Cyber Intelligence: Best Practices and Biggest Challenges

featuring Jared Ettinger 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 SEI. Today, I am here with my colleague, Jared Ettinger. We're going to talk about a recent report that the SEI did that he co-authored on cyber intelligence, how it's different from cybersecurity and other things like that. Before we actually get into that, how did you end up doing this kind of work? What made you decide that cyber intelligence was a field you wanted to be part of?

Jared Ettinger: My passions are in intelligence and counterintelligence, whether it's inside or outside of the cyber domain. My background has been doing intel and counterintelligence analysis and operations. Before I came to CMU in 2015, that is what I was doing. Towards the end of my tenure supporting a number of three-letter agencies, I started to get into the cyber domain and learned a little bit, just the fundamentals and the basics. I was doing that self-study on the side. Then my work took me in that direction toward the end of my time when I was living in the D.C. area. Then I lucked out in 2015, and came up here to CMU, the Software Engineering Institute, where I've continued that line of work. At the SEI, I work in a group called the Emerging Technology Center.

At the Emerging Technology Center, we have three general broad areas of focus: they are advanced computing, applied AI/machine learning, and then the last one is called human and machine interaction. We do research in those three areas to support a number of different mission areas. Cyber intelligence is one of those mission areas. Since I have been here, my work has predominantly been in that mission space. I also teach a class here at CMU. It's a graduate-level course out of the College of Engineering Information Networking Institute called the Introduction to Cyber Intelligence.

Suzanne: You have both the operational and the technology sides, which is important to note when we're talking about intelligence. Intelligence, cyber intelligence, cybersecurity are not the same, in many ways the same way that intelligence work and security work are not the same.

Why don't you talk about that a little bit because I think that is one of the things that comes out in your report is that those are not the same thing. Help our readers and viewers to understand why they are not exactly the same.

Jared: Sure, I mean that is a great question. Absolutely. Here's the thing. Words mean different things to different people, right? We all have our own unique background and experiences and that gives us our different perspectives. In life that's something we celebrate in people, right? When it comes to also solving complex problems and towards an important mission, it can be challenging when words mean different things to different people.

What we found is when we did our research—and I'll talk a little bit more about how we did our research—we asked organizations how do you define key words in this line of work. So, *How do you define cyber intelligence? How do you define cybersecurity, cyber threat intelligence, strategic operational intelligence, etc.?* What we found is exactly that. There were a ton of different definitions for those words, and they were kind of all over the place.

What we had to do is we had to categorize them and put them together. We got a ton of definitions. We did some affinity clustering. We did some grouping. We also pulled definitions from publicly available information to help us come up with these terms. What we are hoping is that our common lexicon of terms that we put into the report is something that people can use as, *When I say cybersecurity, you know what I'm talking about*. When we have a common lexicon, it does two things. One, it enhances information sharing. The second is it builds on trust. When you are talking the same language, you can share information, you can collaborate, and then you can build trust.

To get back to your initial question, what is the difference between cybersecurity and cyber intelligence, think of it this way: If you break the words apart, cybersecurity, it's basically the discipline of security in the cyber domain. What does that really mean? It means securing your information and computer systems. You want to protect the confidentiality, the integrity, and availability of your data and computer systems. We came up—based on the definitions that we got from our interviews, and again, I said some publicly available information we pulled from DHS—with the following definition. I probably am not going to be able to cite it verbatim from our report, but it's something to the effect...

Suzanne: That would be very impressive if you did.

Jared: I'll try. It is something to the effect of,

Security measures or actions to ensure a state of inviolability to the confidentiality, integrity, and availability of your data and computer systems from hostile actors or threats.

We also heard the term *cyber hygiene* being used.

Suzanne: That's a new one.

Jared: Cyber hygiene sometimes was referred to as, *cybersecurity or actions to improve one's organizational cybersecurity*. An example or things that you would do for cyber hygiene might be patching your systems, vulnerability management, configuration management, scanning, and assuring that your network, your hardware and software configurations, and your inventory are up to date. Now all of that is different than cyber intelligence.

