Situational Awareness for Cybersecurity: Beyond the Network

Featuring Angela Horneman and Timothy Morrow 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: Good afternoon. My name is Suzanne Miller. I am a principal researcher here at the SEI. Today, I am joined by my colleagues Angela Horneman and Timothy Morrow, who are both in the CERT Division, working in the area of situational awareness for cybersecurity. So, that's what we are going to talk about today, is situational awareness in the context of cybersecurity.

I want to welcome both of you and ask, first of all, what got you into that end of things? I mean, we do a lot of different kinds of work at the SEI. What brought you to working with the situational awareness topic?

Timothy: I'll go first. So, I've been fortunate I've been with the SEI now 17 years. I started out in our acquisition group, thenI moved to our architecture group. By coming over to security, the CERT side of things, it has been a really nice opportunity to kind of pull together a lot of different experiences. I saw from the cybersecurity side, a lot of people have been more ad hoc, reactive mode. So, for me, becoming manager of situational awareness, it's an opportunity to add some structure, bring forth some vision, and try to get more stability into what situational awareness means. That's why I'm excited to be here.

Suzanne: Angela?

Angela: I've been with the SEI now for about seven years. I got into the situational awareness team when there were some open positions. I interviewed, and I had interned here. The manager who chose me was the head of the situational awareness team at the time. I really like it because I really like to help people make sense of their world and understand what's going on and how to make better decisions.

Suzanne: That is one of the ways that I've heard situational awareness described just in general: it's the sense making of what you are seeing. It's not just about, *What are you seeing*, but it's making sense of what you're seeing. Is that, does that hold true when we start applying that to cybersecurity as well?

Angela: Yes, definitely. That is a good one-sentence summary of situational awareness, although it goes so much deeper than that.

Suzanne: Why is that such an important topic in today's security environment? Why is it important that we add some structure to how we think about the things that we are seeing?

Timothy: I think a lot of people are used to network situational awareness and their enterprises, but they don't understand that networking has changed a lot now. We see that most of our customers have moved to the cloud. There are changes in software-defined networks. It's all very fluid. So, it's one thing to understand what type of security you need, but then understanding, *Given that infrastructure, where do I get my data? How do I make my decisions*? That is why our field is very dynamic right now.

Suzanne: So, we've gone beyond, and I, I remember interviewing some folks about network situational awareness. We are kind of going beyond that to look at data, to look at how the world interacts with the networks that we're part of. What else has been added to that idea of network situational awareness?

Angela: I think one of the big areas that has always been missing in the concept of situational awareness for cybersecurity, whether you are talking just about the network or more generally, is, *What is it that you are getting situational awareness about? So, what are the assets that comprise your realm, your territory, as the military would say? What are the business services that you're supporting? What are the policies and legal aspects and governance aspects that people need to know to be able to make sense of what they are seeing?* A lot of that has always been missing. Like you will get bits and pieces to your cybersecurity folks, but very seldom have your security operations teams within an organization gotten the full picture of how everything works together beyond just their security architecture.

Suzanne: One way I could envision that is that I could talk about it as you're really dealing with the entire ecosystem that has to be dealt with, not just the network, not just the boundary of the network to the world. You are looking at the ecosystem that it interacts with and not just what your network interacts with, but your applications, your data, all the things that are important to your business or your operation.

Angela: Right. With that view, you may be able to detect when things go wrong, which is what most people think about cybersecurity as being is stopping attacks or stopping threats. But we are

in a world where there are so many threats, there are so many attacks on a day-to-day basis, especially for large organizations but even for small organizations. Without that greater context, you can't effectively respond to the threats that are most detrimental to your organization or could have the most impacts.

Suzanne: So, today, it's more a matter of prioritizing, *What are the threats that I feel like I have to respond to*? and that is very context dependent. If I'm a first responder in an emergency situation, threats to my network, denial of service, or things like that, take a very different context than if I'm a big retailer who is dealing with more of a financial aspect if I get denial of service. That is going to be one of the big things that I think our readers and our listeners are kind of interested in is, *How do I do that prioritization*?

Timothy: Right, or even just getting a vision. I think that is the part where we are trying to bring more architecture, system of systems view into things.

Suzanne: I was wondering if you were going to bring system ofsystems into it. You and I go back a long way on that topic.

