Secure by Design, Secure by Default

featuring Greg Touhill 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. I am a principal researcher in the SEI Software Solutions Division. Today, I am excited to be joined by Gregory J. Touhill. He is the director of the SEI CERT Division, and he is going to talk about the concept of secure by design, a longstanding tenet of the work of the SEI and CERT in particular and a practice that has been in the news of late. So we are going to get into some of that.

But first a little bit about our guest. Besides his role at CERT, he is also an adjunct faculty member at CMU's Heinz College. He is a retired U.S. Air Force brigadier general, was the first chief information security officer of the U.S. federal government, and a senior cybersecurity leader in the Department of Homeland Security [DHS]. So, both military and federal, and an author of several books, and those we will refer to in our transcript. Prior to his appointment as the head of CERT, he served as president of Appgate Federal Group, a government-facing cybersecurity products and services division.

We want to welcome you today, Greg, very excited to have this conversation. Lots of good timing. Since you are new to our podcast series, one of the

things we would like to do is have you give a little bit of an introduction of yourself, but especially what brought you to the SEI, and what are the fun things about working at the SEI for you?

Greg: Well, thank you. You know, as I have taken a look at my career trajectory, I guess the real seminal moment that was the inflection point was back when I was a second lieutenant. I was assigned to the 25th Air Division out at McChord Air Force Base. At my office, I was the maintenance control officer for the division's electronics. I had 12 radar sites that ranged from Minnesota along the periphery of the United States down to California. We had radars, computers, telecommunications, etc.

I came down from my office on the third floor of the facility to pick up my paper mail out of the main offices. There was my boss the lieutenant colonel, with his omnipresent coffee cup, hand on his hip going, *What the heck is that?* and pointing at a box. My peer who was a captain, he walked by and he said, *Well, that is a box, si*r. But I came in as the lieutenant, said, *Oh, cool we got a computer*. And the colonel said, *Do you know what that is?* I said, Yes, sir I do. And he said, *Take it out of here. It is yours now, figure out how to make it work*.

I ended up learning how to code, how to program that machine, and how to implement automation across not only our offices, but across the air division. I ended up getting a master's degree in systems management with a computer systems option from University of Southern California. That kind of set me up.

Suzanne: Sir, you and I have that in common. I am also an MS in systems management.

Gregory: Did you get the information systems certificate?

Suzanne: No, I was not the information systems. I was doing some other things.

Gregory: Well, we can compare notes on that.

Suzanne: Yes.

Gregory: That was back in 1984. Throughout the trajectory of my career in the military, I had great jobs. I had great mentors, and my mentors were folks that were enlisted. They were officers. They were career civilians. I had a thirst for learning, and I had people who teamed up with me to help make

me better.

I was introduced to the SEI very early in my career. SEI was founded in [19]84, and my first operational assignment was in '84, after I got out of a year of technical training. I came back to Pittsburgh very often because not only did I grow up here and started my professional career as a summer intern at the Mellon Institute next door, but I saw the development of SEI from their products or capabilities through research. I came to the institute many, many times as a customer in the military. And then as I continued my service to the nation at DHS, those relationships were reinforced.

Then when the position became open, I received calls from my friends at Carnegie Mellon, from DHS, and other places that said, *Hey, Greg, please apply for this job*. I did not have to think quickly about it. Because sure, I have been in really cool jobs. I got to be a general in the Air Force. I got to be the deputy assistant secretary for cybersecurity and communications at DHS. I concluded my federal career as the chief information security officer of the United States government. But there was one thing missing, and that was to climb the pyramid even higher, and to lead the community as the CERT director is just a dream come true for me.

Suzanne: I am very excited about how excited you are about being here. *Our heart is in the work* is the mantra of Carnegie Mellon. People that feel that is really what I think makes the SEI special as a part of CMU. I am glad to have you here, and I am glad to start getting to know you. And systems management, we will have to talk about that.

All right. This February, it was reported that the Cybersecurity Infrastructure Security Agency that we know as CISA planned to push technology manufacturers to make their products secure by design and to make that their default setting when customers are dealing with them. Let's talk about the cyber landscape right now and the catalyst behind this push. I think it may have also been something that they have talked to us about, because secure by design has been something we have been pushing for as long as I can remember. Talk about what do you see as the cyber landscape? We have seen some things from the CISA perspective, but what do you see?