If you were to ask, or if an organization were to ask, *What are the major threat actors targeting my organization? How are they going to attack my organization? Why are they going to attack my organization? What are the supply-chain risks to my organization? What are the emerging technologies that are out there that can help improve my organizational performance, yet can be leveraged by attackers as well? What are the geopolitical threats or foreign-policy threats that my organization might need to deal with should I want to move outside of the United States or put our organization, or put an office building, in a foreign country?*

Those are the type of things that cyber intelligence can answer. Now let's break that word down. You have the discipline of intelligence in the cyber domain. And intelligence is different than security. When we think about intelligence, again, we got definitions from our interviews and basically from publicly available information, from key documents, and from ODNI, DoD, CIA, etc. We proposed the following definition in our report. Again—I don't know if I'll do justice by citing it verbatim—but it's something to the effect of,

Acquiring, protecting, analyzing, and then disseminating information that identifies, tracks, and predicts the threats, risks, and opportunities to your organization for the purpose of enhancing decision making for decision makers.

Suzanne: That is a little bit broader because what you didn't say in there is, *enhancing decision making about security*. It's not just about the security aspect. That was one of the things I picked up in reading it that the cyber intelligence is intelligence in the cyber space. So it really is broader than just looking at intelligence to protect my computer systems and data.

Jared: Right. It's not just about that. It is intelligence in the cyber domain. That is why it's cyber intelligence, but it's beyond security. Decision makers would use it to largely protect their vital interests and vital interest basically comes down to their financial reputation, their brand, their stature, and their reputation, etc. That is how organizations would use cyber intelligence. Now in addition, your lower level to mid-level, your mid-senior-level decision makers, your CISO, your CIO, would use it to protect their data.

Suzanne: Right. That's part of the vital interest that they're responsible for.

Jared: Exactly.

Suzanne: This report, you've already talked about the fact that you use interviews. What is the breadth of participants that were involved in this? Because a lot of times when you see studies like this, you say, *Oh, they only talked to these people*. What really represents the breadth of the report, things you were reporting on?

Jared: Great question. First, I would just tell you that the study that we put out a few weeks ago, I think it was May 22 it went out, that is our second study. It's an update to a 2013 study. In the 2013 study, I think we interviewed almost 30 organizations across government, industry, and academia. When we went back to our sponsor, who was the ODNI for the 2013 and the current one, we said, *Hey, a lot happens in cyber. Things change quickly every day. A lot changes in five years. Would you be interested in doing this again.* They said yes. With that in mind, we kicked off the study, I think, in August of 2017. We had our game plan. We reached out to a number of organizations and participants. What we ended up doing was interviewing 32 organizations. We tried to get a nice representation across DHS critical infrastructures. I think we were able to do that. So we were able to focus on, again, government, industry, and academia.

We targeted as many critical infrastructures as we could. We got the defense industrial base, finance, government, IT, communications, let's see, who else? Retail. I'm probably missing some. Food and agriculture, energy, we hit energy to get a wide range of organizations. We got 32 organizations. We interviewed them in 2018. I'll tell you what we did is we used our 2013 information as a starting point. Those were the best practices then. *What has changed, right? What is the state of practice now? What had changed, etc.?*

We used that information, and then we went and we interviewed these organizations to do two things. One, we wanted to make sure, *What was the best practice then? Is it still a best practice now? What has changed?* We needed to update our criteria. Then, as we went around and interviewed organizations, the other thing we had to do was make sure we were asking the right questions. We had to come up with questions. We had to ask the questions. Each time we did our interviews, specifically in kind of in chunks, right, in blocks. We would go out and do a set of interviews and say, *OK, are we asking the right questions*? Then we would update and iterate etc., until we felt were at a point where *OK, we know we're starting to get the right information*. So we did that.

In doing that, we also came up with assessment factors. We had 33 assessment factors for how we would softly assess organizations across a cyber-intelligence framework. That framework is largely discussed in the 2013 report. We brought it over with a little modification to the 2019 report that came out. We gathered all this information from organizations in terms of conversational questions. Kind of like you're asking me, these kind of conversational questions; we would do the same things within organizations we talked with. We would talk to their cyber-intelligence teams, sometimes their CIOs, sometimes their CISO, high-level leadership. These types of conversational questions are where we found that we could really get some awesome, amazing, golden nuggets of data and hear really, truthfully, and honestly, what's working and what's not working.

