Carnegie Mellon University
Software Engineering Institute

SEI Podcasts

Conversations in Software Engineering

Identifying and Preventing the Next SolarWinds

Featuring Gregory J. 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, a production of Carnegie Mellon University's Software Engineering Institute. My name is Suzanne Miller, and I am a principal researcher in the Software Solutions Division of the SEI. Today I am joined by Greg Touhill, director of our SEI CERT Division. Our topic of discussion today is how to identify and prevent the next SolarWinds attack, and we will talk about what that is in case you do not know about that already, but most of us do.

But first, a little bit about our guest. In addition to his role at the CERT Division, he is also an adjunct faculty member in CMU's Heinz College. He is an author, a retired U.S. Air Force brigadier general, and was a senior cybersecurity leader in the Department of Homeland Security [DHS]. He was also the first chief information security officer of the U.S. federal government. Prior to his appointment as the head of the CERT Division, Greg served as president of Appgate Federal Group, a government-facing cybersecurity services firm. Welcome, Greg.

Greg Touhill: Hey, thank you for having me today.

Suzanne: Nice to talk to you again.

Greg: Absolutely. I am looking forward to it.

Suzanne: We previously talked about secure by design, secure by default as a strategy for the future of security. Today, we are here to talk about other things that are one of the reasons we need secure by design and secure by default. I do want to tell our audience that if you did not see that first podcast, I do recommend it. We will link to it in our transcript, and it gives a lot of background on some of the things that are going on currently related to trying to address these issues. Before we get into SolarWinds, which is a fascinating topic by any measure, tell us what you think is the best thing about your job here at the SEI.

Greg: Well, it definitely has to be the people. One of the things that is attractive to almost everybody who comes here, either as a visitor or as an employee, is the mission. And our mission is great: helping our government partners in the military and the federal-civilian executive branch better defend national security, but also national prosperity. That is an attractive mission set, and it is something I have done throughout my professional life.

As we work with our different mission partners in the Department of Defense, Homeland Security, State, Treasury, all the different parts of the government that protect and defend the American people, that is a great mission that helps attract all sorts of talent here. But what really brought me here is having been a customer of the SEI in my military roles, in my roles at Homeland Security and the White House, it has always been the great people that we have here in executing that mission. I love getting up from my desk and walking the halls. I am just amazed when I get to bump into the world's leading experts in these different disciplines that we have here. We have the world's greatest software engineering experts. We have folks who are creating the artificial intelligence engineering discipline. And here we have the cybersecurity birthplace with the CERT Division that I am so fortunate to work with. Our team, not only in my technical division of CERT but across the SEI and across the campus, this is a great place to continue to serve the nation and one of the reasons why I wanted to be here.

Suzanne: And I will say after being here over 20 years that people keep me here as much as the mission. I am with you in terms of the mission is what drew me here, but it is the people that keep you here.

Greg: Absolutely.

Suzanne: And so that is a great recruitment speech there. Thank you, Greg.

Greg: You are welcome.

Suzanne: All right, but today, we are here to talk about SolarWinds, and we want to talk about the initial attack. SolarWinds is the name of a company. It is a company based in Texas. At the time of the attack, they provided software to our federal government. In late 2020, news surfaced about a cyberattack that had already been underway for several months, so that is not good. The attack had reportedly compromised 250 government agencies, including the Treasury Department, the State Department, some of the ones you have already mentioned, as well as nuclear research labs. And, in addition to data that was compromised, it resulted in financial losses of more than $90 million. If you have not heard of SolarWinds before, this is probably one of the most dangerous modern attacks on software and software-based businesses and agencies and government in the recent past. What do we know about the origins of that attack, and how did it actually unfold?

Greg: First of all, let's make it perfectly clear to our audience that SolarWinds as a company were the victims here.

Suzanne: Absolutely, correct.

Greg: They were the victims of a well-conceived and well-executed attack on their software supply chain. As you take a look at how America's economy and actually the world's economy has been increasingly IT-enabled, the SolarWinds product actually is one of the best products out there in providing visibility across enterprises. I personally, when I was the chief information officer of USTRANSCOM [U.S. Transportation Command] and before that, Air Mobility Command, we were customers. It was because they had a superior product in the marketplace.

Adversaries that took a look at the capabilities of that particular software set said, *That same visibility that CIOs and businesses were leveraging, given by that product, could be tampered with for nefarious purposes*. They launched a very exquisite attack to go after the code for that company and got inside the product-development cycle. And with subtle tweaks in the code, they were able to gain access that gave them greater insight into the customers that were using that code base.