Timothy: It's all about the vision, and I think understanding what the world is, it's what we talk about among our team. We are no longer just analysts who are looking at things. You have to pull yourself up. You are more of a systems person. You have to understand the trade-offs, the world that you're living in. We are stressing a lot more that you need to have a roadmap, where I want to get to, what are my business drivers. I need to have multiple views from an architecture point of view of what's deployed where, how am I controlling that with my access, who are my developers, where are they stationed, how do they get their access through the system? So, there are multiple views. It's broadening the horizon for our team to be able to start bringing some of that in and having that understanding because that is where we make our impact with our customers in getting them to see that vision. That is where they need to get to.

Suzanne: I'm going to refer back to our mutual architecture background, because what I'm hearing you say is something that we used to say about software architecture years ago is that we need multiple views of the software architecture, not just one. What I am hearing you say is you are applying that same construct to this idea of situational awareness that we need. There is the viewpoint, the legal viewpoint. There is the data viewpoint. There is the human viewpoint in terms of insider threats. There are all kinds of viewpoints that we need to add into this to make it a robust vision, a robust picture of what our situation actually is. Is that…

Angela: Yes, in some ways I like to think about it sort of like as layers. You have your devices and all your infrastructure and how those are all connected, and that is one layer of your system. On top of that, you have a security overlay: all the devices that are put into practice for

protection or monitoring and where those are located, that is another layer. Then on top of that, you have the processes and the analyses that your security operations folks do as another layer.

Suzanne: Then you have got governance on top of that.

Angela: Then you have governance on top of that, or maybe governance is really the first layer down at the bottom.

Suzanne: Probably both.

Angela: Probably a little bit of both. Yes.

Timothy: But I think that is where our customers run into the biggest problem. So, they understand the frameworks, they understand the different layers, but we are saying you need things that cut across all those things. That is where we talk about a mission thread or a work flow to get that type of vision. If you don't understand, *What are your basic missions and how do you accomplish that?* then how can you ever have a sense of, *I'm safe or not*, right? That is more of what we're trying to convey to people, *Get that story straight. Then, you will be able to dig down deeper into your system to see where the right data is, and then what do I need to do with that.*

Suzanne: What are some of the things that you are seeing are being most helpful to programs that you are working with directly in terms of giving them that multi-layer, that multi-dimensional viewpoint? What are some of the techniques that people should look for if they are trying to apply situational awareness concepts?

Angela: One of the simplest things that we have seen people do and has not been done surprisingly in the past very well is better catalogs, I guess, of their assets. So, better asset management, inventories, understanding what you have. But not only what you have, but how it's expected to be used, and how they are interconnected. So, going back to the architecture piece, it doesn't do a whole lot of good just to know that you have a whole bunch of servers here and a whole bunch of desktops here. You have to know for each of those, what is their actual purpose? Why do they exist? What is the business service or driver that requires it to be in existence? Then also, how are they connected?

Suzanne: Taking this back into something—I haven't talked to you guys about this yet—but this is sounding to me a little bit like connecting your system view to your value network and to your value stream. So, understanding, *What are the things that are important to get value from, the business or the operation*, and then looking at how they are connected to the different elements of the system and the different security layers and other things. So, OK, I'm going to come help you with value stream mapping.

Timothy: One thing we are looking into doing is more in the model-based system engineering, actually using some tools. Because a lot of times, all this information is disjointed. You have so many different documents, so many places. We have been using some tools and finding it very helpful to get that vision down and then start to use that to decompose your system. So, I can get down to that data level and be able to see, but I have just one source for all my information. And so that's where we're going to…

Suzanne: The ground truth kind of idea.

Timothy: Absolutely. You can share that with everybody. That is the biggest part about what we are trying to do is you need to convince people they understand what it is they're dealing with, right? *What is that vision*? *I can show you that, and here's how we do that*. It's through views. It's through understanding your data. It's those types of things. But using a tool like that is something that we are going to be doing a lot more of to get that message across.

Suzanne: That technology has come a long way, SysML [Systems Modeling Language] and AADL [Architecture Analysis and Design Language]. We have got lots of different things going on in model-based engineering here at the SEI. But also, the whole world in that it has come a long way to where I can see it being feasible to get those kinds of multiple viewpoints in a model that maybe 10 years ago would have been a little bit tougher to do.

Timothy: Right. It's not like everyone used to be where we dealt with people doing the Department of Defense Architecture Framework (DoDAF) thing. And they would do one diagram of each view for their program. And it's like, *No.* Then it was in Visio or it was in PowerPoint, and it's not active.