Gregory: Well, thanks. It is a really good question. Let me try to frame it for our audience with some very practical talk as to what the cyber landscape looks like and why CISA is making this move forward.

First of all, as you take a look at a lot of the products that are out there—and

it does not matter if it is on your desktop device, if it is in an industrial-control system, an operational technology, an internet of things [IoT], or even something as simple as some of your portable phones, your smartphones that are out there. Many of the products that are out there, you have to configure security into it. Coming out of the box, most systems still are not configured to be secure out of the box. This has a significant impact in a very negative way on the security of our country and the safety of its populace.

If you take a look at a lot of the products out there—and I pick on one particular manufacturer whom I will not name right now—but it takes a technician who has already got all their basic certifications, it takes a technician about 18 months to learn how that system works and how to properly configure it, monitor it, and operate it.

While I was in the military, I was very sensitive to the amount of training time it takes to get to a level of proficiency. Most enlistments are about four years. If you think, I got 90 days for basic training, a block of time for folks that take leave to go home and show their family, friends, and the new stripe on their sleeve. Then they go to technical training, which in the IT and cyber career fields typically will take up to about 10 months. Mine took 10 months. I tried testing out, but they would not let me. It would not have helped anyway; I needed the extra time. If you take a look, that first year you are going through training. Then you go on to the job training to your first assignment. Oh, by the way, there is some leave to go home and show them the next stripe you get on your sleeve. By the time you factor in all this training and 18 months for one particular security system? People are confronted within the military, *Hey, do I reenlist?* An airman who re-enlists is maybe going to get in the low 30s for compensation. *Or, do I go work for somebody in industry or a contractor for well over a hundred on that?*

That is an economic impact, but the mission impact is even more grave from the standpoint of, *I have manpower that is not going to be optimized because of the complexity of the product*. As we have taken a look through CERT over the years, in the vast majority of cyber incidents we find the complexity in products and the fact that products are not out-of-the-box cyber-ready is a major contributor to virtually every single incident that has been out there in the cyber realm.

We can and we must do better. I am pleased to see CISA taking the bold leap forward to push this to the top of the agenda.

Suzanne: A few days ago, Jen Easterly, the head of CISA, spoke at CMU. One

of the things that she spoke about is contrast between different companies. One company who has multifactor authentication [MFA] as an out-of-the-box standard; you have to opt out of it as a user versus other companies that you have to opt in. It was something on the order of 90 plus percent of the users of the one were secure. They were using MFA, and only 3 to 5 percent of the ones that were not MFA out of the box.

To me that speaks to the thing that you are talking about, which is that the technology manufacturers are not accounting for what the users need to do to become secure. That is the heart of many of her remarks and the heart of some of the things that I have heard you say as well. We need to get past that, and this idea of secure by design and secure by default has become a rubric for what we need to do to help technology manufacturers go to the MFA out-of-the-box, versus MFA as an opt-in.

What are some of the things that we are doing at the SEI? Because I have been hearing that secure by design, I have been hearing for years here. What are some of the things that we are doing that are pushing in that same direction?

Gregory: Well, a couple of thoughts on this. First of all, we are very grateful that Director Easterly picked Carnegie Mellon as the venue for her to provide this national address on cybersecurity. Her three main points there were manufacturers need to be more transparent and make sure that their products are as safe as possible; secondly, that they embrace that sense of liability for their products being safe is important; then finally, the reinforcement of not only secure by design, but secure by default.

All of those things are congruent with some of the best practices that CERT has been identifying for many, many years and continues to do so. And then further, and we are very grateful that Director Easterly ended up spending a good portion of her afternoon with us in the SEI where she got to get some briefings from some of our researchers who are just doing brilliant work and knocked her socks off. She sent me a note last night that said she cannot wait to get back because there is some more research that she wants to dig deeper into. But what she brought forth was really a positive affirmation of the CERT Division's strategy, which is built on four main pillars.

The first is *advanced cyber by design*. Sound familiar with her comments? Yes. The second is *enhance cyber resiliency*. The adversaries are always going to have a say so you need to be able to build secure by design in your products so that you can take that cyber punch but keep going; your mission still has

to proceed in the face of adverse circumstances. Third is *move the market*. Our evidence-based research, we need to be able to help move the market by demonstrating through our research and the evidence of that research where these products are failing and where those weaknesses are. But we also have to come to the table with the solutions. *Here is what you need to do to make this better and to prevent this from happening again.* The fourth element is *shaping the future*. We do not want new products to be poorly manufactured or inadequate for the environment. We want information technology to be secure out of the box to really liberate America's workforce and unleash the power and the potential of the United States.