It was detected by a third-party company, Mandiant, which is now owned by Google. Mandiant, which is arguably the world's best cybersecurity incident-response company, Mandiant itself was a SolarWinds customer and determined, *Hey, we are seeing aberrant behavior here*. They raised the alarm. They worked with SolarWinds. They notified the government. They leveraged existing governance and oversight channels. We had a widespread community-of-interest response to that breach. It was wholly unsatisfactory in the results, but as you peel back the onion, we took a look at this as a highly sophisticated attacker who got inside that supply chain and took advantage of that for purposes that still are under speculation.

But all software that is out there has a lesson to be learned as far as the development, the product fielding, the quality—and getting back to our previous message of secure by design and secure by default—that they can learn from the lessons learned in this SolarWinds attack, or perhaps it is better to say, the attack on SolarWinds that affected all of us. As we have taken a look at *What can we learn as a community on this*, that secure-by-design and secure-by-default approach to putting products into the marketplace is critically important, but there are a lot of other things that are out there. From a CERT perspective, we are taking a look out and saying, *OK, what else is out there that could be tampered with that could be exploited? What other areas are not being guarded adequately to prevent something that could be exploited to the detriment of national security and national prosperity?* I think if you take a look at those approaches, it all will start with the secure by design and secure by default.

Suzanne: I know in other podcasts we have also talked about things like the Acquisition Security Framework, which is directly aligned to deal with supply-chain issues for people, for organizations that may not be as sensitive to the risks that are posed by their supply chain. What you said about everything being IT enabled, it is not just IT enabled by my IT, but it is by my first-tier and second-tier and third-tier suppliers. That is really where we got into where the attacker on SolarWinds was very clever in understanding that and in using that as a means of getting access to the primary targets.

Greg: Absolutely, and as you take a look, there are plenty of examples to go back many, many years, and for our audience, I would recommend you can go on YouTube, for example, and type Rob Joyce, R-O-B is his first name, and then Joyce, J-O-Y-C-E, and then type 2016, and then the phrase, U-S-E-N-I-X. Rob spoke at a conference at the USENIX Conference in 2016 when he was the NSA's [National Security Agency's] head of tailored access operations.

That organization, think of those as the top cyberhackers at the NSA. He talked about the tactics, techniques, and procedures used by hackers. Very rarely do hackers use zero-day exploits or things that had not previously been disclosed.

Rather, what they do is they take advantage of weaknesses in the applications of patches, proper procedures, and such. I recommend folks take a look at that great video that Rob outlines, *Hey, here is how folks actually go, from a nation-state, high-level hacker*. *This is what they do*. That comes from, at the time, the nation's top hacker on behalf of the United States.

Suzanne: What this brings to mind, and we have mentioned this before, secure by design and secure by default is not a bunch of technologies. It is really mostly human-based governance, processes, procedures that … As humans, when we become skilled at something, we tend to let go of some of the guardrails that we might have used when we were less competent, because, *Oh, I know how to do this*. But we have to emphasize that the discipline of software engineering is about maintaining that discipline, no matter how much we know, no matter if we are Rob Joyce or Suzanne Miller, who is not nearly as skilled as she used to be. But we have to make sure that the human element …That is really what these attackers are taking advantage of.

Greg: As you take a look at systems, and my educational background includes a systems management engineering background, same as you.

Suzanne: I know.

Greg: There we go. We take a look at it from the cybersecurity standpoint along three lines of effort. The first one is the software. We have to make sure that the software is secure by design and secure by default, but we also are looking at the hardware and the provenance of the hardware. Let's not forget that the hardware is a collection or repository of all sorts of different software, spread out amongst many components.

Then we also do not lose sight of the wetware, the human element. We all are walking computers with the most powerful computer ever invented, but together, all three—the software, the hardware, and the wetware—come together into a system. As you are taking a look at security, you have to factor in all aspects of the system. The wetware, the human element, creates the processes, the procedures, the priorities and such that help make that system work in an optimum measure. Ultimately, what we were looking for is methods that are going to enhance the effectiveness, the efficiency, and the security of that system.

Suzanne: And that means we have to make the humans effective and efficient as well as the software and the hardware.

Greg: We have to engineer the whole system.

Suzanne: Yes. I want to come back to SolarWinds for a minute, because I am sure some people are thinking, *Okay, scary that this had been going on for several months*. If I have any suspicions, what should I be looking for that would help me understand, what are the warning signs that there might be something? What did Mandiant identify that would be warning signs that something might be amiss in my supply chain, in the software that I am using?