Suzanne: PowerPoint engineering.

Timothy: The tool changes that. You can have different views for different needs, and that's OK. I think that's a big part of what we tell people. You have to see what works for you.

Suzanne: Well, back to context is everything, right? The context in the military versus the context in the financials is going to be a little different.

Angela: Beyond the architecture views and using the tooling to actually create a more comprehensive picture that is all in one location, we are also seeing people needing to develop what is commonly referred to as a common operating picture or a map of the terrain, depending on what your background is. Historically, people, even organizations that have a lot of cybersecurity data, will have them in different spare locations. They may have this information over here, that information over here. They may integrate a lot of it into a security management solution like Splunk or ArcSight or whatever, but they still tend to have pieces everywhere.

Organizations are coming to the realization that that is a huge gap for them. It causes them to have major inefficiencies in anything they are trying to accomplish. So, trying to figure out ways to bring that information together in some understandable method is one of the next iterations of how we are improving this situational awareness world.

Suzanne: How is the SEI working on that? What is it that we are doing in that space?

Angela: There's a few different efforts. From a very tool-based effort, there is some work going on in our security automations group to develop some tooling to allow different types of information to be put into maybe a data lake or something like an elastic stack, where various types of information can all be in the same location and accessed through some sort of API [application programming interface] or programming language altogether. From our team's perspective, one of the things that we are doing is trying to help organizations identify what data makes sense to bring together. You don't necessarily need all the data that is available. But based on your priorities or your mission, what information actually would be needed to be brought together for that common operating picture?

Suzanne: So, in Agile we talk about a minimum viable product. You are really talking about the minimum viable data inventory that is needed to create the picture, the common operating picture. That is going to change depending on what setting you are in. So, this is not a one size fits all…

Angela: It is not a one size fits all.

Suzanne: …kind of a thing. Everybody is looking for a silver bullet. So, I always want to make sure that we don't let them go there.

We do like to emphasize transition in our podcast series, the kinds of things you are talking about, the security automation tools and the techniques. How is it that people that are interested in improving their own organization's situational awareness in this area, how can they get to the materials that you have available and that you have made available for use in different settings?

Timothy: For myself, I always like to go back to the architecture papers [*An Introduction to Mission Thread Workshop*, *Documenting Software Architectures*, and *Quality Attribute Workshop*] that we have done at the SEI. It is a very good starting point to get an understanding of where you need to see your system going. Understanding those drivers, understanding your missions are very key to get that articulated. A lot of times our customers come and they will ask us what product we should buy? We had one vendor in the other week, was *I always buy the products that's in the Gartner reports, it's in the upper right-hand corner. In fact, I'd buy two of them. So, is that good or is that bad*?

I think these are questions that are things that a situation awareness team needs to o be able to answer something like that> I need to convey an idea of what is that security, like you say, and minimum viable product for Agile. What is the minimum viable security for somebody's system? We need to provide that. That is the type of thing that's showing people cross walking those different frameworks and standards to say, *This is what this means to you. Don't just buy this product. But if you do, you should have other products like this*. That's what we need to be starting to transition to our customers. We are starting to do that. So, there's not a lot out there, and I think that is a gap that we are trying to fill for our customers.

Suzanne: A lot of what we do here is gap filling.

Angela: Another thing that we're trying to do is…as I said, I've been here for seven years. The team has existed way longer than that, but I don't think a lot of organizations fully understand what they need for situational awareness. So, we have been trying to document in a more understandable method something that is more easy to comprehend, What does it mean to have situational awareness? You have lots of models out there. You have one by Endsley that goes: you perceive, [you] comprehend, [you] project, [you] decide, and [you] act. That makes sense from a cognitive psychology perspective. Those are your thought processes that you need to have situational awareness. You have the OODA loop, observe–orient–decide–act, very similar. But from a cyber realm, what does that actually mean? We have been working on some documentation, including a blog series, to actually lay out from more of a layman's term, *What does it mean to have situational awareness in your organization?*

Suzanne: *What does orient mean when I am talking about cybersecurity?*

Angela: *What does orient mean? What does it mean to perceive when I sit down at a computer? What am I perceiving? What is the scope of that?* I personally like to think about it more along the lines of, *I need to know what should be. I need to figure out what actually is. Find where those two don't match, and then do something about the differences.*

Suzanne: And prioritize.

Angela: *Prioritize my actions and do something about it.*

Suzanne: Yes, don't forget the act part.