As we take a look at our strategy, as she was making her presentation, it really made us puff our chest out a bit and say, *Yes, we are on target with this*. But here is where we are already going with these things. From a secure by design [standpoint], we have put together a series of best practices that started with things like the Capability Maturity Model, which was birthed here. And into the risk and resiliency work with the risk maturity model and some other work that we have done. And then the development of DevSecOps as a software coding mechanism. Most recently, we have taken that DevSecOps into the reality of the marketplace, with the Platform-Independent Model for DevSecOps. Version 1 came out in May of [20]22, and it was updated, based on a lot of the feedback we got from the marketplace, it was updated in November of [20]22.

As we take a look across the SEI, the SEI has been really leading from the front in secure by design. When we append with the initiatives that Jen's launching now, secure by default, we want to make sure that manufacturers as part of the commitment to safety to the consumers of not only America but around the world, that those products come out of the box, they are easy to use, and they are secure by default, out of the box ready to go. Let's not necessarily be accepting training pipelines that take up to 18 months for us to understand how to properly use a product. That is not going to work, and it is not sustainable for our country.

Suzanne: True. What are some successes in secure by design, secure by default that the SEI has seen? Because when we go out looking for best practices, that is how we find them is we find people that are succeeding in these areas. Can you give a couple of examples?

Gregory: I think I just did with the run-through with CMM, the risk and resilience, the DevSecOps, and the recent Platform-Independent Model or PIM, as we are calling it. But as you take a look at some of the successes from

our mission partners in the government, those are some of the ones that I would like to showcase in answering your question.

As we have taken a look at weapon systems, for example, in the military, and I have got a little bit of experience with that, over 30 years of experience as a uniformed officer. When was the last time we had a major weapons system fail since the SEI was created? I would venture to say that there have not been significant failures. Our weapon systems are safe by design. They are secure by design. They work as advertised, and that this has really translated into stunning successes on the battlefield.

I take a look as a field commander, and I have been an operational commander at the squadron group and wing levels. In my last assignment downrange, I was working for General Petraeus and then General Mattis as one of the generals out in the field. One of the key metrics of success is mission accomplishment, but also casualty rates. I know for a fact being on the receiving end of the support we have gotten from the Software Engineering Institute that because of the work that the Software Engineering Institute has contributed to, our safety rates are higher, our mission effectiveness rates are higher, and our casualty rates are very, very low. I think success on the battlefield is part of the product of our work.

But also, even more importantly, is because of the effectiveness of our military, we have been able to deter an awful lot of other things. As a retired military officer, I am very proud of the impact that SEI has had with our military force. But as a former DHS official, senior official, charged with protecting critical infrastructure, we have seen a lot of great work from the SEI translating into society. Those best practices that the Software Engineering Institute has provided in not only security but in software engineering and now in artificial intelligence engineering, all have contributed to the acceleration of our economy into a more digital and robust and high-velocity, high-precision economy.

Then further, as you take a look at how automation is going into different elements of critical infrastructure, the safety of a lot of our critical infrastructure is much better. We have evidence that OSHA collects, the folks who do the Organizational Safety and Health Administration, the rates of accidents for employees across many critical infrastructures have gone down with the precision automation that is being implemented. Our work matters, and we are seeing it in all elements of society in the .gov, the .mil, the .com, and virtually every domain out there.

Suzanne: One of the things that I am going to infer from your comments is, and it is something that we talk about in customer work a lot, is secure by design, secure by default in many cases translates almost directly into safety by design, safety by default. Even though we are not the Safety Engineering Institute, that is one of the things that we see—that security often is very tightly coupled to safety. I know that there is work that goes on in CERT that relates to that as well.

You talked about Ms. Easterly visiting us, can you tell us a little bit more about the visit and some of the things that she was excited about or things that you were excited to share with her?

Gregory: I will start with campus. As a member of the campus community and in my faculty role as well, we were really excited to give her a dip in the water of Pittsburgh and Carnegie Mellon. This was her first visit to Pittsburgh. The weather was great when she got here, but then we showed her how fast the weather could turn in the afternoon after her address. But there was a lot that we were able to pack in from a campus perspective.