Greg: Well, I have not seen the full Mandiant report myself. However, I have gotten plenty of briefings and had many conversations with folks from Mandiant as well as within our community. You always look for aberration, something that is not expected. In Sesame Street, they would say, *One of these things is not like the others.*

Suzanne: Not like the others, yes.

Greg: That is often where you see tipping and queuing, is when you see some aberrations. Typically, in a maintenance role, you are looking for aberration as a sign of degradation of capabilities, something is going out of tolerance. You can often see through maintenance activities where something is drifting out of tolerance. It is usually a sign that you have to do preventive maintenance, you have to do a replacement. Sometimes you have to do an upgrade.

In this particular case, Mandiant saw telemetry that was inconsistent with how the product was supposed to work. And that caused them to provide a much deeper analysis of what was causing this. Some of their researchers who noticed the fact that this was providing some telemetry that was unexpected, they dug down deeper. What they found was disturbing in comparing to expected and some of the documentation that was out there. They were smart enough to react that, *Hey, this is not right*. They raised the alarm. They got with their supplier and compared notes. *Is this normal?* And when the supplier said, *No, it is not*, then a much deeper investigation was initiated, and the call to the community went out.

As different folks are taking a look at their systems, they should have a really good feel for what is the expected behavior of their system, what is the expected behavior of their telemetry, continually monitoring their data. Security operations centers specialize in this and have a lot of automated tools that can help them identify when things are out of tolerance, but a lot of us are not necessarily software engineers or cybersecurity engineers. We do this with normal, day-to-day living too. When you are driving your car, if your car is not in alignment, you can feel it pulling to the right or left. If you have a tire that is not having the proper tire pressure, you can rely on the tire-pressure monitor, the TPM, which a lot of vehicles now have. But you can also do the visual, *Hey, that tire looks a little low. I am going to go check that*. Similarly, as we are looking at these software-intensive systems, we have a lot of tools that are put into the software to help us monitor, but then we also have the human element that can help us go and monitor and look for aberrations.

Suzanne: Ultimately, that is what Mandiant, that was the thing they did. I also want to highlight the fact that they did not stay quiet about it, because that is one of the things that we know is a barrier for organizations, the embarrassment of people saying, *Oh, You have been hacked*, has sometimes in the past led people to wait to make a statement about this, and Mandiant did not wait. They went forward with it, and that is really the behavior that you need, so that the community can be protected because, as we found out, Mandiant was not the only victim of this as a primary target. There were 250 or more, so…

Greg: There was not a lot of delay at all. Kevin Mandia, a fellow Pittsburgher and airman or former airman in Kevin's case, Kevin Mandia, as the CEO of Mandiant, stood up and he said, *Look, we have been breached. Here is how it happened*. Kevin reiterated SolarWinds is a victim. Mandiant is a victim, and there are a lot more out there. He showed bold leadership in an environment where many companies would say, *Oh, I do not want to identify a material weakness because it could adversely affect my stock price or the value of my company.* Mr. Mandia stood up as a leader and said, *We have a problem and it affects the whole community, the whole of our fabric*. That is the type of leadership we need throughout society is when you find a problem, you stand up, you own it, and you take immediate action to fix it. Mandiant did a great job in standing up, identifying the problem, and took a leadership role in identifying how we can fix it together.

Suzanne: We have already mentioned a couple of resources that are available to people to find out more about the general topic of supply-chain risk to software, secure by design, secure by default, if you are actually producing software. For organizations that may feel like they are a little bit behind the curve on this, what are some transition resources for building their competency to prevent their own—being like SolarWinds and being a victim of this kind of deep supply-chain hack? What can we offer to them?

Greg: You mentioned the Acquisition Security Framework, which is, what I think is step one. I think as you take a look at the great work of Dr. Carol Woody and Chris Alberts and a lot of our other researchers that have really taken a solid look at how we acquire goods and services and software development and such, creating that Acquisition Security Framework. It is a great way of companies of all sizes, from the really large, multi-national companies, all the way down to the small and medium businesses as well.

I think it is important for our audience to recognize that sometimes you put out stuff that only applies to certain businesses of certain sizes. But I think the Acquisition Security Framework scales really well all the way down to small and medium businesses as well. I recommend folks go to our website, sei.cmu.edu. In the keyword, type A-S-F, or Acquisition Security Framework, and you will see a wealth of information on the research regarding this, as well as some details on how you can, in your organization, tailor your decision-making to take a look at, *Here is this thing that you have to take a look at, this thing, this thing, this thing, this thing.* When you do that, you are evaluating risk every step along the way. You will never get risk to zero, but you can manage it. Then further, you will be making risk-informed decisions that will help you better protect not only your business but your contributions to national security and national prosperity.