Then we were able to gather that data and assemble a ton of best practices and common challenges. Those best practices and common challenges—we had themes—are what drive the content of this report. Really quick, I want to mention some other things. First, is that this is a qualitative study. By no means is this a quantitative, statistical, advanced statistical research study by any means. It is not. It is a qualitative study where it was based on our 2013 interview data, leveraging that, and then getting our new research data from our interviews. Then, a little bit sprinkled in there, is some SEI expertise as well.

The other thing that I want to mention is that it is a snapshot in time. Things change quickly, so that information that people are reading now is from the 2018 timeframe. We stopped our last interview in November of 2018. Then, from there we went to like hardcore, roll-up-the-sleeves analysis and start writing. It is a snapshot in time.

The other thing I would say is it is a long report. It is designed to be like that on purpose. First, we wanted to make sure that there was something in it for everyone. What I mean by that is that there are going to be people that read this report that are very technical: your malware forensics analysts, your incident response, your PEN testers, exploitation folks, your network analysts that will probably find some value in this report specifically in the threat-analysis and data-gathering phases. They might not find as much value as a CISO would when reading the reporting and feedback and strategic-analyst analysis section. So we tried to make this as broad and as comprehensive as possible.

It is also long because it's very detailed and thorough. One of the distinctions from the 2013 report is this, is that in the 2013 report we had our cyber-intelligence framework. It is called environmental context, which means you understand your environment. Then, once you do that you collect data. Then you do analysis, and then you report that up to decision makers. That is the framework, and then what we did in 2013 was you got a list of best practices and common challenges, and we generalized them across those components that I just mentioned. This report is a lot more in depth because what we did is those 33 assessment factors that I mentioned—instead of just saying best practices and common challenges across those components—we did best practices and biggest challenges across all 33 assessment factors that are sprinkled within those components. That is why it is as detailed and thorough and long as it is.

The other thing I would say is that we wanted it to be as detailed and as thorough as possible because we are at the point in talking about cyber intelligence, where we are past talking about generalizations. We need to move past, like we need to share information better. We need to gather data. We need to protect our systems. We need to get past that and really start talking about details, so you can take actionable steps. This report has actionable steps that organizations can take to move beyond wherever state they are in to start going towards the path of high performing. That is what this report does.

Additionally, this report has three implementation guides, which people can find when they go online. Implementation guides are a little bit different than a study. There is a continuity path between them. They all relate back to the study, but their difference is that they're step-by-step procedures organizations can take across three areas. The first one is AI and cyber intelligence, specifically machine learning, how to adopt or apply machine-learning practices for your organization or at least the questions to ask for how to get there. The second one is IoT and cyber intelligence. And not IoT just an understanding like, *Hey, we have a huge attack surface with all these different devices that are now talking to us*, but more how can you leverage that information...

Suzanne: How can you use IoT to your advantage?

Jared: …to your advantage to then inform your intelligence picture. The last one is cyber-threat frameworks where we got a number of public cyber-threat frameworks and compared them in terms of how organizations can use them based on the situation that they are in and the threat that they're looking at. We looked at the MITRE ATT&CK, the ODNI CTF, the Diamond Model, and Lockheed Martin Kill Chain. I think there is another one in there I can't remember off the top of my head. Again, they are step-by-step guides for what organizations can do to help them get to high performing.

Suzanne: The way I would frame the report, the report itself is really a toolkit.

Jared: That is a good word for it.

Suzanne: It's got things for, it's got implementation ideas for different situations, and it's got things for different roles in the organization. Viewers should not be daunted by its size, it's really, *Look for the pieces of it that are going to be most relevant to your role and your situation*.

Jared: Yes, absolutely. One of the things that we are working on right now is a top 10 list that will come out that organizations can pull: just look at this top 10 list. Then, if that intrigues them, they can go to the section in the report as well. This toolkit is your one-stop shop. It's a comprehensive guide to how to do cyber intelligence to understand what the best practices are, the common challenges, and the current state of the practice is today.

Suzanne: One of the things I'm always interested in is how things change over time in fast-moving technology areas like this. Are there any practices that were identified as best practice in the 2013 timeframe that not only are no longer best practice, but you would actually say, *Oh, no, no, no please don't do that. That used to be something we recommended, but now we know that that's going to harm you in this way*? Is there anything like that?

