK, and the World Economic Forum is the source for those.

Matt: Yes.

Suzanne: I imagine we link to those from our blog posts and things like that. We will link to those from the transcript for today's podcast as well. We always like to include external things like that.

Matt: Yes. I would offer this as well, so that will see us mention specific tools, techniques, standards for practice. Well, not surprisingly, we are drawing on things that in some part we've created.

Suzanne: Yes.

Matt: So really the SEI catalog of artifacts is another source.

Suzanne: Good, good, good. So what is next for Matt? You've got kind of…this is arguably a very capstone kind of very high visibility thing. What are some of the other things that are interesting you in terms of problem spaces that you and your team are working to solve that are not necessarily represented in this activity?

Matt: Yes, certainly. There are many to pick from, but I will highlight just a few. We take it as ground truth that certain things in cyber are important. I am thinking of specific controls and specific safeguards. We are working on ways to add some scientific rigor to that. To say, *Well, OK, if this safeguard really is important, how important is it in relation to other things? How do you measure that?* And then that leads to something else that we are very keen to understand, which is the investment decisions that are made in cyber.

Suzanne: OK. So you are looking at value analysis and investment analysis and merging those together for those very foundational safeguards, is the way I would put it.

Matt: Correct. Yes, and I would say that the efficacy of controls is something that is underexplored in cyber.

Suzanne: OK.

Matt: I think as cyber evolves and matures as a discipline or a profession, we are going to see, I hope, the level of analysis in quantification that you see in software engineering applied to cyber. We have done that with things like maturity models we have built. But I think one of the foundational elements we could make better in cyber is measurement, so, heavy focus on measurement in my group.

Suzanne: Yes. One of the things I have observed over the last 10 years in particular, as cyber has become more personal. I will put it that way. The guy that owns the hair salon where I get my purple hair, he talks to me about cyber issues because I work at the SEI. And 20 years ago, I would not be talking to a salon owner about cybersecurity. The more personal and ubiquitous the concern gets, I think there is actually more of a responsibility for us to say, *Yes, we know. We don't just assume that these controls are the right ones, here is the evidence. Here is the real evidence that they are, and it's not just anecdotal anymore. We have a big enough sample that we can actually do more quantified and quantifiable measurement of it.* I think that is a great direction. Because I think there is going to be a point where people are going to rebel and say, *I am tired of dealing with all the cybersecurity. I have got to do 16 things to get into my phone*. We have to have a way of saying, *Well, here is where the science is. Here is where the benefits* *are. These four over here, minimal efficacy unless you are in these settings. These 12—sorry dude, it's 12—if you don't want ransomware, you're going to have to go through this.*

Matt: Exactly right. So, something that I find myself saying in the executive-education space, we need to remind ourselves—and CISOs don't always love this message, especially if they're, like, technologists by background. Everything we do in cybersecurity supports a risk decision. The risk-informed selection of control safeguards, this is really essential. To your point, we have to focus on the critical few. That also leads to the understanding of a return of security investment, which is largely voodoo in many circles right now. We want to make strides there.

I think also understanding that it is the combination of technology, people, and process that is actually important. Again, not to sound too pejorative, but I think moving from this being the domain of the technologist to this being the domain of the risk analyst is going to change for us.

Suzanne: And the human behaviorist. One of the things that I have always admired about the work done in CERT is that there has always been people that have been looking at the human element of this and understanding that it is humans that make the risk decisions and the implementation decisions about what we are or are not going to implement. So understanding the human aspect of this—this is a true socio-technical system—and we can't just let the technologists rule as much as it might be attractive to do so.

Matt: Well, Suzanne, if I may, there is another element to this we should discuss. There are also a number of nascent privacy projects that we are very interested in developing. I am thinking about your description of making this personal. The number one set of questions that we get at the barbershop, or at the grocery store, or from my relatives, are really about privacy. How do we know that our information is not being stolen or misused? So those personal risk calculations, the trustworthiness of the technology, all these things have to fit together. I do think that the ability to gather data and analyze data has outpaced our thinking about the correct ethical uses of the data. I think this is another frontier for us to serve.

Suzanne: Yes. This relates also to our artificial intelligence, machine learning, all of that, the ethics component is coming to the forefront way more than it has in the last 20 years. I think you are going to be busy, is what I think.

Matt: Yes, and in a good way. I think that the work we have done for the World Economic Forum, which is again a whole-of-CMU initiative, I think that we will see more of this, that we are going to draw on those who know the most and have the most to add coming from many elements. Here at the SEI, we are quite proud of the collaboration we have with SSD and with ETC [Emerging Technology Center].

Suzanne: Yes. Well, I have been associated with the SEI since 1993, and we get these opportunities once in a while. They don't come all the time. So it is very exciting when we get something like this that we really can have a worldwide impact. That is when I feel like it goes to our DoD mission, *How do we make our world safer?* One of the ways we make it safer is by making it safer to have an economy that blooms across the world, so that people aren't feeling like they have to compete all the time and competition leads to other things. There is a whole lot that this really serves in terms of our mission. Thank you very much for working through this, because I know that there had to have been some interesting moments as you went through these discussions.

Matt: Absolutely, yes. It was the best kind of busy though. It is certainly of high impact and enduring, and it was a pleasure to do it.

Suzanne: We didn't talk about this before, but how much were you able to do virtually versus how much did you do in person for this activity since we are in a COVID world right now?

Matt: Yes. So that was a really interesting aspect to this, too. Well, I believe all of the revisions of the transformation map happened virtually. So this was unfolding essentially late last winter into early this spring before I was back in the office or anyone else in my team really consistently.

Suzanne: Yes.

Matt: Yes, it was done essentially all virtually, and then we were having calls with people in Geneva. So, it was international and virtual.

Suzanne: Yes. OK. So you didn't get all the extra travel points out of it, but you were able to stay home and stay safe so that is good too.

Matt: Yes. I am hoping at some point we can parlay that into a trip to Geneva. But yes, it was all virtual…

Suzanne: We all want a trip to Geneva, of course we do. Yes. All right, I want to thank you so much for talking with us and our audience today about this work. I am very excited about it and to see where it goes from here. For our audience, we will include links in the transcripts to resources we have talked about during the podcast. Matt, I look forward to plotting with you in the future and thank you so much for joining us today.

Matt: Well, thank you. It was my pleasure.

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.*