That is one. There are other things that you can do, such as work with our mission partners at CISA and subscribe to CISA's alerts. And CISA, for those who do not know, is the Cybersecurity and Infrastructure Security Agency [C-I-S-A]. Go to cisa.gov, or cisa.dhs.gov. I think they resolve to the same site. You can sign up for alerts so that if in fact something bad happens in the cyber neighborhood, we in the CERT Division at the Software Engineering Institute help provide information to CISA at DHS to be the neighborhood watch captain for cybersecurity.

Suzanne: The clearinghouse.

Greg: Right. If we see something, we say something, and we encourage the citizens of the country, the companies of the country to say something too, but if you are not subscribed to that cyber neighborhood-watch alerting system, then you are missing out. And you do not get the timely results that you need to better manage your risk. I recommend folks visit the CISA website at cisa.gov and sign up for the alerts so that you can have a very timely alerting system. One thing too is we help CISA in characterizing these different attacks with the *so what? Here is the problem, here is what the potential impacts are, and here is what you can do.* I think CISA over time has done a really good job at providing actionable intelligence and information. There is still a long ways to go, but it has been doing a really good job. We are really proud at the CERT Division here at SEI to be a major contributor to that conversation.

Suzanne: We actually did have a conversation about CISA and its future and the things, the ways that we are working together in another podcast, which we will reference in the transcript just like we will reference the Acquisition Security Framework. I had a great conversation with Carol Woody and Chris Alberts about things related to that.

We have plumbed the depths of SolarWinds and things that we can do to prevent that, but I know that you, as the director of CERT, have lots of other things, so just give us a little preview of some of the things that you have in the works that people may not already know about who are listening to the podcast.

Greg: Well, there are a couple of things. First of all, we have been taking a look at software security for years. We invented the discipline of cybersecurity engineering here at the Software Engineering Institute and putting together those best practices and the lessons learned from attacks that we are seeing, not only with the supply-chain attacks but other attacks that are going on.

The first thing that I would like to highlight is the fact that it is important to know where your software came from, and making sure that your software, in fact, has that secure-by-design and secure-by-default capability in there. One of the things that we have been involved in is this conversation on the software [bill of materials], and particularly from the standpoint of the security lens. Working with our colleagues in the Software Solutions Division, we are finding some best practices and sharing them widely as far as, here are some of the best practices in understanding where your software came from, as well as gauging the risk of the software and the resilience of the software and advising our mission partners in the government as to how to implement such things like the Acquisition Security Framework to assess the material weaknesses or strengths of the software. A software bill of materials, I think, is a really good thing, but how far down do you go on that?

Suzanne: Good question.

Greg: Particularly when it comes to open-source software? We can go back to incidents back in 2014 like Shellshock and Heartbleed where old code suddenly had material weaknesses in them. We are finding hackers out there are finding that old is new again when it comes to hacking.

A lot of alerts that have gone out in the past that said, well, *Patch this, patch that,* or *This has weaknesses here or there.* We are finding that across the world and across the country, there is a lot of old system and a lot of old code that is still in operation.

Suzanne: People are afraid to touch it, because the people that built it are retired, and nobody knows what is going to happen. It works, right?

Greg: Right.

Suzanne: That is, if it is not broke, do not fix it, but that gives an opening to people that are willing to break it.

Greg: Right, and as a lot of organizations have put these legacy systems in place, sometimes their attention gets drawn away to the newer systems that are out there and the newer software. And they are not necessarily paying attention to that old legacy code with the same level of security awareness as perhaps they are with the enterprise IT.

Suzanne: Sure.

Greg: What is old is now new for a lot of hackers, and folks that have the legacy system out there are best advised to pay even closer attention to that.

Two is, we find that folks continue to have what I call target fixation on enterprise IT and are not necessarily paying as much attention to their data that is at risk and exposed in operational technology, internet of things [IoT], industrial control systems, and I will add to that the RF-enabled [radio frequency enabled] devices that they have and some of the data that they have in third-party clouds. A lot of software-as-a-service entities are custodians of your data that could be very valuable, and in the wrong hands, could provide a great measure of risk to your organization.