She was able to meet with senior faculty members and deans of different departments across the campus and get a feel for where their priorities are and how they are working in their different academic departments to improve the posture of cybersecurity awareness in their curriculum. Two, she got to meet with a lot of students as well. We thought that that was really critically important so that she could see the great caliber of not only our faculty but also of our students. She was so impressed she turned it into kind of a semi-recruiting tour as well. Three, she got to see some of the really cool research that is being done on campus. Given the time constraints, we had to focus on one, and we picked the robotics engineering research. I would have loved to have given her some more time with the human–computer interface, but she got to see the robotics and the power and the potential of the research that is being done on campus. It served as a really great segue into the work that is being done in CyLab, which as you know, Suzanne, was co-founded by CERT and campus as the security and privacy institute of the university. The previous meetings provided that capability for her to go in and see what is going on in CyLab and then come over here to SEI for three quick briefings. But in between, we did feed her.

Suzanne: Always good. Easy to do in Pittsburgh.

Gregory: Carnegie Mellon and Pittsburgh are very welcoming when it comes to meals. One thing I remember during my military service that took me all

around the world was that old channel 4 ditty, the ABC affiliate, *This is the best hometown*. I am getting all choked up with that. During lunch, she also was able to meet with the folks from WiCyS [Women in Cybersecurity], our students that are part of the Women in Cybersecurity group. Michelle Tomasic, who works in CERT, has done a magnificent job in leading the growth of WiCyS on campus, in the SEI, and around the country. Getting Jen to spend some more time with Michelle was great. But Michelle got to introduce some of the students that are part of that initiative. That really swelled Jen's heart, as to showing her that our heart is in the work, and we are very inclusive here on campus.

We topped her day off with a great presentation series. We took her to our Platform Insights team. She got some great insight into the work we are doing in evaluating various products on behalf of government and military customers. We put all the toys out on the table, and she could see some of the things that we are doing research on. But she also heard some of the things, the alarm bells that we are finding with our research.

Then we took her upstairs for two briefings, not focused on PowerPoint, but more on conversation. The first one was taking a look at software that is in the firmware. When you boot up your computer, you have got to have something to boot from, and that is located in the firmware on the device. We have some great research that has been done by Vijay Sarvepalli, Cory Cohen, Jeff Gennari, and folks from our Threat Analysis directorate. She was wowed by the depth and magnitude of that research. We basically talked, okay, so where is this leading? What is the impact? We gave her some information and some suggestions as to potential next steps that collectively we can take together. Then we topped off the day with a tremendous briefing from Dr. Nathan VanHoudnos, and Dr. Shing-hon Lau on adversarial AI [artificial intelligence]. For those who are not familiar with that, think AI for cyber, but also cyber for AI. We had a great conversation with her on that, and we whetted her appetite on a few other subjects that she is just going to have to come back on.

Suzanne: I suspect she will be back.

Gregory: I hope so.

Suzanne: And not just for the food, so…

Gregory: Well, you can't beat the food.

Suzanne: There is that. Are there some concrete steps that you have agreed to or are exploring with the SEI, CERT working together with CISA on some of these initiatives, or is that yet to come?

Gregory: Absolutely. We are in the process of actually renewing our agreements with the folks at DHS and CISA. That is moving along extremely well. We have been engaged in the DHS mission as a Software Engineering Institute since the inception of DHS and even before that, with its predecessors.

As we take a look at where CISA is going and where the nation needs CISA to be, our work is going to change a bit with them. I think that is because of the successes that we have had. Let's not forget that CERT served as the national Computer Emergency Response Team, starting in 1988, in response to the Morris Worm. That was well before the 2003 initial creation of the Department of Homeland Security and the Office of Cybersecurity and Communications that came out a year or two after that. We have been there all the way through.

But we have got to change too. I think it is not necessarily retirement or a transition of this or that. I think it is an evolution. We have all grown together. As we look forward, one of the things I have talked about is CERT started as Computer Emergency Response Team. But we have already birthed that industry from starting here. That industry is relatively mature. We have identified the best practices. We stay plugged in. We, through our research, continue to refine those best practices and share widely.