Jared: Not off the top of my head. I think in 2013 cyber intelligence was a buzzword. You could make the case that it kind of still is, but back then it was really, really new. There's nothing that really comes in my head that says, *Don't do this anymore*. We were moving in the right direction then. Some of the same lessons that we talk about in our 2018 report, some of the best practices that we say, you can see the path, the linear path of how the...

Suzanne: You can see the source of it.

Jared: Yes, you can see that we were getting there from 2013. For example, like workflows and having defined and repeatable workflows for how to do cyber intelligence and threat prioritization, things like that. Even back in 2013, you saw high-performing organizations were starting a script and starting to learn how to automate some of the tasks to help them do analysis and gather the data. That has certainly continued and increased. We saw a number of high-performing organizations doing amazing things when it comes to automating manual tasks. They were even adopting…there's technology out there that even adopts, helps the organizations do this thing called SOAR technology which can help from...

Suzanne: Would you expand that for our viewers?

Jared: Let me see if I can. Security Orchestration and Automated Response off the top of my head. If you're struggling with resources and manpower, SOAR tools are a good way to help you automate some tasks that you might not have thought of.

Suzanne: Different aspect of the SOAR, same idea. Are there things in the 2019 report that weren't even really thought about, that really have no source in the 2013 report that are new things that have come in since you wrote the 2013 report? Did you go, *Ooh, we didn't catch that, and now this is a really important thing?*

Jared: Yes, we really talk a lot about fusion centers in the 2019 report. To some extent that was going on in 2013, because of the challenge of silos was prevalent in 2013. Unfortunately, I would make the case that based on our interviews, it still exists today. We met organizations that are really having a challenging time locating their data, finding, understanding their entire attack surface, getting access to that data. For a number of reasons, whether it's different technology stacks, cultural differences, or they have an office overseas or they are having challenges getting that data back. So fusion centers for a number of organizations, especially large organizations, have this capability where they bring different people in from different parts of the organization, where they are able to create teams where people are working together and analyzing disparate information from across the organization to form that cyber-intelligence picture. Now, we talk a lot about fusion centers, but I would also tell you these things take time to develop and mature, get buy in, like years and years. We provide in the report a way for organizations to think about what you might want to do to get to a fusion center and the teams that you might want to consider to build a fusion center. They are not hard-and-fast rules, they are just something to think about.

Suzanne: Some heuristics.

Jared: Yes. The question again, I am trying to remember.

Suzanne: Things that really didn't have a source in 2013 that became important in the 2019 report.

Jared: Machine learning. We started to see....

Suzanne: We weren't really talking about that.

Jared: We weren't talking about that. That's why we developed a whole implementation guide on that. Organizations, at least the organizations that have the resources to do it, are starting to build in their homegrown machine-learning capabilities that helps them digest all the information, helps them with analysis, finding anomalies, and detecting patterns that humans might not have been able to do. We definitely heard about that, and organizations talked to us about that.

Some of the other things that we heard—and I would often say this is a continuation of the 2013 report—back in 2013, it was the best practice to link a strategic analyst with your technical folks. That was considered a best practice, and that still is today. What we are also seeing is high-performing organizations that have the resources bring in data scientists and machine-learning experts into a fusion center to help them with processing their data, along with the software development teams to help them build their own tools, etc. In terms of people, one of the things we heard that we talk about in our report in our organizations is that you can teach the technical. I would back up and say that it's always good to find the person that has at least some technical experience, that understands networking, that understands cybersecurity and what worms are, and viruses, and how malware works, and things like that. But we heard time and time again that they can teach people the technical skills to use tools and how to quickly manipulate them to get information quickly for the decision maker.

What we also heard is that some other skills are really, really important. It specifically was critical thinking, the ability to problem solve and think out of the box, and ask questions like, *Do we still need to be doing things this way*? *What if we changed our paradigm or thinking about something*? The other thing I would say is that organizations are starting to turn to NIST NICE 800-181, that's a document on America's Cybersecurity Workforce to map position requisitions KSAs (knowledge, skills, and abilities), for what they're looking for in people. Communication skills, we heard that countless times, being able to communicate to different levels of leadership at different altitudes, and be able to take technical information and communicate that in risk-based terms to decision makers. We also even heard things like emotional intelligence and self-awareness as important skills for people in this field.