One of the things that we at the CERT Division here at the Software Engineering Institute, we are trying to raise the awareness for your entire cyber ecosystem and the protection of your data wherever it resides and getting folks to understand that the operational technology…A great example of operational technology is critical manufacturing devices, for example. Everything is computerized now. There is a measure of automation in all sorts of systems. So your operational technology, if you are in the military, an F-35 is a computer system with wings.

Suzanne: Yes, it is.

Greg: Actually, many computer systems with wings. An M1A2 Abrams Main Battle Tank, many computer systems with treads. Same thing with our ships and our submarines. But in the business world, you have numerous devices that are not necessarily desktop computers.

You have to be thinking operational technology, your industrial control systems—pumps, valves, switches, everything that keeps the lights on, the water flowing, internet-of-things devices, RF devices, software as a service, hybrid clouds, all of that. The attack surface is wider. Your attention needs to be wider. Understanding your risk with all the data that is out there is important.

The third thing is, think what is hidden, and what is your risk with some of those things that are hidden to you? One of the things that our researchers are doing is taking a look at a system that is called the Unified Extensible Firmware Interface, or UEFI. Many folks are familiar with the basic input/output system or BIOS. Once you go and you turn on your computer, it goes through the boot-up sequence. Well, over the years, we have retired, as a technology community, the traditional BIOS that many of us grew up with and have moved over to a much more powerful system called UEFI. Well, that is all under the hood, as it were.

Suzanne: Right.

Greg: It is not only on the firmware, but in a partition of the boot disk, and it is very powerful, and it is also in some cases very vulnerable if you do not understand how things work and why. Our team has been taking a look at this as perhaps another attack vector, much like SolarWinds was. But SolarWinds had a finite number of customers. We take a look at, let's just say Windows-based computers. 286 million PCs were sold last year in FY22, or calendar year '22. That is a pretty rich attack surface area. If you take a look at all the others that are out there, the pre-existing Windows-based systems. What is the possibility that a small nugget of code in that UEFI boot stack has been tampered with? And oh, by the way, each vendor has their own custom set. There is a very limited amount of folks who actually write the code for UEFI, but each vendor goes and modifies that stack and through usually 50-to-100 different permutations on each and every device that is out there. Traditional cybersecurity tools do not monitor, do not check that, will not even see it as it goes through the boot cycle.

We just hosted at this year's RSA Conference in San Francisco a discussion for vendors saying, *OK, here is the research that we are doing now, and here are some of the things that we are doing with the community*, because one of the things that we do is, as our background at the CERT Division has, is leadership within the cybersecurity community. So at RSA, we had 150 different vendors attend this session, and a couple of hundred folks either in person or online, and we walked through, *Here are some of the things that we are discovering, but further, here is the community that we have built to go collaborate on the research for this*. There is a lot of work to be done, but we are finding areas where we have recommendations for improvement, so that as new products are coming in and those vendors are doing their modifications to their code for those boot sequences, that secure by design and secure by default [are] built in from the beginning, as opposed to just worrying, *Can I make this thing work regardless of the security posture*? And we got great feedback at RSA for the work that Vijay Sarvepalli, Drew Kompanek, Cory Cohen, Jeff Gennari, and the whole Threat Analysis Directorate have been doing in identifying this issue, helping folks prioritize that, and moreover, providing practical advice on how to make it better.

Suzanne: Excellent, and that is how you prevent the next SolarWinds, is get ahead of it.

Greg: There are other things out there, but I think that one is one right now in our headlights. I am really proud of our team for leaning forward, and like Kevin Mandia raising the alarm saying, *We have a problem here. Let's fix it as a community.*

Suzanne: OK, one more thing for me to worry about is whether my boot-up sequence on my old computer is a UEFI or a BIOS, so, but…

Greg: Well, the thing about it is there are some things, very prudent things that you can do to keep an eye on your systems. First of all, if you do have an older system, I think you don't throw away something that works, but you have to make sure that your defenses are up to date. I for one am not unusual, where I have an older system that has elements of it that are no longer supported. I have in fact recapitalized on my home system. I have a much more modern system that I use for most of my day-to-day internet-connected activities, but that elderly system, it still has a function for me. I have disconnected operations that I do for management of finances, storage of passwords, and all sorts of stuff, but I have deliberately disconnected from the internet. I am finding that I am not alone. There are a lot of folks who have balanced risk and reward and have said, *Well, if the risk of connecting to the internet is high, I am going to disconnect*.

I am also very prudent because I know that you can jump back and forth using different devices and such. I take precautions there because there are methods to attack disconnected things, but it is all a risk-and-reward calculus. For those folks that are, in fact, requiring connection to the internet, do make sure that you are patched. Make sure that your hardware is up to date and is able to run the new, more powerful software that is coming out every day.