But our methodologies, our approaches, the engineering of cybersecurity, we have pivoted towards a cybersecurity engineering and resilience team that is aligned with that secure-by-design and secure-by-default mantra that Director Easterly talked about during this week's speech here in Pittsburgh. I think we are poised for the future in better supporting not only CISA but also our other government and military partners and those in critical infrastructure that we have been partners with for years. As we take a look at secure by design and secure by default, we have already laid the table out. Our best practices that we have identified, that call to action that Director Easterly made, I think you are going to see as folks come back to CISA and say well, *Who can help me better understand how to build secure by design and secure by default?* I think you are going to see Carnegie Mellon, the Software Engineering Institute, and the CERT Division here all being significant players in those conversations.

Suzanne: I want to talk a little bit about transition, because that is at the heart of what makes the SEI different from other research institutes, is that we do not just focus on doing groundbreaking research, but we look at how do we get people to use that research? When I heard Ms. Easterly talk about normalization of deviance—that concept was birthed as part of researching the Challenger disaster—the idea that we normalize things that really we should not, in terms of deviations from safety and other norms. That to me, there is a social-engineering aspect of that of, how do we get people, what is the transition from normalizing deviance to normalizing secure by design, secure by default? Is that part of some of the things that you are looking at, or is that something that is still in the works? Because I see that as a really hard problem.

Gregory: It is a really hard problem, and it is something that we are trying to address. With my arrival here to the CERT team, I am trying to broaden the aperture of how we are looking at issues. Typically, folks when they think cyber, they think two things, they think hardware and software. And I think of systems. I think hardware, software, and wetware, the human element.

As we take a look at the lessons learned from things like the Challenger, and I am intimately aware and familiar with not only the incident, but also all the resulting studies after that. You do not want to become numb to the things that are wrong because they are always there. I think that call to action that Director Easterly made is a really good refresher that we should not be satisfied with the status quo. The fact that I have enculturated myself to every morning, when I get up, I look at my smartphone and I see, *Oh, how many patches occurred during the evening?* It is part of my routine in the morning. I go and make sure that before I leave my house, my devices are patched, they are properly patched and configured. Most folks do not necessarily have that same level of discipline.

Suzanne: I can't say that I do it.

Gregory: Yet I am still outraged by the fact that we continue to have these things. Now, no software is going to be perfect. We need to have discipline on it. I think through the work that we are doing and we continue to do, we need to move the ball forward to use that metaphor. We need to get better with time. I think the time is now to embrace some of the tenets of Director Easterly's challenge. The big three that she mentioned were the manufacturers need to step up. They need to put out better products. Two, they need to be more transparent and recognize their liability. Then three, make it secure by design and secure by default, so that we can better hit the

promise of information technology to better society as opposed to drag it down.

We here at the Software Engineering Institute, across all three technical divisions, I think are ready. We have been contributing to the conversation in a very positive way. I am just absolutely delighted that Director Easterly's initiative is aligned with our agenda, our strategies. I think that we are going to see goodness come out of this initiative that we are going to be supporting.

Suzanne: I was really pleased to hear that Director Easterly got a chance to talk to department heads that are not like the cybersecurity department and talk to them about how they are incorporating cybersecurity awareness into their curriculums. That was actually one of the things she mentioned in her speech. But from a transition viewpoint, that is actually one of the key things that we see as a difference, is when it is not just a specialty item—*You have to take a special class in this*—to now, it is something that everybody is taught.

I mean, I looked at Agile practices as an example; 10 years ago, 15 years ago, you had to take a class in Agile. Now, even as an undergrad, you cannot get out of your CS degree or software engineering degree without knowing Agile, and there is no special class. It is just something that is part of that. I am looking forward to that as one of the transition steps is making cybersecurity awareness, and the demand. I guess what I am thinking is that normalization of deviance, the numbness that you talk about, we have got to break that numbness cycle and get people to say, *No, I am not going to accept this product. It is not secure by design*. And getting people, getting students, the next generation aware, it may be a little harder to get my generation to stand up and say, *No, I will not.* But do you see that happening in other places? How is the SEI contributing to that?

Gregory: A couple of things on that. First of all, we must never give in. I think, Winston Churchill said, *Never give up…*

Suzanne: Never give in. Yes.