Angela: Exactly, don't forget the act part. Sometimes people may think that *act* is actually you go do something about it. Sometimes you do. Sometimes it could just be you need to communicate information to people. But one of the things that I also like to remind people is situational awareness for cybersecurity, you are not only concerned about the actual attacks. You are concerned about any of those differences that occur in your thing because those impact, those

impact your security either directly or indirectly. Because if you have those differences, even if they are not a cybersecurity issue, if they continue to exist, they are wasting your analyst's time because they continue to show up. Plus, they often let in vulnerabilities, cause vulnerabilities, increase your risk. So, don't only focus only on the actual threats and the obvious when you are…

Suzanne: Well, and this is one of the, I imagine like the common vulnerability list and things like that that are constantly being updated. One of the challenges for analysts is to keep up with what are the latest vulnerabilities and the latest methods of attacking. Something that is a gap in your position between *should be* and *is*, it wasn't a problem last week, but this week it is. So that constant updating is one of the challenges that people out in this field have to deal with. I applaud all of you that work in that arena because I don't know that I would be able to do that today.

What are some of the big failure modes? We have the privilege of working with a lot of different customers. One of the things that our listeners are often interested in is what are some of the big failure modes that we have seen that they may not have seen yet? You have mentioned one of them: just not paying attention to all the different aspects of *should be* versus *is*. What are some of the other big failure modes that you see in your work with organizations?

Timothy: I think Splunk is one. It's the easy one we keep hearing where everybody collects a lot of data and is like, *Well, what do I do with that data*? So, they have a Splunk. It is basically what it is. They have teams of people, we know customers that spend a lot of money, but they just don't know, *What the heck am I supposed to do with this*? *How do I analyze this? What am I doing*? That is a real concern.

Suzanne: *How do I go from day-to-day information?*

Timothy: Yes, *How do I make it useful?* I don't need to collect everything, but if I prioritize what is important to me from my assets, look at that data, and then figure out what you need to do from there. That is one that is an easy one. Do you have another one?

Angela: Another one that is pretty easy is the mismatched priorities. If you are not providing your SOC [Security Operations Center] analyst with what they need, they are not going to prioritize in the best interest of your organization. They are going to prioritize either what is top of the line for them, what is easiest for them, what they personally care about the most.

Suzanne: What they just heard about in the latest vulnerability report.

Angela: What they have access to. So, that is a big failure mode, is organizations who aren't adequately communicating out the information that their analysts need to know to be able to prioritize what they are doing.

Timothy: Another thing playing off that is risk identification. I think that is a big part of what we think situational awareness is. It is to make that aware to the organization going up the chain. A lot of times, the SOC people or lower-level people don't appreciate how to articulate that message and get it out there. *Everybody has different processes for risk management,* things like that. But I think clearly identifying the risk and the impacts to your business drivers, your systems in a way that the CISOs and all these other people and leaders can get a sense of where they think, *That's where we have to help them fix this.* That's the problem we are seeing a lot. It's all red, red, my risks. You need to get away from that. It needs to make some sense of, *What is reality here?*

Suzanne: One of the things we run into in consulting with organizations on Agile is this idea of rank ordering your priorities. It's not *red, yellow, green*. It's, *What's number one? What's number two? and I'm sorry, you can't have two number ones*. I think you are running into some of the same issues that humans…. That clear definition of *What is a one?* and *What is a two?* means I have to take action differently than if they are both ones and I can choose. And that human aspect I think plays into this like it does in some of the other areas that we work.

Timothy: Yes, getting people to make a decision because it's so hard to get them to say, *Well, this really is my number one*. But I think that's part of what we do at the SEI, because we're trusted advisors, so we're the ones who

come in a lot of times and say, *Okay, I think this should be your rack and stack order for you*. So, it is what we tried out.

Suzanne: That is part of how we gauge what the effect is. If our rack and stacking is something that appears multiple times and works all the time, then we actually may have something we can codify and transition in a more widespread way. So, we have done that definitely in architecture and some other areas that we have worked in before.

I want to thank both of you for joining us today. For those that are not familiar with your work, we do have insights.sei.cmu.edu is where your blog posts will be. There is a whole series of those. This podcast is also one of several, so they can go out and look wherever you get your SEI podcasts. Hopefully, the YouTube channel is one of them. That will be available to people as well. So, thank you to our listeners for joining us in this very interesting conversation.

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.