Be a discerning customer too. Make sure that you are doing your homework and buying systems that meet your need and have the flexibility to grow to your future needs as well. Do not spend more than you really have to, but make sure that you spend wisely and what you really need to based on the value of your work and the data that you have.

Also, a lot of folks, they think recapitalization of hardware and software, but they do not think about recapitalization of the wetware. You need to make sure that you yourself are properly trained to properly operate the systems that you are using. If you are a supervisor, if you are a leader of an organization, you need to make sure that as you are doing your budget, you are factoring in recapitalization of the wetware with training and making sure that folks are, in fact, well-trained and optimized so that the overall result is an effective, an efficient, and a secure operation. There are plenty of ways to do that. Folks come to us all the time and ask us for recommendations on how to recapitalize the wetware through training and certification as well.

Suzanne: Sure, yes. I know for many of us that work in the government, we have annual updates to all of that kind of training, which is wise because there is always new stuff that is coming out. I will be waiting to see some of the new things coming out as time goes on. I actually have observed over time that some of the things we have talked about in the past are making it into that training, down to even my—I am not a supervisor or anything—but individual-level cyber-awareness training, so we are having an effect. That is a good thing.

Greg: The next jump forward that is absolutely necessary now is that once a year is not good enough, in my view.

Suzanne: Oh, Greg.

Greg: It is one and done, but, and I hesitate to use this word *but*, but I think this is one where I have to use it, and I have to emphasize it.

Suzanne: OK. OK.

Greg: The one and done is not good enough. It needs to be continual training and education, and there are some really good examples out there with some of the research that we have done, as well as in partnership with some of our partners on campus through the CyLab and some of the initiatives that have come out of Carnegie Mellon, such as the Cognitive Immunology Research Collaborative, CIRCE, led by some of our colleagues from campus. Andy, I am talking about you. It is Dr. Andy Norman. As you take a look at the psychology of learning, repetitive training and positive reinforcement for positive actions is critically important, but on the same token, you need to build up a measure of cognitive immunity so that you are not going to fall victim to that phishing because you know what to look for.

I think the repetitive but the entertaining is critically important too. One of the great things about being part of the Carnegie Mellon community is a lot of folks outside of Carnegie Mellon do not necessarily recognize that we have some of the greatest arts programs in the world here, with our drama and our arts departments.

Suzanne: And the Entertainment Technology Center is amazing in bringing together drama, art, science, engineering, so yes, it is.

Greg: Absolutely. We have folks that build some of the greatest computer games and recreation stuff, but we also have some of the greatest artists and entertainers, but all of that. You pair that with our software engineering, our cybersecurity engineering, our artificial intelligence engineering capabilities, and the psychologists that we have on staff—really a powerhouse way of looking at, in the future, how do we continually update the wetware in a manner that produces those results that we want?

And the results we want are an effective, efficient, and secure system that helps protect national security as well as national prosperity. I think that one-and-done annually, that was the way to go 10 years ago and before that. I think where we need to go now is the incremental, continual, but it cannot be boring, because when it is boring, you shut down. You have to see the benefit of that learning. Sometimes a little chunk is better than trying to swallow the whole whale at once.

Suzanne: This may be a future podcast, maybe getting a couple of folks out of that community with you together on a panel to talk about some of this stuff, everything from gamification to continual learning. I think that might be something fun to do.

Greg: Well, and we have the world's experts here at Carnegie Mellon. When we do have that conversation, I will be the dumbest guy in the room.

Suzanne: But you will be learning, and I know that that is one of the things that you value. Greg, I cannot thank you enough for having this conversation. We went way beyond just talking about SolarWinds. I really appreciate and I think our audience will appreciate the variety of topics that we were able to talk about today. I do look forward to our next conversation, because I know there will be one. I hope that our audience has gotten some ideas about how they can participate in preventing these kinds of attacks and the resulting tragedies that sometimes ensue with them.

As all of our podcast audience knows, we will be having lots of references in the transcripts for the different things that we have talked about. I also want to make sure that you know that this podcast is available in both audio and video form, and it is available pretty much wherever you are going to get your podcasts, from Google, Apple, Sound[Cloud], Stitcher, all of those places that have become common, as well as, of course, the SEI's own YouTube channel. Thank you very much for listening today, and thank you again, Greg.

Greg: You are most welcome. Thank you, Suzanne.

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.*