Suzanne: So viewers that are looking for a new career, if you have got critical thinking skills and you are amenable to the technology, think about cyber intelligence.

Jared: Think about cyber intelligence.

Suzanne: I'm not going to ask you to name an organization, but when you look across the economic sectors that you were looking at, is there any economic sector that sort of stands out as really kind of leaning forward and going after this kind of cyber intel? I'm going to say leave the defense industry out of it.

Jared: Leave the defense industry out...

Suzanne: ...Because it's kind of not fair. They have to be doing that, but outside of that, are there any economic areas that, again, if you want to go into this as your future job, where should you be looking?

Jared: This is Jared's opinion based on the information that we collected during our interviews. If this is the question that you are asking in terms of like what sectors are doing the best in terms of cyber? Again, Jared's opinion, definitely the finance sector, the IT sector, the communication sector, the energy sector, and I would say the defense sector. They have the resources, at least from the organizations we interviewed. We only hit 32, so there could be things that we are missing that we don't know about, but that's just based on the information that we have.

Suzanne: That is all you can base it on. That's not really that surprising. It is also heartening in my view that, you know, those are all elements of critical infrastructure. One I would hope actually gets better at this, maybe it's not mentioned, there is healthcare.

Jared: Healthcare.

Suzanne: I understand...

Jared: I agree with you.

Suzanne: There are a lot of challenges in that field.

Jared: Even retail I think is doing some great, amazing things with that sector as well so, I forgot to mention that.

Suzanne: Almost anywhere you want to go to work, this is something that's up and coming.

Jared: Yes. If you're passionate about the field, if you want to learn, then go help make a difference.

Suzanne: We have talked a lot, around a lot of different aspects of this. What would be, if I'm an organization that is wanting to stand up cyber intel—I may have cybersecurity already nailed, but I really don't feel like I have my cyber intel team really kind of doing the best things—what are the three things that you would say...?

Jared: Three things.

Suzanne: If you can just do these three things, nothing will solve everything, but you'll get improvements in your ability to execute a cyber-intel mission.

Jared: I would first make the comment that every organization is different. They have their own unique circumstances, and experiencing their own environment. It's all dependent on the type of organization you are and the situation that you are in. Going off of the model that you just described with the assumption that they have a cybersecurity basic foundation of your network-host monitoring, your vulnerability team, considered response, etc., what I would do first is something called...I would do two things. I would do a crown-jewel exercise, and I would get leadership buy-in.

First in terms of leadership buy-in. By that I mean what you want to do is start it by going and meeting with your leadership and saying, *Hey, what keeps you up at night*? I'm not just talking about the CEO, or the president, or vice president. I'm talking about them and across your organization-wide. Go meet with these people and say, *What keeps you up at night? What are you scared about? What are you worried about?* Or, *What do you want to know?*

Figure out what all those questions are because those become your highest-level intelligence requirements for your organization. Find out what those are. At the same time do a crown-jewel exercise. A crown-jewel exercise is basically the idea of going around your organization and figuring out what are your most prized assets that need to be protected, from data, to pending technologies, to new tools, to whatever it is. Figure out what...

Suzanne: Could be patents.

Jared: It could be patents, yes. Figure out what it is, who has access to that, how were they accessed, where are they accessed, when are they accessed. Get to know those people and figure out what are they worried about as well. Now you have two things. You know what needs to be protected, and you know the questions that seniors are asking. What you don't have are the answers to those questions. So, to get the answers to those questions, I would say to leadership, *Look, you have these questions. We know what needs to be protected. Right now we are in a reactive state. If you want to be proactive, if you want to be anticipatory so that we can take the right defensive measures to better protect our most prized assets, then we would need cyber intelligence. Additionally, if you want to make better informed decisions about how to go about advancing our vital interests, our brand, our reputation, and ensuring that our financial health is strong and growing, then cyber intelligence is something we need. We can't answer your questions yet. To answer your questions, we need data and we need the infrastructure to be able to take the data in. We need the right data. We need to be able to validate that data, and we need analysts to understand, and machines to make sense of that data.*

That is your business case right there. Once you have that, then you can start doing the analysis. I would recommend, once the data is coming in, you want to start hiring some very technical people to do some real technical telemetry analysis on what is happening on your network and understanding IOCs and malware campaigns that are happening outside of your network and tracking threat actors and campaigns, etc. Then you would start to build out collection-management teams and having a whole collection-management team to understand your intelligence requirements and doing sub requirements, which we call PIRs. Then it gets even more. I can keep talking. Like specific intelligence requirements.