Gregory: I recall back in the late [19]90s, I was a lieutenant colonel and a squadron commander, and I was responsible for a squadron of almost 900 people supporting a very large base in the western United States. We had a lot of computers, and we had a depot for airplanes, we had a research facility with a nuclear reactor on the base, we had all sorts of different things. And we were just beleaguered by the patch-of-the-day type stuff. You never knew

what you are going to get, we did not have any predictability. We bumped it up the chain of command. We said, *This is not acceptable for us, it is not sustainable.*

And our senior leaders went out to Redmond, [WA], for example, to Microsoft, and they said, *Well, things have got to change. We need better security in your products, or we are going to have to start looking somewhere else.* As a result of that, Bill Gates sent out his famous we are a security company memo and made it a priority on the agenda, and things got a little bit better. That is where the Patch Tuesday came from.

Jen picked on Patch Tuesday because it has been out there for now 23-plus years, but we continue to see the number of patches growing. Sure, everybody knows when the patches are coming, but they are growing. If you look at the metrics, they are growing at a rate that is unacceptable. I think it is time to revisit it. I am not picking just on Microsoft. But it is on all the vendors, [who] really need to take a good look at the security of their products and the data that is out there. I also think from our perspective at the SEI, there is a lot more work that we can and should do. Without tipping the hand as to some of the classified work and some of the research, nobody wants another Solar Winds. We are working on that with our government partners on supply-chain security. Perhaps we can talk another time on that.

Suzanne: I would be very happy to talk about that.

Gregory: We are doing some really great research too on some of the architectures, configurations, and strategies, such as zero trust, which is something that I have been a huge proponent of since my time in government and continue to do my research here, both through Heinz as well as SEI.

And then, as I take a look at opportunities for the government following on to what we just discussed with Director Easterly and talking with other department heads, the government has a program within the National Centers of Academic Excellence in Cybersecurity, and they have awarded that to numerous universities around the country. But sadly, not all of those universities are teaching cybersecurity to everybody who needs it. I think that program needs to be updated and revamped.

I think every student, before you get a degree from a United States university, every student should take a course in cybersecurity. Now that may be a bit disingenuous sounding to some, coming from the CERT director

here. But as I take a look at it, I want my teachers to be teaching the K through 12, as well as in the universities. I want our up-and-coming workforce to understand the threats to privacy, security, intellectual property. Data has value. We should teach our kids about it, and then further, our teachers need to be prepared to teach. Our law schools…

Suzanne: Had not even thought about that group, yes.

Gregory: Our lawyers are one of the principal targets of cyber criminals. Because lawyers aggregate information that is very sensitive. It is like a super-duper honeypot, when you score a cyber hit on a lawyer. Our law schools, it is not only just intellectual property, it is actually the data that they gather.

What about our business schools and our business classes? You should not be able to get a bachelor of business and not understand the impact of the technology that your business is going to rely on, and the impact of cybersecurity issues.

The focus has largely been on computer science, computer engineering. We need to broaden the aperture because America's economy is based on information technology. It touches every facet of our lives. I think the government, by updating that program, could have a really profound impact on the next 10 years of getting everybody to be thinking secure by design, secure by default; then be better customers as a result, more demanding and informed customers.

Suzanne: I have a brother who works in the security field. One of his challenges is going into private companies, to speak to your business-school analogy; he is constantly having to prove the ROI [return on investment] on improving security. To me, it is a hygiene thing. You should not even have to do that, and I agree exactly with what you are saying. We need to educate people that are going into business. This is not the place you are looking for ROI. This is the place you are looking for baseline, floor-level, cannot do business without this level of security.

Gregory: Well, and we have actually had great relationships with insurance companies. The CERT Division has actually been working to refine our research and our data by working with insurance companies, because what you are trying to do in making a return on investment is often argue, what is the cost if this bad event happens? That is the same type of work that actuarials do in insurance companies. Our researchers have already been

reaching out to different insurance companies and comparing notes, and building out frameworks and models that can help folks better understand that return on investment and the consequences of not making those investments. I think that makes our research richer and more valuable, but it also helps the industry become more educated, informed, and transparent into how they go about doing things like cyber insurance.

Suzanne: Interesting. I had not made that connection before, but I see it. Yes, there is some cool stuff.

Gregory: It is really interdisciplinary. It reinforces my notion that we need to take that national cyber academic excellence program to the next level. Because it is not just the technical teams that need to be trained. It is, we need to make this a national imperative. And every academic discipline is reliant nowadays on safe, secured, and assured information technology and products and services.