Suzanne: Eyes rolling in the head [laughter]…

Jared: You have a collection-management team that will manage this whole collection process and to be able to validate the data. You don't just want to validate the data, you want to validate the data sources. You have a collection-management team that is part of your intelligence team that helps understand what these requirements are because they're constantly changing. As the world changes, your critical assets are changing, the environment is changing, your leadership has different requirements, etc. That's a continuous process.

Then as you grow in maturity, you would probably start to say, *OK, I need people to help to do really strategic analysis, like I want deep dives on these threat actors. I want to really understand how I can better protect my organization. I want to understand if we move to a different, a foreign location, what that means for us. I want to understand what quantum and 5G is going to do to my organization. I want to understand what this merger would mean for me or my partners, so mergers and acquisitions, supply chain*. That is when you really start having a strategic capability. The last thing I would say is I talked about leadership buy-in in the beginning. Leadership needs to remain committed. You can't just get them to buy in the fund and then walk away. Leadership...

Suzanne: You need engagement.

Jared: You need engagement. That is one of the things we heard in our report is constant engagement by high-performing teams empowered the cyber-intelligence team. High-performing organizations have cyber-intelligence leaders at the highest levels that are using the information from the cyber-intelligence team to actually advance their decision making. These leaders have questions. They get briefings. They update their requirements. They demand the information, and not only that, they champion the team's work across the organization. They provide feedback, and there are mechanisms to provide feedback, whether that's meeting, daily calls, a wiki portal, etc. So leadership engagement is something that high-performing organizations have, but a number of organizations we met are hoping that there would be more of.

Suzanne: Everyone that is trying to get a change is looking for that kind of leadership engagement. This is one of the ones that I think it may be easier to make that case because if you do the kinds of initial steps that you talked about, *Hey, this is how I answer your questions. They're not my questions. These are your questions. If you want them answered, we have to work together on this.*

Jared: Yes, or *Have you thought about this because we're seeing another type of threat, and we need to start collecting the data to answer this new requirement.*

Suzanne: I think this is a great resource for people who are either in this space, approaching this space, or trying to justify the need to be in this space. This is a big report, as you said. This is a finish-up of a lot of work. What do you see doing in the future, either related to this or other areas since this is the Emerging Technology Center? There has got to be some things emerging. What are you interested in doing next?

Jared: First I'll tell you, I mean, this report was a true labor of love for me. I mean it was the best. I really enjoyed doing this. I want to thank the organizations that participated in it because without them, we would have no report. We met amazing and interesting people doing awesome work, really, really awesome work, so thanks to them.

In terms of what's next for me, I would tell you that I'm going to do work in my passion, what I'm passionate about, and that is intelligence and counterintelligence, emerging technology, and whatever projects I can work on that has that intersection of those three things, then that's what I'm going to work on.

Suzanne: Maybe some potential customers are out there looking for exactly that because we do have customers in all kinds of spaces that need…I can think of some right off the top of my head that probably don't have as much cyber intel as they would need to even in the commercial space, and sometimes even in some of our government spaces. I want to thank you for sharing this with us today. This is an area that I think, I've done a lot of cybersecurity kinds of things and I do see the difference between cyber intel and having a resource like this that helps other people to make that case I think is very important. Otherwise, the cyber resources are going to just be focused on security, and they are going to lose the other vital interests.

Jared: You got it.

Suzanne: This is a great service you've done for us. Thank you.

Jared: Thank you, happy to be here.

Suzanne: I want to tell our viewers that resources we have talked about, the actual report itself and other resources related to it will be up on our website along with the transcript for this audio and video podcast. As always, anywhere you want to get your podcasts is where you'll find us, and especially on our SEI YouTube channel because we have one, and I love it. I thank you all for viewing today. If you have any questions, info@sei.cmu.edu continues to be a way to get to Jared and to any of us if you have questions. Thank you very much.

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.*