Suzanne: And data.

Gregory: It is all about the data.

Suzanne: It is all about the data.

Gregory: Data is the fuel of our economy.

Suzanne: Yes. So people that are fired up by what you have been saying and want to learn more about secure by design, secure by default and the things you have been talking about that CERT is doing, what are some first steps that you would recommend to them to get more informed on these topics?

Gregory: Come visit us online, sei.cmu.edu. Come take a look at what we have been writing about—our blogs. You can go into our knowledge base, and just type the subject that you want to learn more about. I have had a lot of my colleagues from government and military who have said, *Hey, Greg, what are you guys doing?* And I say, *Just come visit us. We are open 24 by 7. Type in what you are interested in, and then see what we have published. And if we have not published something you are interested in, that indicates there is a gap, and maybe we ought to be researching. So come back to me if you find a gap.*

As we have taken a look at the 30-some plus years of experience of the CERT and almost 40 years of the SEI. We will be celebrating 40 years next year.

Suzanne: Oh, wow. Yes.

Gregory: There has been so much great work, great research, and vision out of our organization during our lifetimes. I am excited about the future. I am always looking for gaps, where we can take our unique skill sets to better protect national security and national prosperity. But our gateway is always open; come visit us at sei.cmu.edu.

Suzanne: I know there are tons of resources. Every time I do a podcast that relates to CERT, I am out there looking at our published stuff, because we have more out there probably than anybody about any of these topics.

Gregory: Yes, and we have had folks that have reached out and said, *Well, you know, Greg, can I have somebody from the CERT talk to my group or do a webcast,* and we do all of that too. So all the contact information for those things is on our website as well.

Suzanne: Good. You mentioned supply chain is something that is on your horizon. What are some other things that are on the horizon for you that you want to work on next that are not necessarily at the top of the agenda for the moment?

Gregory: In addition to software supply chain—and I do think that is an imperative for research funded by the government and the military—I am also very bullish on the need to expand that adversarial AI research, that AI for cyber and cyber for AI. In partnership with our AI Division, I think much more needs to be done there.

Then, I think as a third, I want to circle back to what we were both saying about data. People do not necessarily have the right aperture when they are thinking about cybersecurity. They are thinking enterprise IT. They have target fixation. I think we need to get our heads up out of the cockpit, to use the Air Force's terminology, and recognize that the cyber ecosystem includes enterprise IT, industrial control systems, operational technology, cloud-based environments, IoT. I think we need to recognize that there are risks out there. People need to understand that unstructured and semi-structured data that they typically would have in the enterprise IT is just a fraction of the total data that is available to an adversary set. You need to append to that metadata, and the semi-structured, structured, unstructured, all of the datasets that are out there in all of your systems. And businesses need to recognize that as well. You will see us be more evangelistic on data and trying to educate and inform folks as to all the data that is out there, and the risk

exposure, the risk landscape, and the potential attack surface.

Suzanne: OK, so you are going to be busy for a while.

Gregory: I came here because my heart is in the work. The work that we do matters. I was always raised that, being a Pittsburgh kid by my origin story, you should never measure the value of your life by how much money you make, but by the difference you make in the world. I think we here at the Software Engineering Institute get to make a difference every day. I hope that we will have the opportunity to make a positive difference in the lives of people not only across the country, but around the world with the work we continue to do.

Suzanne: Good. Well, we do. I know we can go on for days about anecdotes of ways in which the SEI has helped the world. I just want to thank you for this conversation. I believe that your vision for CERT moving forward, as you said, what are we doing for the next generation, is going to resonate, and hopefully we will draw some people that want to do some of that research to us as well. Because we always need people that can have that kind of impact on the world. And so, I just really want to thank you for being with us today.

Gregory: Thank you. It is a pleasure to be with you.

Suzanne: This is great stuff. For our audience, as you know, we will include links in the transcript to many of the things that we have talked about today. I also want to make sure that you remember that there is not just one place you can get our podcasts. You can go to whatever your favorite is: Stitcher, Google, Apple, whoever you like. We also offer our YouTube channel where you get to have the video. We encourage you to go look there. I want to thank all of you for listening today. And we will go ahead and conclude this. Thank you again to Greg Touhill.

Gregory: You are most welcome.

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 do not hesitate to email us at info@sei.cmu.edu.